

# TREND MICRO

## Control Manager™ 3

Enterprise Virus Outbreak and Content Security Management

Installation Guide



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 Installation Guide, which are available from Trend Micro's Web site at:

[www.trendmicro.com/download/documentation/](http://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.

Trend Micro, the Trend Micro t-ball logo, Control Manager, Damage Cleanup Services, Outbreak Prevention Services, Trend Virus Control System, Trend VCS, ServerProtect, OfficeScan, ScanMail, InterScan, and eManager are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

All other brand and product names are trademarks or registered trademarks of their respective companies or organizations.

Copyright© 1998-2006 Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

Document Part No. CMEM32569/51128

Release Date: March 2006

The Installation Guide for Trend Micro Control Manager™ is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

For technical support, please refer to Contacting Technical Support starting on page 9-2 for technical support information and contact details. Detailed information about how to use specific features within the software is 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](http://www.trendmicro.com/download/documentation/rating.asp)

---

# Contents

## Preface

What's New in This Version .....	ii
Trend Micro Management Communication Protocol Agents .....	iii
Single Sign-on for Managed Trend Micro Products.....	iii
Spyware/Grayware Detection and Cleanup.....	iii
Improved Communication Security.....	iv
Configure Multiple Update Sources .....	iv
Component Download Granularity.....	v
Component Knowledge Updates .....	v
Active Directory Authentication Integration .....	v
New Event Center Events.....	v
Latest Component Version Updates Through TrendLabs Message Board .....	vi
New Logging Enhancements.....	vi
New Reporting Functions and Presentations .....	vii
Secure Sockets Layer (SSL) Support Management Console and ActiveUpdate .....	vii
Increased Managed Product Support .....	viii
Microsoft Data Engine (MSDE) 2000 Support for Control Manager Database .....	viii
Control Manager 3.0 Service Pack Enhancements.....	viii
Control Manager™ Documentation.....	ix
About This Installation Guide .....	xi
Audience .....	xi
Document Conventions.....	xii

## Chapter 1: Introducing Trend Micro Control Manager™ 3.5

Control Manager Basic Features .....	1-2
Understanding Trend Micro Management Communication Protocol .....	1-3
Reduced Network Loading and Package Size .....	1-3
NAT and Firewall Traversal Support .....	1-4
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 .....	1-6
Cluster Node Support .....	1-7
Control Manager 3.5 Standard and Enterprise Editions .....	1-7
Control Manager Architecture .....	1-8

## **Chapter 2: Planning and Implementing the Control Manager Deployment**

Server Distribution Plan .....	2-2
Network Traffic Plan .....	2-2
Sources of Network Traffic .....	2-3
Log Traffic .....	2-3
Trend Management Infrastructure Policies .....	2-4
Product Registration Traffic .....	2-5
Traffic Frequency .....	2-5
Logs .....	2-6
Trend Micro Management Infrastructure (TMI) Policies .....	2-6
Data Storage Plan .....	2-6
Database Recommendations .....	2-7
ODBC Drivers .....	2-7
Authentication .....	2-7
Administration Plan .....	2-8
Web Server Configuration .....	2-9
Identify Deployment Architecture and Strategy .....	2-10
Test Control Manager Deployment at One Location .....	2-16

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

System Requirements .....	3-2
Minimum System Requirements .....	3-2
Control Manager Agents .....	3-4
Recommended System Requirements .....	3-4
Installing a Control Manager Server .....	3-9
Verifying Successful Installations .....	3-32
Verify a Successful Control Manager Server Installation .....	3-32

---

Post-Installation Configuration .....	3-33
Register and Activate Control Manager .....	3-33
Configure User Accounts .....	3-34
Download the Latest Components .....	3-34
Set Notifications .....	3-34
Registering and Activating Your Software .....	3-34
Activate Control Manager .....	3-35
Convert to the Full Version .....	3-35
Renew Your Product Maintenance .....	3-36

## **Chapter 4: Installing Control Manager Agents**

System Requirements .....	4-2
Control Manager Agents .....	4-2
Installing Control Manager Agents .....	4-3
Prepare for Control Manager Agent Installation .....	4-4
Understanding the Control Manager Agent	
Remote Installation .....	4-5
RemoteInstall.exe .....	4-5
CMAgentSetup.exe .....	4-6
Performing the Installation .....	4-6
Step One: Obtain Required Files .....	4-7
Step Two: Obtain Agent Packages (Optional) .....	4-9
Step Three: Install the Agents .....	4-12
Install the Control Manager agent for	
NetScreen™ Firewall .....	4-25
Verifying Successful Installations .....	4-27
Verify a Successful Agent Installation .....	4-27
Configure MCP for Two-way Communication .....	4-28
Verify the Communication Method Between	
MCP and Control Manager .....	4-29

## **Chapter 5: Upgrading Servers or Migrating Agents to Control Manager 3.5**

Upgrading to Control Manager 3.5 .....	5-2
Upgrade Trend VCS 1.8x Servers .....	5-3
Upgrade Control Manager 2.5 or 3.0 Servers .....	5-3
Roll Back to Trend VCS 1.8x Server .....	5-6

Roll Back to Control Manager 2.5 or 3.0 Server .....	5-7
Planning Trend VCS or Control Manager Agent Migration .....	5-8
Migration Scenarios Trend VCS 1.8x or Control Manager 2.5x Agents .....	5-11
Trend VCS 1.8x Agent Migration Flow .....	5-11
Control Manager 2.5x Agent Migration Flow .....	5-11
MCP Agent Migration Flow .....	5-12
Migrate Trend VCS, Control Manager 2.x, or MCP Agents .....	5-12
Generate a Migration List .....	5-14
Migrate the Control Manager Database .....	5-15
Migrate Control Manager SQL 2000 Database to Another SQL 2000 Server .....	5-15

## **Chapter 6: Getting Started with Control Manager**

Use the Management Console .....	6-2
The Function-Locking Mechanism .....	6-4
Access the Management Console .....	6-5
Assign HTTPS Access to the Control Manager Management Console .....	6-5
Access the HTTPS Management Console .....	6-7
Configure Control Manager User Accounts and Groups .....	6-8
Additional Root Account Privileges .....	6-10
Understanding the User Manager .....	6-11
Setting Access Rights .....	6-11
View .....	6-11
Execute .....	6-12
Configure .....	6-12
Edit Directory .....	6-12
Add a User Account .....	6-12
Import Active Directory Users .....	6-14
Edit a User Account .....	6-15
Disable a User Account .....	6-16
Delete a User Account .....	6-17
Add a User Group .....	6-17
Edit a User Group .....	6-18
Delete a User Group .....	6-18

---

Administer Managed Products .....	6-19
Configure Managed Products Using the	
Product Directory .....	6-19
Default Folder for Managed Products .....	6-21
Use the Product Directory Tabs .....	6-21
Group Managed Products Using Directory Manager .....	6-22
Manage Child Servers .....	6-22
Configure Child Server Using the Cascading Structure Tree .....	6-23
Use the Cascading Structure Tree Tabs .....	6-24
Registering or Unregistering Child Servers .....	6-25
Download and Deploy New Components .....	6-28
Manually Downloading Components .....	6-29
Automatically Downloading Components .....	6-32
Configure Scheduled Download Schedule	
and Frequency .....	6-36
Configure Scheduled Download Settings .....	6-36
Configure Scheduled Download Automatic	
Deployment Settings .....	6-37
Configure Proxy Server Connection for Component	
Download and Trend VCS Agents .....	6-38
Enable HTTPS Download .....	6-38
Enable UNC Download .....	6-39
Set "Log on as batch job" Policy .....	6-40
Deploy Updated Components .....	6-41
Create Deployment Plans .....	6-42
Update All Outdated Components .....	6-43
Monitor the Control Manager Environment .....	6-44
Use Command Tracking .....	6-45
Query and View Commands Issued in the	
Past 24 Hours .....	6-46
Use Event Center .....	6-46
Enable or Disable Notifications .....	6-48
Configure Notification Method .....	6-48
Configure Notification Recipients and Test	
Notification Delivery .....	6-49
Configure Virus Outbreak Alert Settings .....	6-50
Configure Special Virus Alert Settings .....	6-50



Configure Special Spyware/Grayware Alert Settings .....	6-51
Use Reports .....	6-51
Create Report Profiles .....	6-52
Generate On-demand Scheduled Reports .....	6-55
View Generated Reports .....	6-56

## **Chapter 7: Using Tools**

Agent Migration Tool (AgentMigrateTool.exe) .....	7-2
Cascading Management Structure Tool (CasTool.exe) .....	7-2
CasTool.exe Commands .....	7-3
IIS Restoration Tool (SetupPatch.exe) .....	7-5
Web Server and Port Configuration Tool (CMWebCfg.bat) .....	7-6
Using the Control Manager MIB File .....	7-7
Using the NVW 1.x SNMPv2 MIB File .....	7-7
Using the NVW Enforcer SNMPv2 MIB File .....	7-8
Use the NVW System Log Viewer .....	7-8
Use the NVW 1.x Rescue Utility .....	7-8

## **Chapter 8: Removing Trend Micro Control Manager**

Remove a Control Manager Server .....	8-2
Remove a Windows-based Control Manager Agent .....	8-2
Manually Removing Control Manager .....	8-6
Remove the Control Manager Application .....	8-7
Stop the IIS and Control Manager Services .....	8-7
Remove IIS Settings .....	8-8
Delete Control Manager-related Files/Registry Keys .....	8-9
Remove Crystal Reports .....	8-9
Remove the Trend Micro Management Infrastructure .....	8-10
Stop the TMI Service .....	8-10
Delete TMI-related Files .....	8-10
Delete Relevant Registry Keys .....	8-10
Remove the Common CGI Modules .....	8-11
Stop the IIS and CCGI Services .....	8-11
Delete CCGI-related Files .....	8-11
Delete Relevant Registry Keys .....	8-11
Remove Windows Installer Settings .....	8-12
Remove the Database Components .....	8-12

---

Stop the MSDE Service .....	8-12
Stop the SQL Service Manager .....	8-13
Delete MSDE-related Files .....	8-13
Delete Relevant Registry Keys .....	8-13
<b>Chapter 9: Getting Support</b>	
Before Contacting Technical Support .....	9-2
Contacting Technical Support .....	9-2
TrendLabs™ .....	9-3
Other Useful Resources .....	9-3
<b>Appendix A: System Checklists</b>	
Server Address Checklist .....	A-1
Ports Checklist .....	A-3
Agent Installation Checklist .....	A-4
<b>Appendix B: Version Comparison Checklist</b>	
Trend Virus Control System and Trend Micro Control Manager Product Features .....	B-1

## Index



---

# Preface

This Installation Guide introduces Trend Micro Control Manager™ 3.5, guides you through the installation planning and steps, and walks you through the basics of configuring Control Manager to function according your needs.

This preface discusses the following topics:

- *What's New in This Version* on page ii
- *Control Manager™ Documentation* on page ix
- *About This Installation Guide* on page xi
- *Audience* on page xi
- *Document Conventions* on page xii

## What's New in This Version

Trend Micro Control Manager 3.5 represents a significant advance in antivirus and content security products monitoring and management software. Architectural improvements in this new version make Control Manager more flexible and scalable than ever before.

The following new features are available in version 3.5:

- *Trend Micro Management Communication Protocol Agents*
- *Single Sign-on for Managed Trend Micro Products*
- *Spyware/Grayware Detection and Cleanup*
- *Improved Communication Security*
- *Configure Multiple Update Sources*
- *Component Download Granularity*
- *Component Knowledge Updates*
- *Active Directory Authentication Integration*
- *New Event Center Events*
- *Latest Component Version Updates Through TrendLabs Message Board*
- *New Logging Enhancements*
- *New Reporting Functions and Presentations*
- *Secure Sockets Layer (SSL) Support Management Console and ActiveUpdate*
- *Increased Managed Product Support*
- *Microsoft Data Engine (MSDE) 2000 Support for Control Manager Database*
- *Control Manager 3.0 Service Pack Enhancements*

## Trend Micro Management Communication Protocol Agents

Trend Micro Management Communication Protocol (MCP) is Trend Micro's next generation agent for managed products. MCP replaces TMI as the way Control Manager communicates with managed products. See *Understanding Trend Micro Management Communication Protocol* on page 1-3 for more information about MCP.

MCP has several advantages over TMI:

- 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
- Cluster node support

## Single Sign-on for Managed Trend Micro Products

Control Manager 3.5 now 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. The following products support SSO with Control Manager 3.5:

- SeverProtect for Linux version 2.5
- Network VirusWall Enforcer 2500

## Spyware/Grayware Detection and Cleanup

Control Manager 3.5 provides specialized detection and cleanup of spyware/grayware. Control Manager 3.5 logs spyware/grayware events and can send you spyware/grayware notifications. You can also create spyware/grayware specific reports to show the extent of spyware/grayware infection on your environment.

Control Manager now separates viruses and spyware/grayware items in old logs. Converting old logs to the new format can significantly extend the time required to install Control Manager.

## Improved Communication Security

Security Level applies to the virtual folders of IIS, and there are 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 correspond to each security level listed below:

FEATURES	SECURITY LEVEL		
	HIGH	MEDIUM	NORMAL
Supports only HTTPS UI access	●	●	
Supports HTTPS and HTTP UI access			●
Supports redirect to HTTPS or HTTP product UI	●	●	●
Only integrates with HTTPS supported products (MCP)	●		
Integrates with both HTTP and HTTPS supported products		●	●
Supports TVCS 1.x agent		●	●
Allow products to download updates from Control Manager through either HTTP or HTTPS	●	●	●

**TABLE PREFACE-1. Security Level Behavior**

## Configure Multiple Update Sources

From the Update Manager of Control Manager 3.5, you can configure up to five update sources for downloading components. When downloading components Control Manager will attempt to download components from specified update sources sequentially.

## Component Download Granularity

For Control Manager 3.5, the Update Manager now supports granular downloading of component updates.

Both manual and scheduled downloading of components allow you to select which components you want to download. Scheduled downloads also allow you to specify a schedule for each component or component group to update.

## Component Knowledge Updates

This feature allows you to download new component knowledge (information about a new product's components) and import the data by using the merge tool. The information displays on the Control Manager console after a data merge.

## Active Directory Authentication Integration

Control Manager integration with Active Directory supports the following:

- Control Manager can now install on a domain host
- You can now log on to the Control Manager Web console using Active Directory user credentials
- Active Directory users have automatic log-on rights for the Control Manager Web console

## New Event Center Events

Configure Control Manager to send notifications based on Outbreak Prevention Services and Damage Cleanup Services related events (see *Use Event Center* on page 6-46).

Control Manager 3.5 provides the following new events from the Event Center:

- **Special spyware/grayware alert:** applicable to anti-spyware/grayware products
- **Spyware/grayware found:** applicable to anti-spyware/grayware managed products



- **Spyware/grayware found:** first and second actions unsuccessful/unavailable - applicable to anti-spyware/grayware managed products
- **Statistics:** provides statistics on the number of host policy violations versus host compliances complied by Network VirusWall devices

## Latest Component Version Updates Through TrendLabs Message Board

The Trend Micro TrendLabs Message Board provides the version numbers and the time TrendLabs releases antivirus, content security, and services components to help identify the threats so you can proactively update your Control Manager system.

## New Logging Enhancements

Control Manager 3.5 provides new log summary mechanisms generate reports more rapidly and offer significant performance enhancements when sending logs in a cascading environment. Also, child Control Manager logs from managed products get compressed to preserve disk space and increase sending speed. And, Network VirusWall logs can now include 64 byte virus names.

Control Manager 3.5 also supports the following new log types:

- **Policy Violation Statistics Log:** indicates the number of clients that currently violate the policy of Network VirusWall devices. The violation statistics exclude the clients that have complied with the policy that they violated.
- **Policy Violation Log:** indicates the number of clients that violate the policy of Network VirusWall devices.
- **Policy Compliance Log:** indicates the number of clients that comply with the policy minus that clients have violated the policy of Network VirusWall devices.
- **End Point Network Virus Log:** indicates the number of network virus attacks on an OfficeScan client (derived from Common Virus Wall logs)

## New Reporting Functions and Presentations

Control Manager 3.5 enhances reporting with the following:

1. Support for the report category **Network Products** for Network VirusWall devices and the following new report types for Network VirusWall devices
  - Service Violation Report
  - Policy Violation Report
  - Most Commonly Detected Clients in Violation Report
2. Support for machine filtering by IP address or IP segment. Network VirusWall then includes specified machines in the Network VirusWall generated reports.
3. Support for setting report frequency by calendar day. This feature allows you configure the start and end time of the data range for your reports.
  - When enabled: Use the calendar day option to set the data range from 00:00:00 for the start date to 23:59:59 for the end date.
  - When disabled: The calendar day option sets the same time for the start date and end date.
4. Spyware/grayware items are not counted as viruses in virus statistics reports.
5. Support for new report types. Control Manager now supports the following new report types:
  - OfficeScan 7.0 license update report
  - OPS report (After OPP stops, Control Manager generates an OPS report automatically. The report shows the number of viruses present during OPS)

## Secure Sockets Layer (SSL) Support Management Console and ActiveUpdate

Utilize Secure Sockets Layer (SSL) to help ensure secure communications between your Web browser and the Control Manager server. In addition, Control Manager supports secure component download either from the Trend Micro ActiveUpdate server or from your companies update server.

## Increased Managed Product Support

Control Manager 3.5 has expanded support to the following Trend Micro managed products:

- Trend Micro InterScan for Cisco Content Security and Control Security Services Module (ISC CSC SSM)
- Server Protect for Linux 2.5
- Network VirusWall 2500 2.0
- Anti-Spyware Enterprise Edition 1.0
- Damage Cleanup Service 3.0
- ScanMail for Exchange 7.0
- Trend Micro IM Security for Microsoft™ Office Live Communications Server 1.0

## Microsoft Data Engine (MSDE) 2000 Support for Control Manager Database

In addition to Microsoft SQL Server 7.0 Desktop Engine, Control Manager 3.0 supports MSDE 2000 that allows reliable storage engine and query processor.

The Control Manager installation package contains MSDE 2000 Service Pack 3.

## Control Manager 3.0 Service Pack Enhancements

The following enhancements are derived from Control Manager 3.0 Service Packs 3 and 4:

1. TCM provides a flexible log/command proxy mechanism to allow third-party managed products to receive logs from Control Manager and send commands to managed products through Control Manager.
2. Control Manager now supports the Case Diagnostic Tool (CDT) mechanism.
3. Product profile/binary upload supports build upgrade/replacement. The new builds replace the originals that have the same version (major and minor) and language.

4. New Java Runtime environments supported for Windows platforms:
  - Java(TM) 2 Runtime Environment Standard Edition 1.4.2\_08
  - J2SE(TM) Runtime Environment 5.0 Update 4
5. Supports Window 2003 Server Service Pack 1.
6. Improved performance when deleting temporary logs on child servers.

## Control Manager™ Documentation

The Control Manager™ documentation consists of the following:

DOCUMENT	DESCRIPTION
<b>Online Help</b>	<p>Web-based documentation that is accessible from the Control Manager™ management console.</p> <p>The online help contains explanations of Control Manager™ components and features, as well as procedures needed to configure Control Manager.</p>
<b>Knowledge Base</b>	<p>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:</p> <p><a href="http://kb.trendmicro.com">http://kb.trendmicro.com</a></p>
<b>Readme file</b>	<p>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.</p>
<b>Installation Guide</b>	<p>Printed documentation provided in the package contents and PDF form that is accessible from the Trend Micro Enterprise CD or downloadable from the Trend Micro Web site.</p> <p>The Installation Guide contains detailed instructions of how to install Control Manager and configure basic settings to get you "up and running". See <i>About This Installation Guide</i> for a summary of the chapters available in this book.</p>

**TABLE PREFACE-2. Control Manager Documentation**

DOCUMENT	DESCRIPTION
<b>Administrator's Guide</b>	PDF documentation that is accessible from the Trend Micro Solutions CD for Control Manager™ or downloadable from the Trend Micro Web site.  This 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.

**TABLE PREFACE-2. Control Manager Documentation**

---

**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 Installation Guide

The Control Manager Installation Guide provides the following information:

TASK	DESCRIPTION
Pre-Installation	<b>Chapter 1:</b> Provides an overview of the Control Manager, product architecture, and a description of all features
	<b>Chapter 2:</b> Provides deployment and product application information and Trend Micro recommendations on the optimal deployment of Control Manager
Installation and Upgrading	<b>Chapter 3:</b> Provides installation instructions for Trend Micro Control Manager 3.5
	<b>Chapter 4:</b> Provides information on migrating TCVS and Control Manager 2.x agents to Control Manager 3.5 servers
Post Installation	<b>Chapter 5:</b> Provides information on basic Web console navigation, managing and updating managed products and child servers, and monitoring the Control Manager environment
	<b>Chapter 6:</b> Provides information and procedures for using Control Manager tools
	<b>Chapter 7:</b> Provides information and procedures for removing Control Manager
	<b>Chapter 8:</b> Provides information for troubleshooting tips on issues encountered during administration, which includes debug and error log information
Appendices	<ul style="list-style-type: none"> <li>• <i>System Checklists</i></li> <li>• <i>Version Comparison Checklist</i></li> </ul>


TABLE PREFACE-3. Installation Guide High-Level Overview

## 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 (Online help and Installation Guide) uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
<b>Bold</b>	Menus and menu commands, command buttons, tabs, and options
Monospace	Examples, sample command lines, program code, and program output
	Represents Control Manager 3.5 Enterprise edition topics
<hr/> <p style="text-align: center;"><b>Note:</b></p> <hr/>	Provides configuration notes or recommendations

**TABLE PREFACE-4. Control Manager Documentation Conventions**

# Introducing Trend Micro Control Manager™ 3.5

Trend Micro Control Manager™ is a central management console that manages Trend Micro products and services, third-party antivirus and content security products 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 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 discusses the following topics:

- *Control Manager Basic Features* on page 1-2
- *Understanding Trend Micro Management Communication Protocol* on page 1-3
- *Control Manager 3.5 Standard and Enterprise Editions* on page 1-7
- *Control Manager Architecture* on page 1-8



## Control Manager Basic Features

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

Major Control Manager features include:

- **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 and content security policies.
- **Proactive outbreak prevention:** With Outbreak Prevention Services (OPS), take proactive steps to secure your network against an emerging virus outbreak
- **Secure communication infrastructure:** Control Manager uses a communications infrastructure built on the Secure Socket Layer (SSL) protocol  
Depending on the security settings used, Control Manager can encrypt messages or encrypt them with authentication.
- **Secure configuration and component download:** These features allow you to configure secure 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 via 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 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
- **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) 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 advantages over TMI:

- 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
- Cluster node 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 the 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.

With the issues mentioned above, MCP's data format is devised 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 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 is 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 IPs 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 TMI-based 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 agent sits behind a NAT device (or TCMC 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 TCMC 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. You can configure MCP agents to use one-way or two-way communication with MCP agents. For more information, see *Configure MCP for Two-way Communication* on page 4-28.

### 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 end needs to have 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 3.5 now 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.

The following products support SSO with Control Manager 3.5:

- SeverProtect for Linux version 2.5
- Network VirusWall 2500 version. 2.0

## Cluster Node Support

Under varying cases administrators may like to group certain product instances as a logical unit, or cluster (for example products installed under a cluster environment present all installed product instances under one cluster group). However, from the Control Manager server's perspective, each product instance that goes through the formal registration process is regarded as an independent managed unit and each managed unit is no different from another.

Through MCP, Control Manager supports cluster nodes.

## Control Manager 3.5 Standard and Enterprise Editions

Control Manager has two versions:

- The **Standard edition** provides powerful management and configuration features that allow you to manage your corporate antivirus and content security.
- The **Enterprise edition** adds a variety of advanced features to the Standard edition, including cascading console support and reporting functions.

The following table presents the features supported by each edition:

FEATURE	STANDARD	ENTERPRISE
Cascading management structure	No	Yes
Managed product reporting	No	Yes
Managed products administration	Yes	Yes
Outbreak Prevention Services	Subscription-based	Subscription-based
Damage Cleanup Services	Subscription-based	Subscription-based
Vulnerability Assessment	Subscription-based	Subscription-based
TrendLabs message board	Yes	Yes
Child server monitoring	n/a	Yes
Child server task issuance	n/a	Yes

**TABLE 1-1. Feature comparison between Enterprise and Standard editions**

FEATURE	STANDARD	ENTERPRISE
Child server reporting	n/a	Yes
Trend Micro Product Registration server support	Yes	Yes
HTTPS management console	Yes	Yes
HTTPS ActiveUpdate	Yes	Yes
Trend Micro Network VirusWall 1200 and InterScan Web Security Service integration	Yes	Yes
MSN Messenger notification	Yes	Yes

**TABLE 1-1. Feature comparison between Enterprise and Standard editions**

The Control Manager Standard edition provides management of antivirus and content security products without the reporting feature. The cascading management structure of Control Manager Enterprise edition allows system administrators to administer other Control Manager servers and monitor overall Control Manager network status via logs and reports.

This documentation covers all features of Control Manager. Except for the Feature List Comparison, the Control Manager online help and Installation Guide do not distinguish between the two versions.

## Control Manager Architecture

Trend Micro Control Manager provides a means to control Trend Micro products and services, and third-party antivirus and content security products from a central location. This application simplifies the administration of a corporate virus and content security policy. Control Manager uses the following components:

- **Control Manager server** - acts as a repository for all data collected from the agents. It can be a Standard or Enterprise 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** via email

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, Windows event log, MSN Messenger, SNMP, pager, or any in-house/industry standard application used by your organization to send notification.

- A **report server**, *present only in the Enterprise edition*, that generates antivirus and content security product reports

A Control Manager report is an online collection of figures about virus and content security events that occur on the Control Manager network.

- **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 installs 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 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 managed products. They interact with Control Manager agents to communicate to managed products.

- **Agent** - 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, you must install agents on the same machine as managed products.



- **Web-based management console** - allows an administrator to manage Control Manager from virtually any computer with an Internet connection and Microsoft™ Internet Explorer™

The Control Manager management console is a Web-based console published on the Internet via the Microsoft Internet Information Server (IIS) and hosted by the Control Manager server. It lets you administer the Control Manager network from any machine using a compatible Web browser.

# Planning and Implementing the Control Manager Deployment

Several factors must be taken into consideration before deploying Control Manager to your network. This chapter helps you plan for Control Manager deployment and manage a Control Manager test deployment.

This chapter discusses the following topics:

- *Server Distribution Plan* on page 2-2
- *Network Traffic Plan* on page 2-2
- *Data Storage Plan* on page 2-6
- *Administration Plan* on page 2-8
- *Web Server Configuration* on page 2-9
- *Identify Deployment Architecture and Strategy* on page 2-10
- *Test Control Manager Deployment at One Location* on page 2-16

## Server Distribution Plan

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.

---

**Note:** Now that Control Manager supports multiple user accounts, segregation that was necessary for Trend Virus Control System (Trend VCS) is no longer needed. For information on merging multiple Trend VCS servers under a single Control Manager server, see *Migration Scenarios Trend VCS 1.8x or Control Manager 2.5x Agents* on page 5-11.

---

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

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 (see the next section).

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.

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 *Network Traffic Plan* on page 2-2.

## Network Traffic Plan

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

The following section helps you understand the traffic that is generated by your Control Manager network 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.

## Sources of Network Traffic

The following Control Manager sources generate network traffic:

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

## Log Traffic

A perpetual source of network traffic in a Control Manager network are the ‘Client logs’ — logs that managed products regularly send to the Control Manager server.

LOG	CONTAINS INFORMATION ABOUT
Virus/Spyware/Grayware	Detected viruses, spyware/grayware, and other Internet threats
Security	Violations reported by content security products
Web Security	Violations reported by Web security products
Event	Miscellaneous events that are not included in the aforementioned logs (for example, component updates, generic security violations, etc.)
Status	The environment of a managed product. The Status tab of the Product Directory displays this information
Network Virus	Outbreaks occurred on networks
Network Outbreak Monitor	Virus detected in network packets

**FIGURE 2-1. Control Manager Logs**

LOG	CONTAINS INFORMATION ABOUT
URL Usage	Violations reported by Web security products
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

**FIGURE 2-1. Control Manager Logs**

## Trend Management Infrastructure Policies

The Trend Management Infrastructure (TMI) — the communications backbone of Control Manager — generates its own ‘housekeeping’ traffic. TMI implements two policies:

- Communicator Heartbeat
- Work-hour policy

### Communicator

The Communicator, the commercial name for 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.

Two types of information, however, 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, etc.)
- Product name
- Product version
- Menu version
- Log format
- Update component information (updates that the product supports, for example, virus pattern files, etc.)
- Command information

By default, Control Manager servers contain all the product profiles that were available when the products were 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.

## Traffic Frequency

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

- Logs
- Trend Micro Management Infrastructure policies
- MCP policies

## Logs

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

## Trend Micro Management Infrastructure (TMI) Policies

By default, TMI sends heartbeat messages every sixty minutes. This can be adjusted to anywhere 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 a Communicator is resolved between heartbeats, it then becomes possible to communicate with a Communicator—even if its status appears as "Inactive" or "Abnormal".

- **Short-interval Heartbeats (below 60 minutes)** - short intervals between heartbeats presents a more up-to-date picture of your network status at the Control Manager server. However, this increases the amount of network bandwidth used.

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.

## 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 Database Engine (MSDE). However, due to the limitations of MSDE, large networks require an SQL server.

---

**Note:** Control Manager uses mixed-mode authentication, not Windows authentication, to access the SQL server.

---

## Database Recommendations

If you install Control Manager and its SQL server on the same machine, 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 machine. 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, not Windows authentication.



## Administration Plan

Early on, 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.

Refer to *Group Managed Products Using Directory Manager* on page 6-22 for details on how to group managed products.

## 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.

In Control Manager 3.5, the setup program offers three Web access security levels for administrators accessing the Control Manager Web console:

- **Normal – HTTP based:** Access to the Web console through HTTP only
- **Medium – HTTPS primary:** Access to the Web console through HTTPS in the environment supports HTTPS. If the environment does not support HTTPS, HTTP is used instead
- **High – HTTPS only:** Access to the Web console through HTTPS only

## Identify Deployment Architecture and Strategy

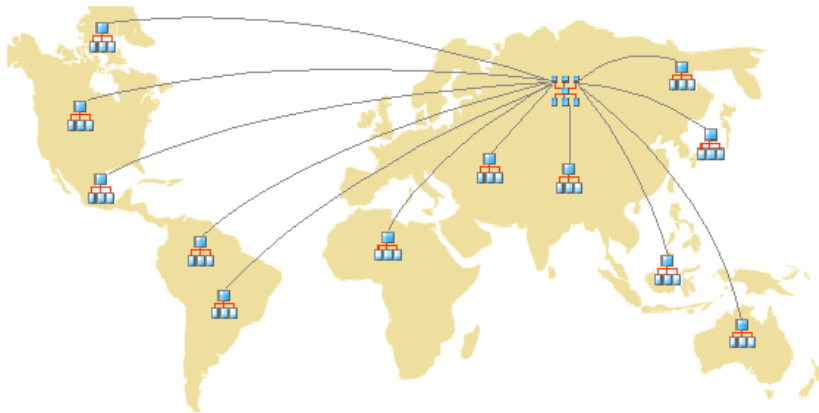
Deployment is the process of strategically distributing Control Manager servers to your network environment to facilitate and provide optimal management of antivirus and content security products.

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 applies to your environment.



**FIGURE 2-2. A single-server deployment using Enterprise Control Manager parent server and child servers**

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

- Determine 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 position 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.

- Plan 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* on page 3-4 as a guide in determining the CPU and RAM requirements for your Control Manager network.

- Designate the Standard Control Manager server or Enterprise Control Manager server

Based on the number of managed products and cascading structure requirements, decide and designate your Control Manager server. Decide whether to designate an Enterprise or Standard server (refer to *Feature comparison between Enterprise and Standard editions* on page 1-7).

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

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

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

If 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.

---

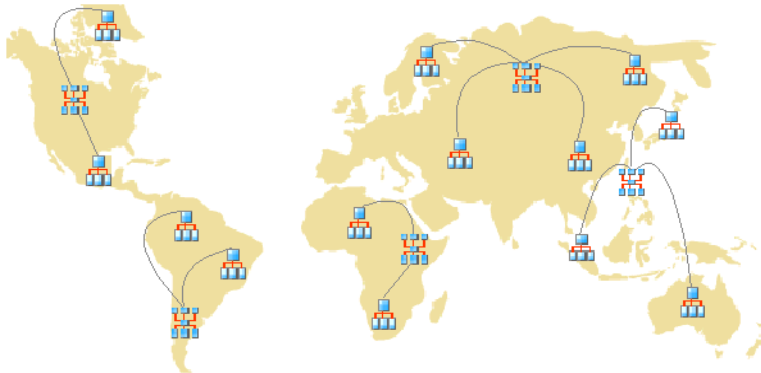
**Note:** Both OfficeScan and Control Manager use IIS to communicate with clients and agents/child servers, respectively. These two applications do not conflict, but since both use IIS resources, Trend Micro recommends installing Control Manager on another machine to reduce performance stress on the server.

---

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

- **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.



**FIGURE 2-3. A multi-site deployment using multiple Enterprise Control Manager parent server and mixed child servers**

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

Specifically, you need to:

- Group managed products or child servers

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

- 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.

- Determine the number of sites

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

You may get this information from your organization's WAN or LAN topology charts.

- Determine 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 be managing. 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.

- Plan 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 its impact on an organization's network by consider the following Control Manager-related network traffic sources:

- 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

Refer to *Network Traffic Plan* on page 2-2 for more information.

- Plan for an optimal server-managed products/cascading structure ratio

When deploying Control Manager across the WAN, the Control Manager server in the main office manages 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 a diversified 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.

- Designate the Standard Control Manager server or Enterprise Control Manager server
- Decide where to install the Control Manager server

Once you know how many clients and servers you need to install, decide where to install your Control Manager servers. Decide if you must install all servers in the central office or if some must go into remote offices.

Strategically arrange the servers 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 the majority of the managed products and child servers in an 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.

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, bandwidth limitations may influence communication to and from the Control Manager 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.

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

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

---

**Note:** If using Control Manager for the first time, Trend Micro recommends using a Control Manager Enterprise edition parent server to handle single-site and multiple-site deployments.

---



## Test Control Manager Deployment at One Location

Trend Micro recommends conducting a test/pilot deployment before performing a full-scale deployment. A pilot deployment allows you to gather feedback, learn how features work and determine what level of support you will likely need after a full deployment.

Testing Control Manager at one location accomplishes the following:

- Familiarity with Control Manager and managed products
- Develop or refinement of the company's network policies

A test 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
- Selecting a test site
- Creating a rollback plan
- Beginning the test deployment
- Evaluating the test deployment

### Preparing for the Test Deployment

Complete the following activities during the preparation stage:

1. Decide the Control Manager server and agent configuration for the test environment.
2. Establish TCP/IP connectivity among all systems in a heterogeneous trial configuration.
3. Verify bidirectional TCP/IP communications by sending a ping command to each agent system from the manager system and vice versa.
4. Evaluate the different deployment methods to see which ones are suitable for your particular environment.
5. Complete the System Checklists to be used for the test deployment.

### **Selecting a Test Site**

Select a test 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**

Trend Micro recommends creating a disaster recovery or rollback plan (for example, how to roll back to Control Manager 2.x or Trend VCS 1.8x server) should you experience difficulties with the installation or upgrade.

### **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.



# Installing Trend Micro Control Manager for the First Time

This chapter guides you through installing Control Manager server and agents. In addition to listing the system requirements for both the Control Manager server and agents it 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 3-9
- *Verifying Successful Installations* on page 3-32
- *Post-Installation Configuration* on page 3-33
- *Registering and Activating Your Software* on page 3-34

## 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:** Minimal requirements of child CM Server:

- Control Manager 3.0
- Control Manager 3.0 SP1 to SP5
- Control Manager 3.5

Control Manager 2.5 cannot be part of a cascading environment.

---

HARDWARE/SOFTWARE SPECIFICATION	MINIMUM REQUIREMENT
<b>CPU</b>	Intel™ Pentium™ III Processor 600 MHz <ul style="list-style-type: none"> <li>• Single CPU</li> <li>• Dual CPU</li> <li>• Quad CPU</li> </ul>
<b>Hard Disk</b>	300 MB
<b>Memory</b>	512 MB of RAM and above

**TABLE 3-1. Trend Micro Control Manager 3.5 Server Minimum System Requirements**

HARDWARE/SOFTWARE SPECIFICATION	MINIMUM REQUIREMENT
<b>Operating System</b>	<ul style="list-style-type: none"> <li>• Microsoft Windows 2000 Server + SP1/SP2/SP3/SP4</li> <li>• Windows 2000 Advanced Server + SP1/SP2/SP3/SP4</li> <li>• Windows 2003 Standard Edition + SP1</li> <li>• Windows 2003 Enterprise Edition + SP1</li> </ul>
<b>Web Server</b>	<ul style="list-style-type: none"> <li>• Microsoft SQL 7.0</li> <li>• Microsoft MSDE 2000</li> <li>• Microsoft SQL 2000</li> <li>• Microsoft IIS server 5.0 (For 2000 platform)</li> <li>• Microsoft IIS server 6.0 (For 2003 platform)</li> </ul>
<b>Display</b>	VGA (800 x 600 / 256 color) or higher

**TABLE 3-1. Trend Micro Control Manager 3.5 Server Minimum System Requirements**

HARDWARE/SOFTWARE SPECIFICATION	MINIMUM REQUIREMENT
<b>CPU</b>	Intel Pentium III Processor 600Mhz
<b>Hard Disk</b>	20 MB
<b>Memory</b>	128 MB of RAM (256 MB recommended)
<b>Operating System</b>	<ul style="list-style-type: none"> <li>• Windows 98/ME</li> <li>• Windows NT 4.0</li> <li>• Windows 2000 Professional</li> <li>• Windows XP</li> <li>• Windows 2000Server</li> <li>• Windows 2000 Advanced Server</li> <li>• Windows 2003 Standard</li> <li>• Windows 2003 Enterprise</li> </ul>

**TABLE 3-2. Trend Micro Control Manager 3.5 Management Console Minimum System Requirements**

HARDWARE/SOFTWARE SPECIFICATION	MINIMUM REQUIREMENT
Other	<ul style="list-style-type: none"> <li>• VGA (800 x 600 / 256 color) or higher</li> <li>• IE 5.5 + SP2 or above</li> <li>• MS JVE</li> <li>• Sun JVE 1.4.2, 1.5.0</li> </ul>

**TABLE 3-2. Trend Micro Control Manager 3.5 Management Console Minimum System Requirements**

## Control Manager Agents

MICROSOFT	OTHERS
<ul style="list-style-type: none"> <li>• Windows XP Professional Version</li> <li>• Windows 2000 Server</li> <li>• Windows 2000 Advanced Server</li> <li>• Windows NT 4.0 + SP3</li> <li>• Windows NT 4.0 + SP6a or later</li> <li>• Windows 2003 Standard Edition</li> <li>• Windows 2003 Enterprise Edition</li> </ul>	<ul style="list-style-type: none"> <li>• Novell Desktop 9</li> <li>• AIX</li> <li>• Red Hat Linux 6.2, 7.1, 7.2</li> <li>• RedHat Enterprise Linux 4.3</li> <li>• Turbolinux 6.5, 7.0</li> <li>• SuSE Linux 6.3, 7.2, 7.3</li> <li>• SuSE Enterprise 9.2</li> <li>• AS/400</li> <li>• OS390</li> <li>• Others: GateLock, Linux 6.x kernel, Solaris 2.6, 2.7, 2.8, Debian 3.1 4</li> </ul>

Please refer to the managed product documentation for detailed agent system requirements. Refer to the following URL to download the latest Control Manager 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 Trend Micro Control Manager on a Primary Domain Controller (PDC) or a Backup Domain Controller (BDC)
- Physical memory is a system resource – all applications on the server share it. Scale the memory with the processor; do not overpopulate with memory

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.

**TABLE 3-3. General Control Manager server recommendations**

## Sizing Recommendations

The following are recommendations for a single Control Manager server and for a parent Control Manager server.

The following recommendations apply to the indicated network sizes for a single Control Manager server.

CONTROL MANAGER SERVER	ENVIRONMENT	RECOMMENDATION
Single	Number of: <ul style="list-style-type: none"> <li>• Control Manager agents: 1000</li> <li>• TVCS agents: 500</li> <li>• OSCE 6.5 clients: 2000</li> <li>• Total above: 2000</li> </ul>	<ul style="list-style-type: none"> <li>• Intel Pentium III 450MHz or equivalent</li> <li>• 256MB</li> <li>• MSDE (local)</li> </ul>

**TABLE 3-4. Control Manager recommended system requirements**



CONTROL MANAGER SERVER	ENVIRONMENT	RECOMMENDATION
Single/Child	Number of: <ul style="list-style-type: none"> <li>• Control Manager agents: 1500</li> <li>• TVCS agents: 500</li> <li>• OSCE 6.5 clients: 5000</li> <li>• Total above: 5000</li> </ul>	<ul style="list-style-type: none"> <li>• Intel Pentium III 1GHz or equivalent</li> <li>• 512MB RAM</li> <li>• SQL Server (local)</li> </ul>
Parent	Number of: <ul style="list-style-type: none"> <li>• Control Manager agents: 10000</li> <li>• TVCS agents: 2500</li> <li>• OSCE 6.5 clients: 10000</li> <li>• Total above: 10000</li> <li>• Child Control Manager servers: 50</li> </ul>	
Single/Child	Number of: <ul style="list-style-type: none"> <li>• Control Manager agents: 2000</li> <li>• TVCS agents: 500</li> <li>• OSCE 6.5 clients: 10000</li> <li>• Total above: 10000</li> </ul>	<ul style="list-style-type: none"> <li>• Intel Pentium III 1GHz or equivalent</li> <li>• 1GB RAM</li> <li>• SQL Server (remote)</li> </ul>
Parent	Number of: <ul style="list-style-type: none"> <li>• Control Manager agents: 20000</li> <li>• TVCS agents: 5000</li> <li>• OSCE 6.5 clients: 100000</li> <li>• Total above: 100000</li> <li>• Child Control Manager servers: 100</li> </ul>	

**TABLE 3-4. Control Manager recommended system requirements**

CONTROL MANAGER SERVER	ENVIRONMENT	RECOMMENDATION
Single/Child	Number of: <ul style="list-style-type: none"> <li>Control Manager agents: 5000</li> <li>TVCS agents: 1000</li> <li>OSCE 6.5 clients: 10000</li> <li>Total above: 15000</li> </ul>	<ul style="list-style-type: none"> <li>Intel Pentium 4 2GHz or equivalent</li> <li>2GB RAM</li> <li>SQL Server (remote)</li> </ul>
Parent	Number of: <ul style="list-style-type: none"> <li>Control Manager agents: 50000</li> <li>TVCS agents: 10000</li> <li>OSCE 6.5 clients: 200000</li> <li>Total above: 200000</li> <li>Child Control Manager servers: 200</li> </ul>	

**TABLE 3-4. Control Manager recommended system requirements**

NUMBER OF MANAGED PRODUCTS	NUMBER OF CPUs	CPU SPECIFICATION	RAM	DATABASE REQUIREMENTS
Less than 500 products	One	Intel Pentium III 500MHz	500MB	MSDE (2GB)
500 to 1,000 products	One	Intel Pentium III 500MHz	500MB	MSDE or MS SQL 7 / 2000
Above 1,000 products	One	Intel Pentium III 1GHz	1GB	MSDE or MS SQL 7 / 2000 Dedicated connection between the Control Manager database and SQL server.

**TABLE 3-5. Additional recommended system requirements for a single Control Manager server**

MAXIMUM LOGS/HR	NUMBER OF ENTITIES	CPU SPECIFICATIONS	RAM	DISK
20,000	1-1,000	Single Intel Xeon™ 2.0 GHz	512MB	IDE 7200 RPM or SCSI 17 GB
36,522	1-1,000	Single Intel Xeon™ 2.0 GHz	1GB	IDE 7200 RPM or SCSI 17 GB
46,452	1-1,000	Single Intel Xeon™ 2.0 GHz with Hyper-Threading (HT)	1GB	IDE 7200 RPM or SCSI 17 GB
75,000	1-1,000	Dual Intel Xeon™ 2.4 GHz	1GB	SCSI 17 GB
90,000	1-10,000	Dual Intel Xeon™ 2.4 GHz with HT	1GB	SCSI 17 GB

**TABLE 3-6. Minimum suggested hardware for Control Manager 3.5 server with database installed**

MAXIMUM LOGS/HR	NUMBER OF ENTITIES	CPU SPECIFICATIONS	RAM	DISK
40,000	1-1,000	Single Intel Xeon™ 2.0 GHz	256MB	IDE 7200 RPM or SCSI 17 GB
63,717	1-1,000	Single Intel Xeon™ 2.0 GHz	512MB	IDE 7200 RPM or SCSI 17 GB
66,667	1-1,000	Single Intel Xeon™ 2.0 GHz with HT	512MB	IDE 7200 RPM or SCSI 17 GB
112,500	1-10,000	Dual Intel Xeon™ 2.4 GHz	512MB	SCSI 17 GB

**TABLE 3-7. Minimum suggested hardware for Control Manager 3.5 server with separate database Server**

MAXIMUM LOGS/HR	NUMBER OF ENTITIES	CPU SPECIFICATIONS	RAM	DISK
40,000	1-1,000	Single Intel Xeon™ 2.0 GHz	512MB	IDE 7200 RPM or SCSI 17 GB
63,717	1-1,000	Single Intel Xeon™ 2.0 GHz	1GB	IDE 7200 RPM or SCSI 17 GB
66,667	1-1,000	Single Intel Xeon™ 2.0 GHz	1GB	IDE 7200 RPM or SCSI 17 GB
112,500	1-10,000	Dual Intel Xeon™ 2.4 GHz with HT	1GB	SCSI 17 GB

**TABLE 3-8. Minimum suggested hardware for remote SQL database server**

DATABASE	PROCESSORS	RAM	DATABASE
Microsoft Desktop/Data Engine	2	2GB	2 Gigabytes
Microsoft SQL Server 2000 Standard Edition	4	2GB	1048516 Terabytes
Microsoft SQL Server 2000 Enterprise Edition	32	64GB	1048516 Terabytes

**TABLE 3-9. Control Manager server limitations imposed by database specifications**

## 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-1 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 mixed-mode authentication, not Windows authentication, 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 MSDE, which can only handle a limited number of connections

Installing Control Manager requires performing the following steps:

**Step 1:** Registering and activating the product and services

**Step 2:** Specifying Control Manager server file location and communications settings

**Step 3:** Choosing and configuring database information

**Step 4:** Setting up root accounts and configuring proxy servers

**Step 5:** Configuring notification settings

---

**Tip:** Trend Micro recommends that you install Control Manager 3.0 on a separate server, rather than upgrading Trend VCS 1.x or Control Manager 2.5 to version 3.0. This way, the original server remains intact, allowing you to de-commission the original server in a timely and effective manner. For more information about upgrading, see [Upgrading to Control Manager 3.5](#) on page 5-2.

---

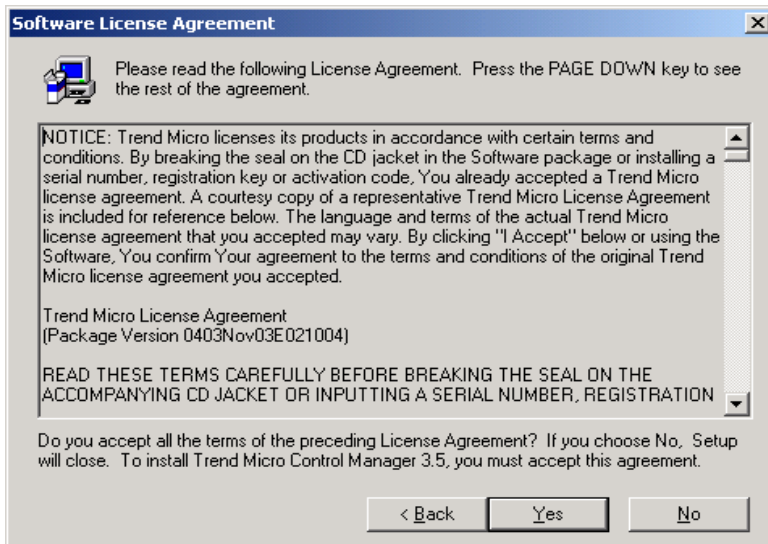
## To install a Control Manager server:

### Step 1: Register and activate the product and services

1. On the Windows taskbar, click **Start** > **Run**, and then locate the Control Manager installation program (Setup.exe). If you are installing from the Trend Micro Enterprise Protection CD, go to the Control Manager folder on the CD. 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 existing components. The Welcome screen appears.

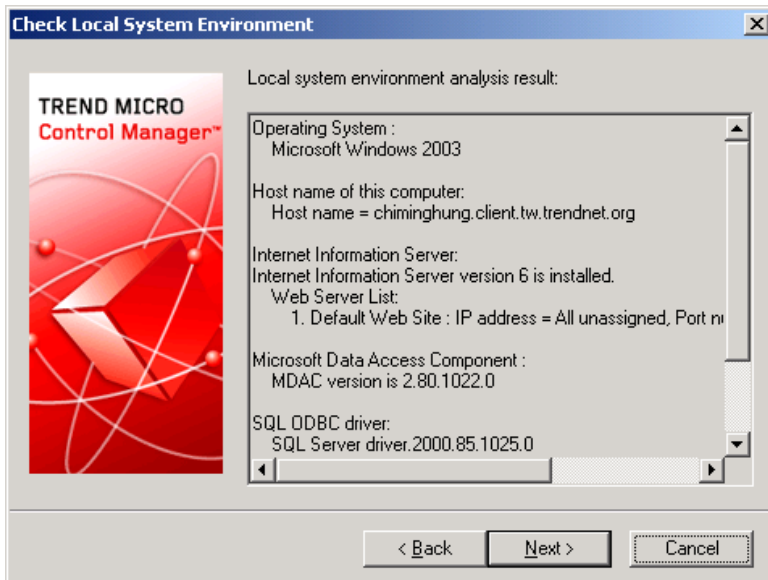
The setup program can detect an existing copy of Trend Virus Control System, and give you the option to migrate it to Control Manager; doing so also upgrades all Trend VCS agents on your system. Before proceeding with the installation close all instances of the Microsoft Management Console. For more information about migration see *Planning Trend VCS or Control Manager Agent Migration* on page 5-8.

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



**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.



**FIGURE 3-2.** Displays local system environment information

3. Click **Next**. The Name and Company Information screen appears.



**Name and Company Information** [X]

TREND MICRO  
Control Manager™

Enter your name and company.

Your name:

Company:

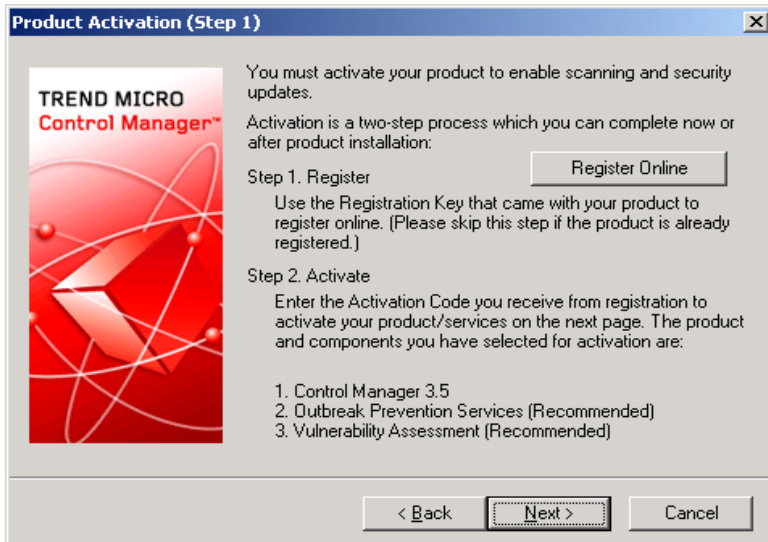
< Back   Next >   Cancel

**FIGURE 3-3.** Enter your name and company

4. Type your name and company.

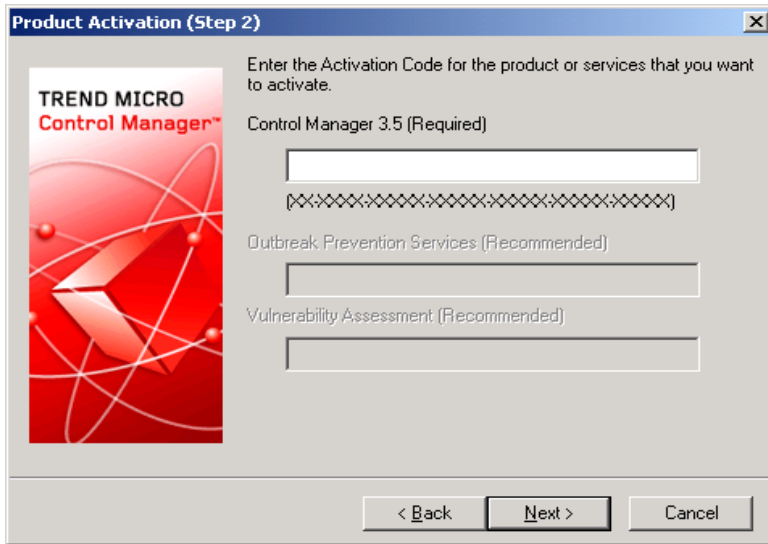


5. Click **Next**. The Product Activation screen (Step 1) appears.



6. Click **Register Online** and follow the Trend Micro Online Registration Web site on-screen instructions to register your product. Register your product to ensure you are eligible to receive the latest security updates and other product and maintenance services. After registration is complete, Trend Micro issues an Activation Code you use to activate Trend Micro software and other Trend Micro services.

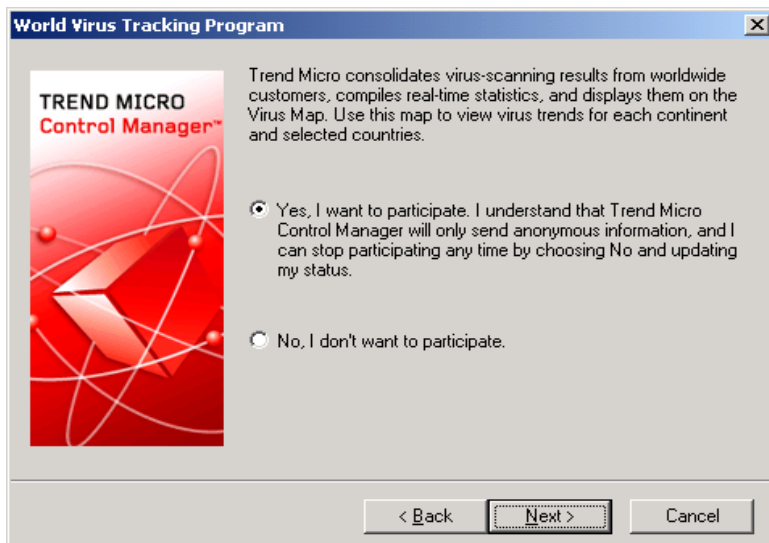
7. Click **Next**. The Product Activation screen (Step 2) appears.



**FIGURE 3-5. Enter the Activation Code to activate Control Manager and services**

8. 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 3.0 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.

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

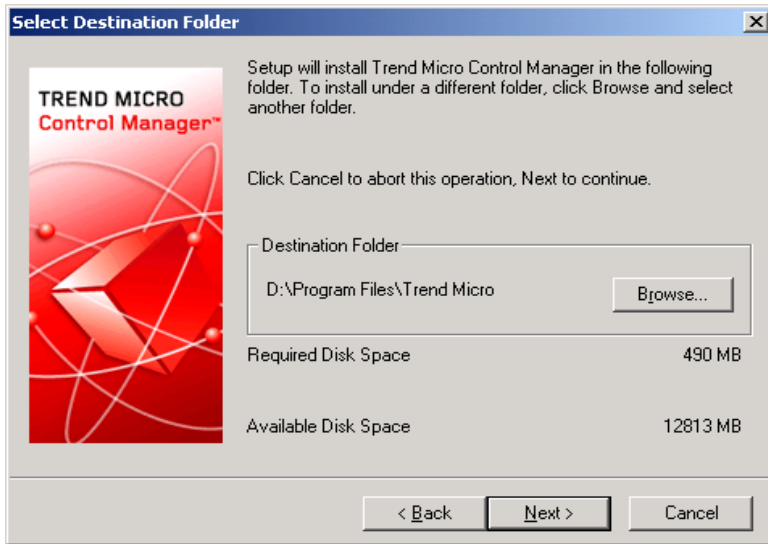


**FIGURE 3-6. Participate in the World Virus Tracking Program**

10. 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 via HTTP, and you can stop participating any time by choosing No and updating your status on the Control Manager management console.

## Step 2: Specify Control Manager server file location and communications settings

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



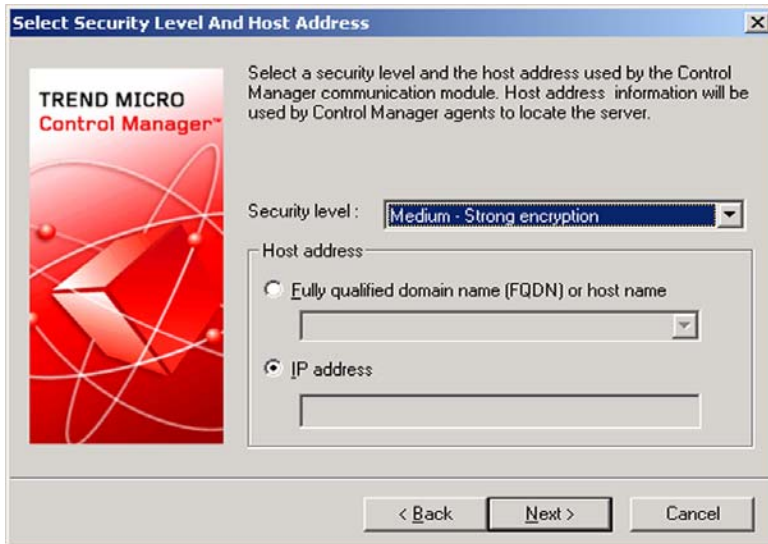
2. Specify a location for Control Manager files. The default location is C:\Program Files\Trend Micro. To change this location, click **Browse**, and then specify an alternate location.

---

**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.

---

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



**FIGURE 3-7.** Select a security level

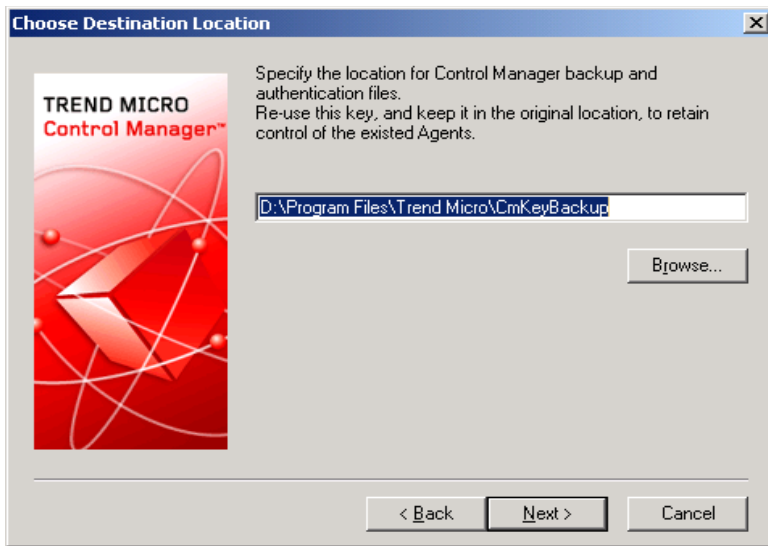
4. From the Security level list, select the security level for Control Manager communication with agents. The options are as follows:
  - **High - HTTPS only:** All communication between Control Manager and managed products uses HTTPS protocol. This ensures the most secure communication between Control Manager and managed products. Select this option if all of your managed products use MCP agents.
  - **Medium - HTTPS primary:** If supported, all communication between Control Manager and managed products uses HTTPS protocol. If HTTPS is unavailable HTTP is used instead. This is the default setting when installing Control Manager. Select this option if you have mixed agents on your network.
  - **Low - HTTP based:** All communication between Control Manager and managed products uses HTTP protocol. This is the least secure communication method between Control Manager and other products.
5. Select a host address for agents to communicate with Control Manager:

**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:**

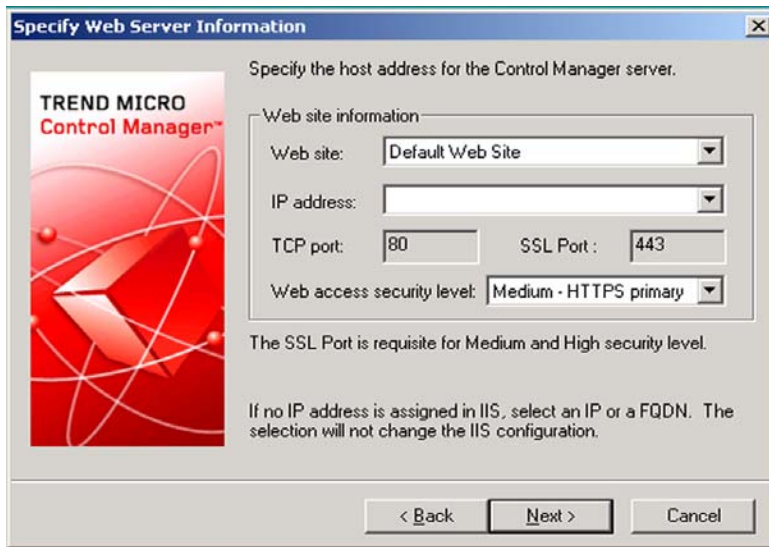
- a. Select **IP address**.
  - b. Type an IP address in the accompanying field. Separate multiple entries using a semi-colon ( ; ).
6. Click **Next**. The Choose Destination Location screen appears.



**FIGURE 3-8. Choose a destination location for backup and authentication files**

7. Specify the location of the Control Manager backup and authentication files (for more information see the *Control Manager 2.5 or 3.0 files that should be backed up* on page 5-4). Click **Browse** to specify an alternate location.

8. 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.



**FIGURE 3-9. Specify Web server information**

9. From the **Web site** list, select the Web site to access Control Manager.
10. 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.

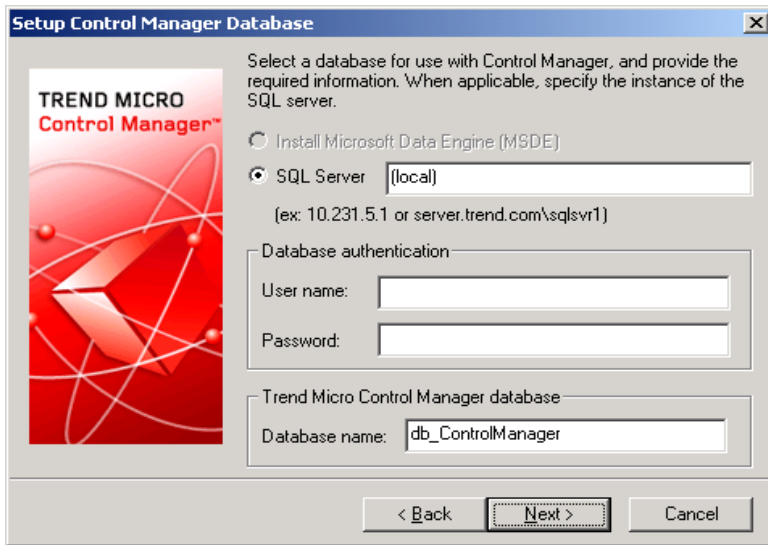
If you use the host name or FQDN to identify your server, make sure that this name can be resolved on the product machines, otherwise the products cannot communicate with the Control Manager server.

11. 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 HTTP is used 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.
12. 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 3: Choose and configure database information

1. Click **Next**. The Setup Control Manager Database screen appears.



**FIGURE 3-10. Choose the Control Manager database**

2. Select a database to use with Control Manager.
  - **Install Microsoft Data Engine (MSDE)** - the setup program automatically selects this option if an SQL server is not installed on this machine. Do not forget to specify a password for this database in the field provided.

---

**Note:** The Microsoft Data Engine (MSDE) is suitable only for a small number of connections. An SQL server is preferable for large Control Manager networks.

---

- **SQL Server** - the setup program automatically selects this option if an SQL server is detected on your 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.*

---

3. Under **Trend Micro Control Manager database**, provide a name for the Control Manager database. The default name is "db\_ControlManager".
4. 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.
  - **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

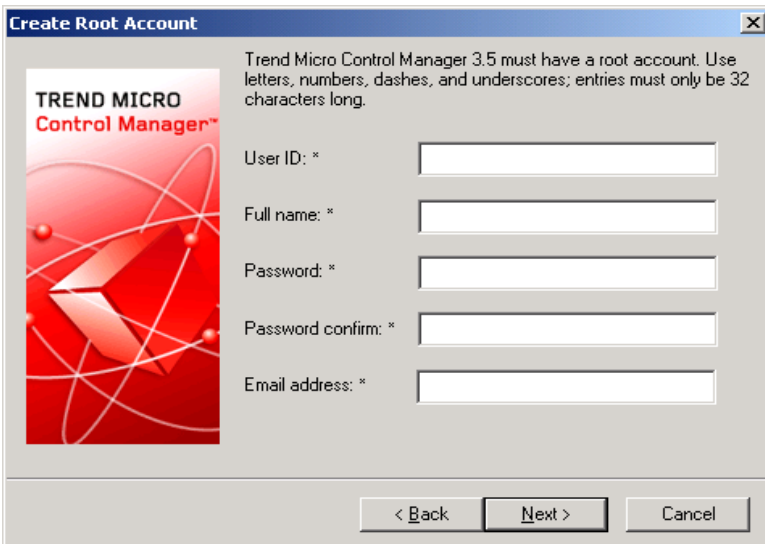
---

**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 4: Set up root account and configure proxy server

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



**Create Root Account**

Trend Micro Control Manager 3.5 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: \*

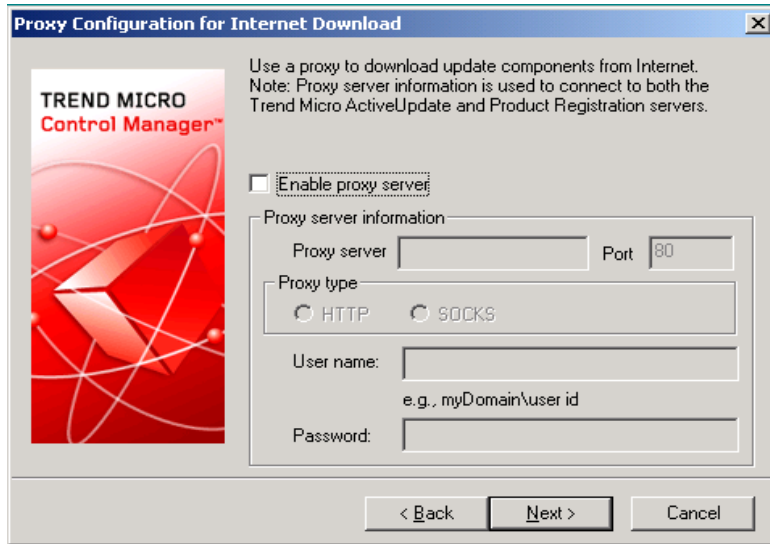
Email address: \*

< Back   Next >   Cancel

**FIGURE 3-11. 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 following screen appears:

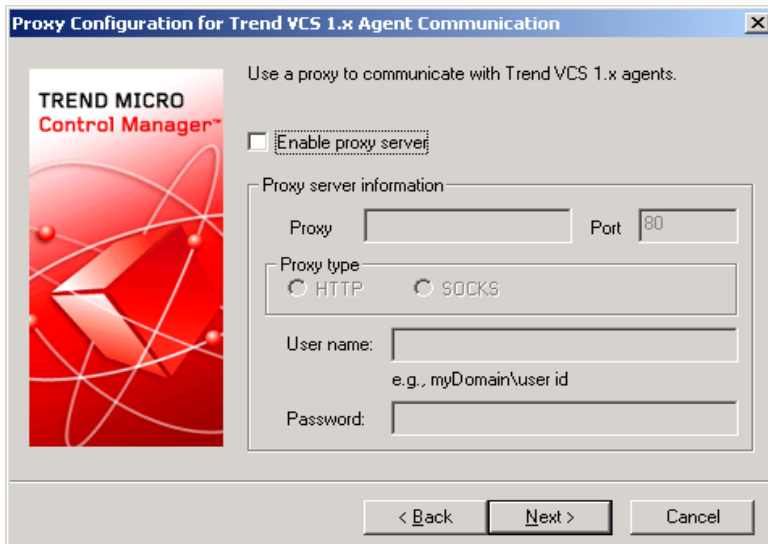


**FIGURE 3-12. Enable proxy server**

If you use a proxy server connect to the Internet, select the **Enable proxy server** check box, and then set the following:

- Proxy server- type the FQDN, IP address, or NetBIOS name of the server
- Port- type the proxy port number
- Proxy type- click the appropriate proxy type: HTTP or SOCKS
- User name- type a logon name that can access the proxy. Provide both the domain name and logon name, for example:  
domain\username
- Password

4. Click **Next**. The system verifies the proxy settings you entered and if correct the proxy configuration screen for Trend VCS agents appears.

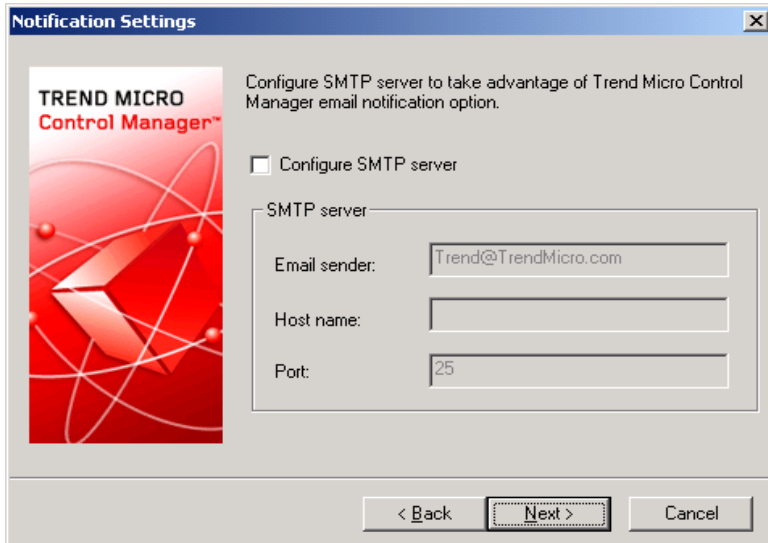


**FIGURE 3-13. Enable proxy server to communicate with Trend VCS 1.x agents**

If you intend to use a proxy server to communicate with these agents, select the **Enable proxy server** check box, and then provide the same set of information you use to connect to the Internet.

## Step 5: Configure notification settings

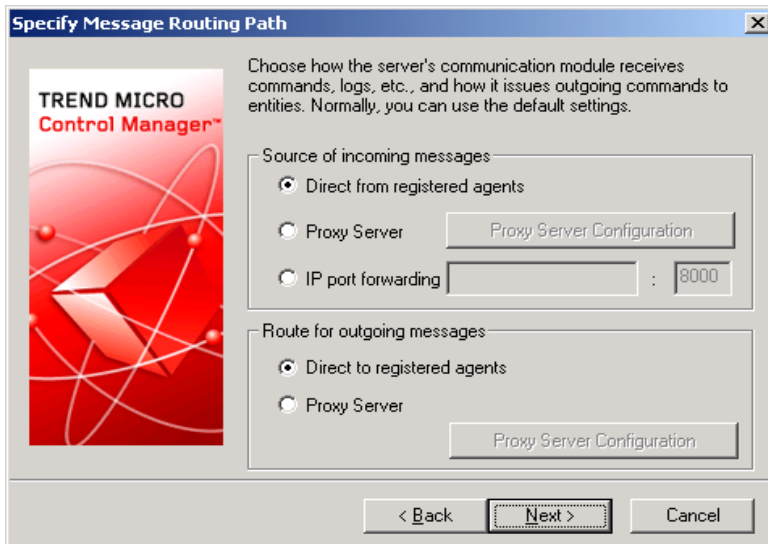
1. Click **Next**. The Notification Settings screen appears.



**FIGURE 3-14. Configure SMTP options**

2. Configure the various settings used for the Control Manager notification functions.
  - **SMTP server:** Allows you to send email notifications via your SMTP server. Provide the SMTP server's FQDN, IP address, or NetBIOS name, and the appropriate port, in the fields provided.
  - **Pager COM Port:** Specify the port used for sending pager alerts.
  - **SNMP Trap Notification:** provide the required Community Name and IP address in the fields provided.

3. Click **Next**. The Specify Message Routing Path screen appears. This screen only appears if the host server does not have TMI installed.



**FIGURE 3-15. 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**

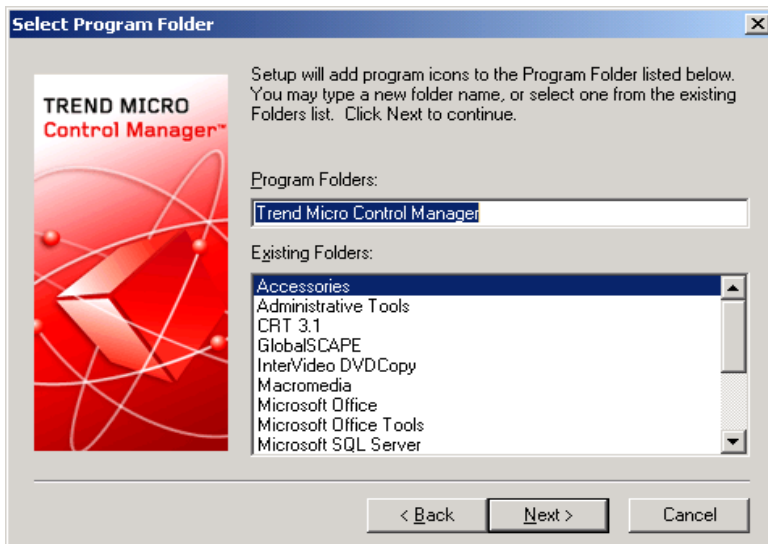
- **Direct from registered agents**- the agents can directly receive incoming messages.
- **Proxy server**- use a proxy server when receiving messages. For additional details about using and configuring proxies, see *Configure Proxy Server Connection for Component Download and Trend VCS Agents* on page 6-38.
- **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 via a proxy server. For additional details about using and configuring proxies, see *Configure Proxy Server Connection for Component Download and Trend VCS Agents* on page 6-38.



5. Click **Next**. The Select Program Folder screen appears.



**FIGURE 3-16.** Select program folder

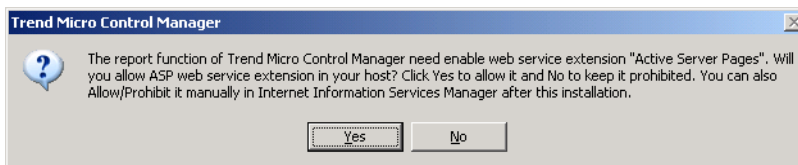
6. Specify the Start menu program folder that will contain the Control Manager shortcut. The default is 'Trend Micro Control Manager'.

---

**Note:** Steps 7 to 10 appear only on Windows 2003 server installations.

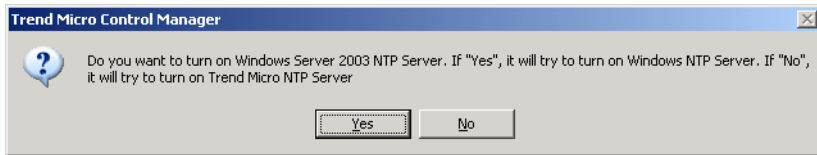
---

7. Click **Next**. The Report Function Confirmation dialog box appears.



8. Click **Yes** to allow ASP Web service extensions to your host. If you click **No**, you cannot generate Crystal reports for Control Manager.

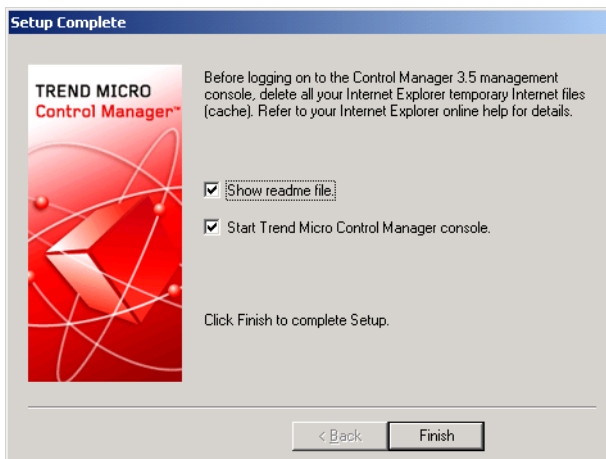
9. Click **Next**. The Choose Time Synchronization dialog box appears.



10. Select one of the following:
  - Click **Yes** if you do not have any Network VirusWall devices installed on your network, but still want the benefits of a Network Time Protocol (NTP) server.
  - Click **No** if you have Network VirusWall devices installed on your network.

The installation begins.

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



**FIGURE 3-17. Setup complete**

## Verifying Successful Installations

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

### Verify a Successful Control Manager Server Installation

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

The three folders exist when you select SQL server. If MSDE is installed, two additional folders MSDE2000 and MSDE2000MSSQL will be created. The following folders appear under the Program Files\Trend Micro directory:

- Common\TMI
- Common\CCGI
- ControlManager

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
- EntityEmulator.exe
- LogRetriever.exe
- CmdProcessor.exe
- UIProcessor.exe
- ReportServer.exe
- NTPD.exe
- DCSPprocessor.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
3. Download the latest components
4. Set notifications

## Register and Activate Control Manager

After you have successfully installed Control Manager, please check the license status and expiration date on the management console, click **Administration > System Settings > License Information**. If the status is not "Activated" or is expired, obtain an Activation Code and activate your software (on the Web console, click **Administration > System Settings > License Information > Activate the product**). If you experience issues with your Activation Code, please contact technical support.

## Configure 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

## Download 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 > System Settings).

## Set Notifications

After installation, configure the events that will trigger notifications to monitor significant virus 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).

## 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 installed 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 are using an evaluation version

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

## Activate 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. Click **Administration** on the main menu.
2. On the left menu under **Registration**, click **License Information**.
3. On the working area under **Control Manager License Information**, click the **Activate the product** link.
4. In the **New** box, type your Activation Code. 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 one.
5. Click **Activate**, and then click **OK**.

## Convert 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.

## Renew Your Product 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.

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. Click **Administration** on the main menu.
2. On the left menu under **Registration**, click **License Information**.
3. On the working area under Control Manager License Information, click **Check Status Online**, and then click **OK**.

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. Click **Administration** on the main menu.
2. On the left menu under **Registration**, click **License Information**.
3. On the working area under **Control Manager License Information**, click the **Activate the product** link.
4. Click the **Specify a new Activation Code** 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**.

# Installing Control Manager Agents

This chapter guides you through installing TVCS and Control Manager 2.x agents. In addition to listing the system requirements for both the Control Manager 2.x agents it also contains post-installation configuration information.

This chapter contains the following topics:

- *System Requirements* on page 4-2
- *Installing Control Manager Agents* on page 4-3
- *Verifying Successful Installations* on page 4-27



## 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.

### Control Manager Agents

MICROSOFT	OTHERS
<ul style="list-style-type: none"> <li>• Windows XP Professional Version</li> <li>• Windows 2000 Server</li> <li>• Windows 2000 Advanced Server</li> <li>• Windows NT 4.0 + SP3</li> <li>• Windows NT 4.0 + SP6a or later</li> <li>• Windows 2003 Standard Edition</li> <li>• Windows 2003 Enterprise Edition</li> </ul>	<ul style="list-style-type: none"> <li>• Novell Desktop 9</li> <li>• AIX</li> <li>• Red Hat Linux 6.2, 7.1, 7.2</li> <li>• RedHat Enterprise Linux 4.3</li> <li>• Turbolinux 6.5, 7.0</li> <li>• SuSE Linux 6.3, 7.2, 7.3</li> <li>• SuSE Enterprise 9.2</li> <li>• AS/400</li> <li>• OS390</li> <li>• Others: GateLock, Linux 6.x kernel, Solaris 2.6, 2.7, 2.8, Debian 3.1 4</li> </ul>

**TABLE 4-1. Control Manager agent supported operating systems**

Please refer to the managed product documentation for detailed agent system requirements. Refer to the following URL to download the latest Control Manager agents:

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

## Installing Control Manager Agents

Control Manager uses agents to manage products on your network. Control Manager uses the following types of agents:

- **Trend VCS agents:** This is an upgraded version of the original Trend VCS agent, specifically designed to be compatible with Control Manager. Older versions of certain Trend Micro products require this agent.
- **Control Manager 2.x agents:** Trend Micro built this agent according to the Control Manager architecture.
- **MCP agents:** Trend Micro Management Communication Protocol (MCP) is Trend Micro's next generation agent for managed products. MCP replaces TMI as the way Control Manager communicates with managed products. For more information on MCP, see [Understanding Trend Micro Management Communication Protocol](#) on page 1-3.

---

**Note:** MCP agents install with their managed products and do not require a separate installation.

---

Trend VCS, Control Manager 2.x agents, and MCP agents essentially perform the same functions. They only differ in the way they communicate with the Control Manager server.

Control Manager can use either an upgraded version of the Trend VCS agent, (version 1.84 or later), a native Control Manager 2.x, or MCP agent.

Control Manager agents receive commands from, and send information to the Control Manager server through an internally developed communications infrastructure called the Communicator. Control Manager only installs one Communicator on each machine, and it's installed along with the agent if Control Manager does not detect an existing Communicator.

If you have installed multiple products on a single machine, the corresponding agents will share a single Communicator.

Trend VCS agents do not utilize this new technology and consequently cannot maximize use of its features, such as improved communication security.

MCP agents install with the product program. There is no separate agent installation with MCP agents. MCP agents offer a number of benefits over Control Manager agents:

- 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
- Cluster node support

For more information on MCP, see *Understanding Trend Micro Management Communication Protocol* on page 1-3.

---

**Note:** Many Trend Micro products released after the fourth quarter of 2003, can install Control Manager agents as an option during product installation. Refer to specific product documentation for agent installation instructions.

---

## Prepare for Control Manager Agent Installation

You need specific information about your product servers before you can install your agents. To help you with this task, print out the provided agent installation checklist to help you record necessary data, see the *Agent Installation Checklist* on page A-4.

Trend Micro recommends installing Control Manager agents during specific product installation.

---

**Note:** You need administrator rights for those target servers to which you want access.

---

To prepare for Control Manager agent installation, Trend Micro recommends gathering the following information:

- The products for which agents will install
- Host name or IP addresses of the product servers
- Administrator or equivalent credentials on the product servers where agents are to be installed

- The User ID of the root account, and of users managing product servers

---

**WARNING!** *Be careful when specifying the User ID above. If you delete the User ID you will have difficulty managing the product.*

---

- The location of the public encryption key of the Control Manager you want to register the agent with. Control Manager agents use this key. See [Public Encryption Key](#) on page 4-7 for instructions on how to obtain a Control Manager public encryption key.

---

**Note:** For non-Windows products, see the Control Manager online Help topic on Planning the Control Manager Deployment > Compatible antivirus and content security products.

---

Refer to the following checklists to collect relevant information:

- For a list of important product-specific information, see [Agent Installation Checklist](#) on page A-4
- For a list of important ports, see [Ports Checklist](#) on page A-3

## Understanding the Control Manager Agent Remote Installation

The Control Manager 3.5 server can support Trend Virus Control System 1.8x, Control Manager 2.5x agents, and MCP agents. MCP agents install with the managed product.

There are two agent remote installation programs:

- RemoteInstall.exe
- CMagentSetup.exe

### RemoteInstall.exe

The `remoteinstall.exe` file is an agent installation tool introduced in Control Manager 2.5 and it serves the following purposes:

- To install agents to supported product servers

- To upload agent packages to Control Manager servers

This tool differs from the original `CMAgentSetup.exe` program in that it contains no actual agents. Instead, the tool identifies agent packages stored on target Control Manager servers, and then the setup programs in the agent packages themselves perform the installation.

After a fresh Control Manager installation, Control Manager servers do not contain agent packages — either the antivirus or content security product uploads and stores their agents on the server before you can install these agents.

---

**Note:** Trend Micro recommends remote installation as the method for deploying agents on large numbers of product servers, so that an administrator can install agents without being physically at the target server.

---

### **`CMAgentSetup.exe`**

A similar program in Trend Virus Control System 1.x serves as the basis of this agent installation program. This file has all agents needed for the corresponding products.

Use the `CMAgentSetup.exe` to install Trend VCS 1.86 agents for all Trend Micro antivirus products and Control Manager agent for InterScan Messaging Security Suite 5.1 (InterScan Messaging Security Suite 5.15 or higher uses the `RemoteInstall.exe` tool).

## **Performing the Installation**

Most products released after the 4th quarter of 2003 can install Control Manager agents as part of the product installation (ScanMail for Lotus Notes versions 2.5x use Trend VCS agents). However you may still need to install agents from Control Manager in the following instances:

- Migration of products managed by Trend VCS to Control Manager
- Centralized implementation of a Control Manager network

Agent installation is performed in three steps:

- Step One: Obtain required files
- Step Two: Obtain agent packages (Optional)

- Step Three: Install the agents

## Step One: Obtain Required Files

The following are required for agent installation:

- One of the following agent installation programs:
  - Installation program for Control Manager agents
  - Installation program for Trend VCS agents and the Control Manager agent for InterScan Messaging Security Suite 5.1
- Public encryption key

### Agent Installation Programs

The agent installation programs allow you to install agents from a single location.

#### To obtain the setup program:

1. Click **Products** on the menu.
2. Click **Add/Remove Product Agents** on the left menu.
3. On the Add/Remove Product Agents screen, click the appropriate **Use this**. For Control Manager agents, you should use the `RemoteInstall.exe` program. For Trend VCS agents and the Control Manager agent for InterScan Messaging Security Suite 5.1, use the `CMAgentSetup.exe` program
4. At the File Download screen, select **Save** this program to disk, and then click **OK**.
5. At the Save As screen, select a location for the program, and then click **Save**.

### Public Encryption Key

Control Manager agents use the encryption key to identify the Control Manager server that it registers with. The key is required during agent installation.

#### To obtain the key:

1. Click **Products** on the menu.
2. Click **Add/Remove Product Agents** on the left menu.

3. Right-click **Public encryption key**, and then click **Save Target As**. Save the `E2EPublic.dat` file to a location that the agent installation program can access.

## Step Two: Obtain Agent Packages (Optional)

This step is optional, and is only required if a Control Manager server does not have the required agent packages. The Control Manager Remote Agent setup program is required for this step.

### To obtain agent packages:

1. Using Windows Explorer, run `RemoteInstall.exe`. The Trend Micro Control Manager Agent Setup program runs.

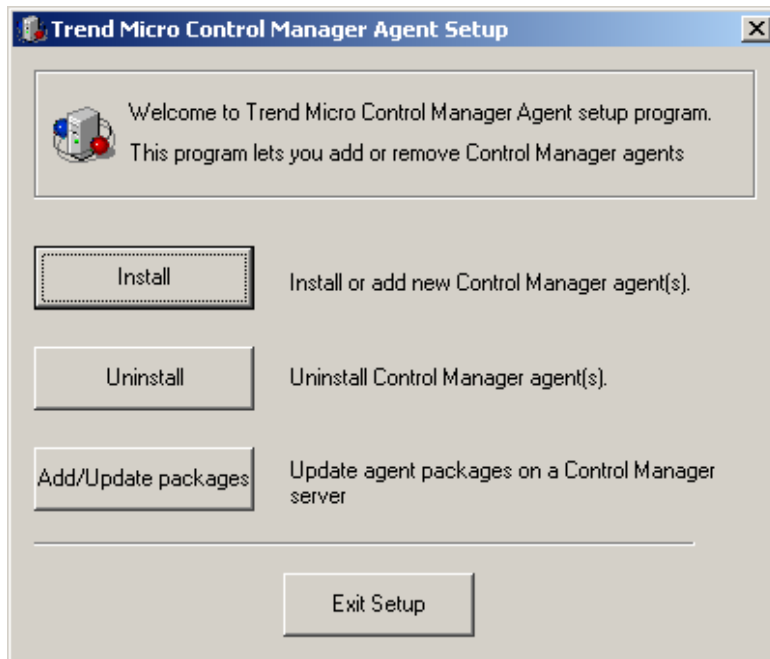
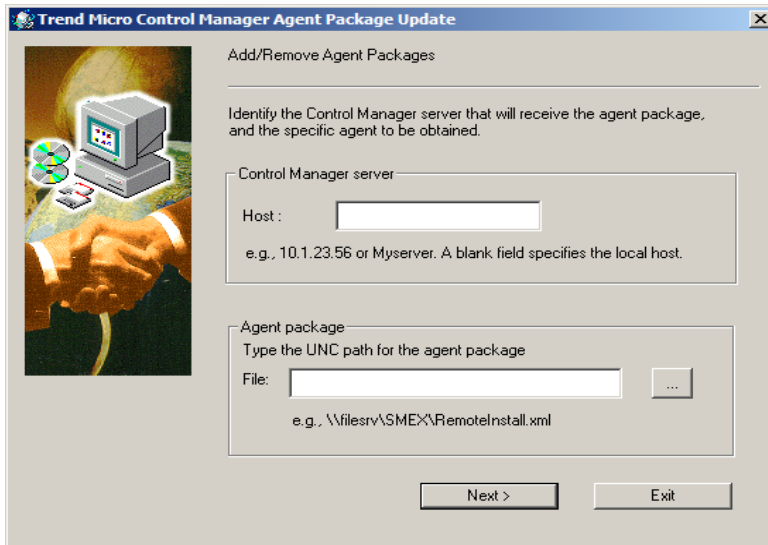


FIGURE 4-1. Control Manager Agent Setup screen



2. On the Control Manager Agent Setup screen, click **Add/Update packages**. The Trend Micro Control Manager Agent Package Update screen appears.

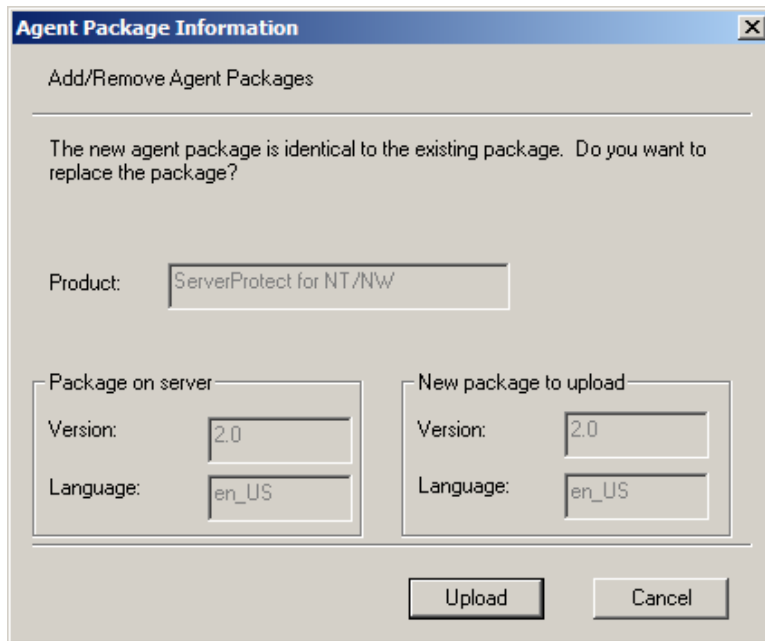


**FIGURE 4-2. Identify the Control Manager server and the agent**

3. Under **Control Manager server**, type the IP address or host name, of the Control Manager server to be updated, in the Host field.
4. Under **Agent package**, type the UNC path of the agent package (RemoteInstall.xml) in the **File** field.

Alternatively, click the browse button, locate the package, and then click **Open**.

5. Click **Next**. The Agent Package Information screen appears.



**FIGURE 4-3. Agent package information**

6. On the Agent Package Information screen, verify the agent package version. Compare the package to be uploaded with the package currently on the Control Manager server. To continue with the upload, click **Upload**.
7. After completing the upload, click **OK**.
8. At the subsequent window, click **Yes** to upload another package, or **No** close the application.

## Step Three: Install the Agents

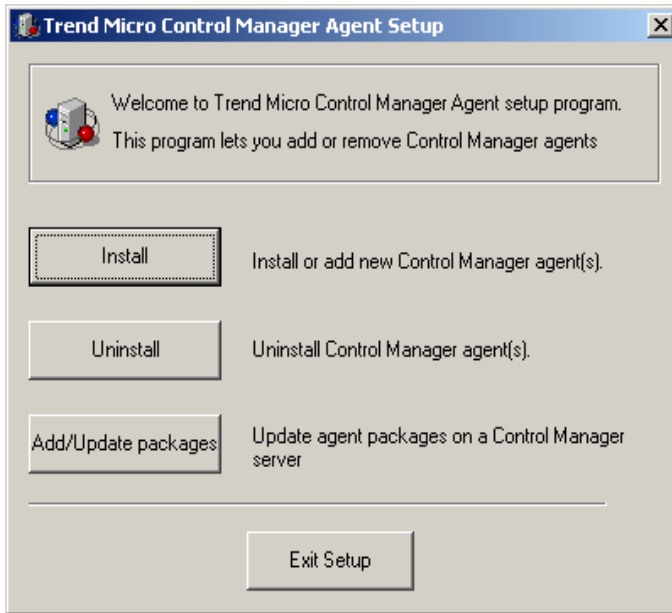
Many Trend Micro products released after the fourth quarter of 2003 can install Control Manager agents during installation. However, you can still deploy agents remotely from the Control Manager server with the required agent packages. For older versions of Trend Micro products, Control Manager can use an upgraded version of the original Trend Virus Control System agent.

### Installing Control Manager Agents With the Remote Agent Setup Tool

Use the Remote Agent Setup tool to deploy Control Manager agents from a central location.

#### To install Control Manager agents:

1. Open the folder where you saved the Remote agent setup tool.
2. Double-click the `RemoteInstall.exe` file.



**FIGURE 4-4. Control Manager Remote Agent Setup**

3. Click **Install**.
4. At the Welcome screen click **Next**. The License Agreement screen appears.

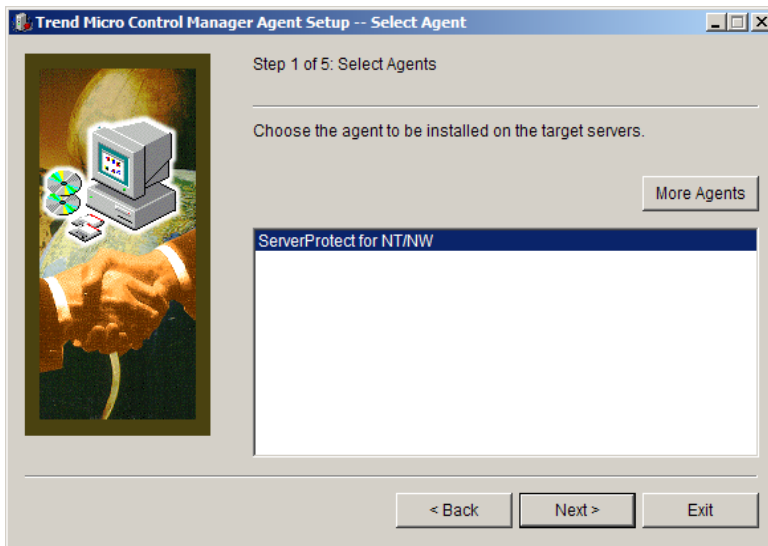
Read the agreement carefully. If you do not agree with the terms of the license, click **No**; the installation will discontinue. Otherwise, click **Yes**. The Control Manager source logon screen appears.



**FIGURE 4-5. Log on to the Control Manager source server**

5. Specify, and provide Administrator-level logon credentials for the Control Manager server that contains the agent package. Type the following information:
  - **Host name**
  - **User name**
  - **Password**

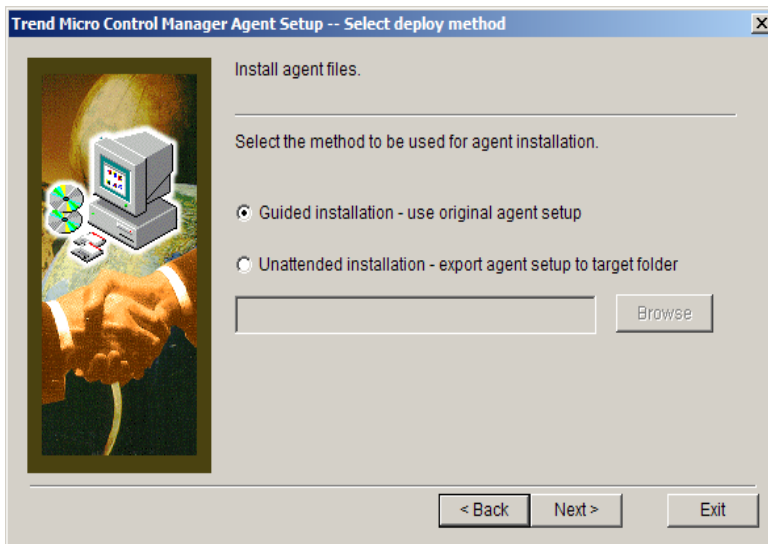
6. Click **Next**. The Select Agent screen appears.



**FIGURE 4-6.** Choose the agent to install on the target server

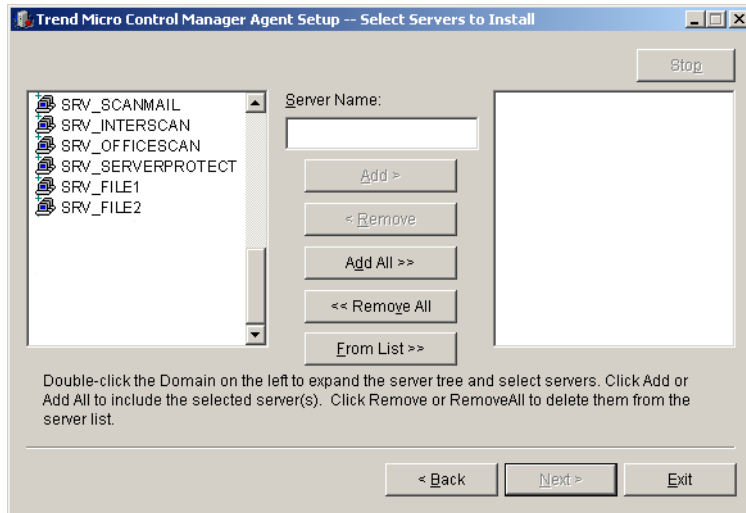
7. Select the agent to install. If the required agent is not on the Control Manager server, either select another server, or click **More Agents** to obtain the necessary agent package.  
For instructions on how to obtain agent packages, see *Step Two: Obtain Agent Packages (Optional)* on page 4-9

8. Click **Next**. The Select Agent Setup Method screen appears.



**FIGURE 4-7.** Select the agent installation method

9. The At the Select Servers to Install screen, select the servers on which to install the agents.



**FIGURE 4-8. Select servers to install**

There are three ways to do this:

**To select from the list:**

- a. At the left list box double click the domain where the antivirus servers are located — this will expand to show all servers in the domain.
- 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 install agents on all servers in the selected domain. Alternatively, you can double-click on a server to add it to the list on the right side.

**To type 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 use a migration list:**

- a. Click **From list**.
- b. At the Open screen, locate the migration list, and then click **Open**.
- c. At the Select Servers to Install screen, the servers in the migration list are added to the right list.

---

**Note:** The Agent Migration tool generates the migration list. For additional information about this list, see *Cascading Management Structure Tool (CasTool.exe)* starting on page 7-2.

---

To remove servers from the list, select a server from the right-hand list box, and then click **Remove**. To remove all servers, click **Remove All**.

10. Click **Next** to continue.
11. At the Log onto the server screen, provide Administrator-level logon credentials for the selected servers. Type an Administrator-level user name and password, for the servers selected previously, in the appropriate fields.  
By default, agents are installed relative to the root-level share (C\$). To specify another drive or folder, click the ellipsis button (. . .).

You can re-use the logon credentials you used for the different servers by selecting the **Retain user name password after logging on?** check box. This eliminates the need to re-type the user name and password on each server. The installation program tries each credential on the list, if none of the existing ones can access the server, you will be prompted for another set of credentials.

12. Click **Log on**.

---

**Note:** Server analysis determines if the agent you are installing is appropriate for the products installed on the server.

---

13. Click **OK** at the dialog window that opens.
14. At the Analyze Selected Servers screen, click **Next**.
15. At the Installation List screen, click **Next**.

- 16.** At the Setup Control Manager Agent screen, type a User ID in the **User ID** field. This determines how the product, hereinafter referred to as entity, appears in the Product Directory.

---

**Note:** Be careful when specifying the User ID above. If the User ID used here is deleted, either deliberately or accidentally, you will encounter difficulties managing the agent. Trend Micro recommends using the Root account in the User ID field when installing agents.

---

- 17.** Click **Next**.

- 18.** At the Message Routing Path Configuration screen, configure how incoming and outgoing messages are routed.

---

**Note:** If a Communicator is already installed on your server, the agent will use the existing Communicator, and steps 16 and 17 will be skipped.

---

**To set the path for incoming messages:**

Under the Source of incoming message, select one of the following options:

- **Any host** - accept messages from any source
- **Firewall** - type the firewall's IP address and the port number, that has been opened for Control Manager communication, in the fields provided
- **Proxy server** - select this to use a proxy

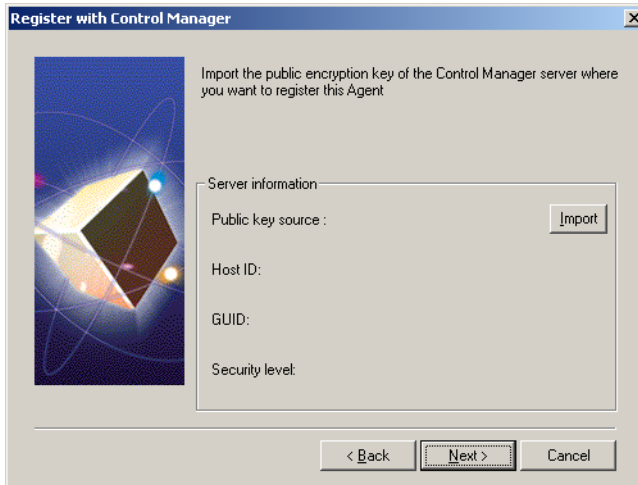
**To set the path for outgoing messages:**

Under Outgoing messages, select one of the following options:

- **Direct to server**
- **Proxy server**

Click **Next**.

19. At the Register with Control Manager screen, click **Import**, locate the encryption key (E2EPublic.dat) of the Control Manager server with which you are registering the agent, and click **Open**. Click **Next** to continue.



**FIGURE 4-9. Encryption key selection screen**

At the Installing Agents screen, monitor the status of the installation.

20. Click **OK**.
21. Click **Exit** to end the setup, or **Next** to install agents for other applications.  
If you clicked **Next**, click **Yes** in the screen that appears.
22. Click **Finish** at the final screen.

### Installing Trend VCS agents

The Trend VCS agent allows you to migrate existing Trend VCS network to your Control Manager server and to manage older version of Trend Micro products that are not compatible with Control Manager agents.

**To install the Trend VCS agent:**

1. Using Windows Explorer, go to the location where you saved the agent setup program.
2. Double-click `CMAgentSetup.exe`.
3. Click **Install** to begin installation. The Software License Agreement appears. Read the agreement carefully. If you do not agree with the terms of the license, click **No**; the installation will discontinue. Otherwise, click **Yes**.
4. On the agent Installation screen, click **Next**. A list of products appears.
5. Select the products for which you want to install agents. Click **Next** to continue. The Select Servers to Install screen appears.

---

**Note:** If you selected the Trend VCS agent for OfficeScan Corporate Edition, proceed to the following online Help topic: Installing Trend Micro Control Manager for the First Time > Trend VCS Agent Installation: OfficeScan Corporate Edition.

---

6. Select the servers where the agents are to be installed. There are two ways to do this: by selecting from a list, or by entering the server name.

**To select from the list:**

- a. At the left list box, double-click the domain where the antivirus servers are located — this will expand to show all servers in the domain.
- b. Select the target server from the left list box, and then click **Add**. The chosen server appears in the right list box. Click **Add All** to add agents to all servers in the selected domain. Alternatively, you can double-click on a server to add it to the right list.

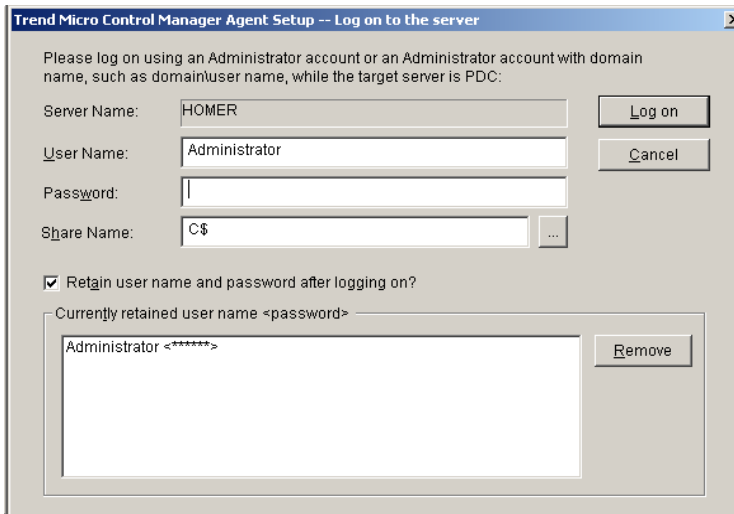
**To enter a server name directly:**

- a. Type the server's host name or IP address in the Server name field.
- b. Click **Add**. The server appears in the right list box.

To remove a server from the list, select the server from the right list box, and then click **Remove**. To remove all servers, click **Remove All**.

7. Click **Next** to continue.

- At the Server Analysis screen, provide Administrator-level logon credentials for the selected servers. Type an Administrator-level user name and password - for the servers selected previously - in the appropriate fields.



**FIGURE 4-10. Logon credentials screen for agent installation**

By default, agents are installed relative to the root-level share (C\$). To specify another drive or folder, click the ellipsis button (. . .).

You can re-use the logon credentials you use for the different servers by selecting the **Retain user name and password after logging on?** check box on this screen. This eliminates the need to re-type your user name and password on each server. The installation program tries each credential on the list. If none of the existing ones can access the server, you will be prompted for another name and password.

---

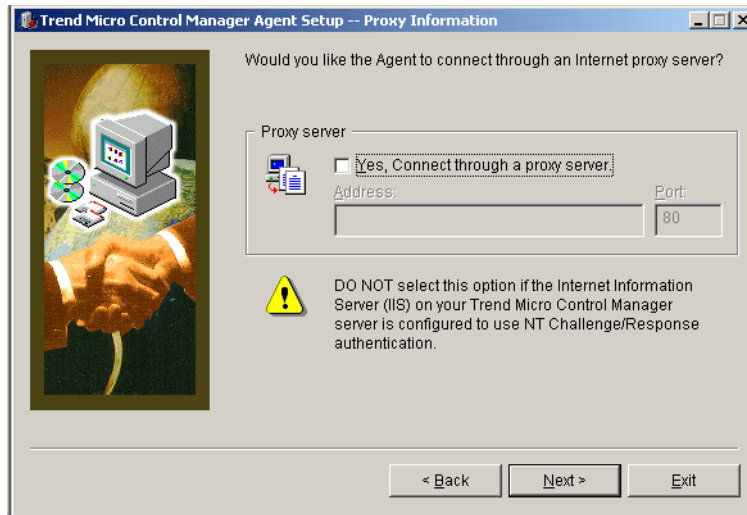
**Note:** Server analysis determines if the agent you are installing is appropriate for the product(s) installed on the server.

---

- Click **OK** in the dialog box that opens after server analysis is completed. The Installation List screen appears.

The table on the screen provides the following details about the target servers: Server name, operating system, IP address, domain, and the agent's product.

10. Click **Next** to start the agent installation. The Proxy Information screen opens.
11. If you intend to use a proxy for Server-Entity communication, select the **Yes, connect through a proxy server** check box.



**FIGURE 4-11.** Trend VCS agent proxy screen

Provide the address of the proxy server used by your Control Manager server you can use the IP address, or Fully Qualified Domain Name (FQDN) - if the agent's DNS server can resolve the FQDN. Click **Next** to continue.

---

**WARNING!** *Do not select this option if the Internet Information Server on your Control Manager server is configured to use NT Challenge/Response authentication.*

---

12. At the Control Manager Server Information screen, type the following information in the appropriate fields:

- *Host name (or IP Address)* - the host name or IP address of your Control Manager server
- *TCP Port* - the port used by the WWW service of your Microsoft Internet Information Server

13. On the Agent Information screen, provide the following data:

- For *Site*, type a site name for the agents. Try to give a name that reflects the agent's actual location (for example, New\_York, Tokyo, or Manila).
- For *Relative destination directory*, give the directory for storing the Trend VCS agent files relative to the shared path you specified earlier.

At the Installing Agents screen, a table shows the installation status of the agents.

14. After the installation, click **OK**, then click **Exit** to end the setup, or **Next** to install agents for other applications.
15. If you clicked **Next**, a dialog box opens. Click **Yes** to install other agents, otherwise, click **No**.
16. Click **Finish**.

## Installing Control Manager agent for InterScan Messaging Security Suite 5.1 for Windows

The InterScan Messaging Security Suite (IMSS) 5.1 for Windows agent comes in the same installation package that contains the Trend VCS agents.



**FIGURE 4-12.** Select Antivirus Product screen; note inclusion of IMSS in the selection

To install this agent, see *Installing Trend VCS agents* on page 4-20, and follow the procedure until step 10. Afterwards, see *Installing Control Manager Agents With the Remote Agent Setup Tool* on page 4-12, and use the procedure starting on step 14.

## Install the Control Manager agent for NetScreen™ Firewall

Obtain the following information before starting the installation:

- IP address of the computer where NetScreen-Global PRO is installed
- Port number used for communicating with Global PRO
- Administrator user name and password for the selected Global PRO Arbitrator
- A valid Certificate Name for the selected Global PRO Arbitrator



The following procedure assumes that you use an existing Arbitrator when logging onto Global PRO.

**To determine the Certificate Name of a Global PRO Arbitrator:**

- a. On the NetScreen Policy Manager logon screen, select an **Arbitrator** used for Global PRO communication. Choose an Arbitrator that uses SSL.
  - b. Click **Edit**.
  - c. Copy the **16-digit certificate number** at the Cert. Name field.
- Location of the Control Manager server public encryption key (E2EPublic.dat)

**To install the agent:**

1. On the **Start** menu, click **Run**, and then go to the NetScreen agent installation program (Setup.exe). If you are installing from the Trend Micro Enterprise Security CD, go to the NetScreen agent folder on the CD.
2. On the Welcome screen, click **Next** to start the installation. The Software License Agreement screen follows.
3. Read the agreement carefully. If you do not agree with the terms of the license, click **No**; the installation will discontinue. Otherwise, click **Yes**.
4. Specify the **location** where you want to copy agent files. By default, the agent installation copies files in the following location: C:\Program Files\TrendMicro\NetScreen. If you want to change this location, click **Browse**, and then specify an alternate location.
5. Click **Next Register** the agent with the Control Manager.
6. Click **Browse** to locate the public encryption key of the Control Manager server and then click **Next**.
7. Identify the NetScreen-Global PRO installation that the agent will manage. Provide the following information and then click **Next**:
  - IP address of the Global PRO machine
  - Port number used for communicating with Global PRO
  - Administrator-level user name
  - Password
  - Certificate name for the Arbitrator (this is a 16-digit number)

8. Provide the following:
    - A managed product name that will identify the NetScreen Firewall product in the Product Directory
    - A permanent user account on the Control Manager server
- 

**Note:** Specify a permanent User ID on the Control Manager server. Should you later delete this account, you will have trouble managing the product.

Trend Micro recommends using the Control Manager superuser account.

---

9. On the Setup Complete screen, click **Finish** to complete the installation.

## Verifying Successful Installations

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

### Verify a Successful Agent Installation

To verify a successful agent installation, check the Control Manager management console to see that the product has successfully registered with Control Manager and the management console lists it as a managed product.

**To verify a successful agent installation:**

1. Click **Products** on the main menu.
2. On the left menu select **Managed Products**, and click **Go**. Under product directory, the managed product for the agent you installed appears.

**If you do not see your managed product, try the following:**

1. Click the icon in the upper right corner of the left menu to refresh the Product Directory.
2. Confirm the connection to the managed product is functioning correctly.
3. Restart the Trend Micro Management Infrastructure service on the product side.
4. Reinstall the agent package.

## Configure MCP for Two-way Communication

MCP agents communicate with Control Manager using one-way communication by default. You can manually configure the agent to communicate with Control Manager using two-way communication. For more information on one-way and two-way communication, see *One-way and Two-way Communication Support* on page 1-6.

### To configure MCP for two-way communication on a Windows environment:

1. Create a folder on the server hosting the MCP agent. For example:

```
cgi-bin
```

2. Put the following files in the folder you created.

- `cgiCmdNotify.exe`
- `libapr-1.dll`
- `libcurl.dll`
- `TrendAprWrapperDll.dll`

3. In the `Product.ini` file, configure the following settings:

- **Port= 80**  
This value represents the Web server's port number.
- **VirtualPath= /cgi-bin/cgiCmdNotify.exe**  
This value is the related file path for `cgiCmdNotify.exe`.
- **ComputerName=** IP address or host name of the host server

---

**Tip:** Trend Micro recommends using the host server's IP address.

---

4. In the `Agent.ini` file configure the following:

- **CGI\_Path= C:\Inetpub\wwwroot\cgi-bin**  
This value is the full file path to `cgiCmdNotify.exe`.
- If you use an HTTPS connection, in the Network section of the file configure the following
  - **TMCM\_Certificate=** leave the space blank, type `./cert.pem`, or get the value from the Control Manager server
  - **SSL\_Enable= 1**

**To configure MCP for two-way communication on a Linux environment:**

1. Create a folder on the server hosting the MCP agent. For example:  
cgi-bin
2. Put the following file in the folder you created.
  - `cgiCmdNotify.exe`
3. In the Product.ini file, configure the following settings:
  - **Port= 80**  
This value represents the Web server's port number.
  - **VirtualPath= /cgi-bin/cgiCmdNotify.exe**  
This value is the related file path for `cgiCmdNotify.exe`.
  - **ComputerName=** IP address or host name of the host server

---

**Tip:** Trend Micro recommends using the host server's IP address.

---

4. In the Agent.ini file configure the following:
  - **CGI\_Path= var\www\cgi-bin**  
This value is the full file path to `cgiCmdNotify.exe`.
  - If you use an HTTPS connection, in the Network section of the file configure the following
    - **TMCN\_Certificate=** leave the space blank, type `./cert.pem`, or get the value from the Control Manager server
    - **SSL\_Enable= 1**

## Verify 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 TCMC 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..."

A "1" signifies that the agent uses one-way communication to communicate with Control Manager.

A "2" signifies that the agent uses two-way communication to communicate with Control Manager.

# Upgrading Servers or Migrating Agents to Control Manager 3.5

Upgrading existing Trend Virus Control 1.8x or Control Manager 2.5x or 3.0 servers to Control Manager 3.5 requires careful consideration and detailed planning. Likewise, the same is true when migrating Trend VCS or Control Manager agents to a Control Manager 3.5 server.

This chapter discusses the following topics:

- *Upgrading to Control Manager 3.5* on page 5-2
- *Planning Trend VCS or Control Manager Agent Migration* on page 5-8
- *Migrate the Control Manager Database* on page 5-15

## Upgrading to Control Manager 3.5

The following table lists the considerations when upgrading to the Standard or Enterprise edition:

CAPABILITY	STANDARD EDITION	ENTERPRISE EDITION
Upgrade Control Manager 2.x or 3.0 servers	Yes	Yes
Retain the reporting functions	No	Yes
Upgrade Trend VCS 1.x servers	Yes	Yes
Upgrade a Standard edition to Enterprise edition  To upgrade from a Standard Edition to an Enterprise Edition, obtain an Enterprise Edition Activation Code (AC), and then reinstall Control Manager (only reinstall: do not uninstall and then reinstall). During installation, enter the new Enterprise Edition AC.	Yes	N/a
Convert Enterprise edition to Standard edition	N/a	No

**TABLE 5-1. Considerations when upgrading to Control Manager 3.5**

Trend Micro recommends that you install Control Manager 3.5 on a separate server, rather than upgrading Trend VCS 1.x or Control Manager 2.5 or 3.0 to version 3.5. This way, the original server remains intact, allowing you to de-commission the original server in a timely and effective manner.

## Upgrade Trend VCS 1.8x Servers

Consider the following points when upgrading from Trend VCS to Control Manager 3.5 server:

- The Control Manager 3.5 installation detects an existing copy of the Trend Virus Control System, and gives you the option to upgrade it to Control Manager
- Upgrading your Trend VCS system to Control Manager automatically upgrades the Trend VCS agents on your system to Trend VCS agent version 1.86
- Upgrading your Trend VCS system to Control Manager disables Trend VCS files and Registry settings, that is, the upgrade will not remove Trend VCS components

This occurs if you install Control Manager on a Trend VCS machine. If removing Trend VCS after installing Control Manager, the Trend VCS removal routine will modify the Internet Information Server (IIS) settings in such a way that will disable Control Manager. To fix this, run SetupPatch.exe (see *IIS Restoration Tool (SetupPatch.exe)* on page 7-5).

Refer to *Planning Trend VCS or Control Manager Agent Migration* on page 5-8 for details on how to migrate Trend VCS 1.8x agents.

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

## Upgrade Control Manager 2.5 or 3.0 Servers

Consider the following points when upgrading from Control Manager 2.5 or 3.0 to version 3.5 servers:

- Control Manager now separates viruses and spyware/grayware items in old logs. Converting old logs to the new format can significantly extend the time required to install Control Manager.
- The Control Manager 3.5 installation detects an existing copy of Control Manager 2.5 or 3.0, and gives you the option to upgrade it to the latest Control Manager version.



---

**Note:** Trend Micro recommends installing Control Manager 3.5 on a separate server, rather than upgrading from version 2.5 to 3.0. This way, the original Control Manager 2.5 or 3.0 server remains intact, allowing you to de-commission the original server in a timely and effective manner.

---

- Before running the Control Manager 3.5 setup program, back up the following Control Manager 2.5 or 3.0 information, files and registry hives to be able to save your original settings and roll back to version 2.5 or 3.0:

CONTROL MANAGER 2.5 OR 3.0 INFORMATION	LOCATION
Authentication information  (ensures that managed products reporting the Control Manager server will report to the same server if Control Manager is restored)	\Program Files\Trend Micro\CmKeyBackup\*.*
Database	Use the SQL Enterprise Manager or osql to backup the Control Manager database. Refer to the Control Manager <i>Back up db_ControlManager using SQL Enterprise Manager / osql</i> online help topics for detailed steps.
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

**TABLE 5-2. Control Manager 2.5 or 3.0 files that should be backed up**

<b>CONTROL MANAGER 2.5 OR 3.0 INFORMATION</b>	<b>LOCATION</b>
Serial number information	Cfg_dm_tms_sn value in \Program files\Trend Micro\COMMON\TMI\TMI.cfg
GUID information	GUID value in \Program files\Trend Micro\COMMON\TMI\TMI.cfg
Hot fix list	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TVCS\hotfix
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 5-2. Control Manager 2.5 or 3.0 files that should be backed up**

CONTROL MANAGER 2.5 OR 3.0 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\TMC
	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\TMC
	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

**TABLE 5-2. Control Manager 2.5 or 3.0 files that should be backed up**

## Roll Back to Trend VCS 1.8x Server

In the unlikely event of an unsuccessful upgrade to Control Manager 3.5, you can roll back to your original Trend VCS system.

**To roll back to Trend VCS 1.8x:**

1. Remove Control Manager (Optional).

You can skip this step if you still want to retain Control Manager on your system. If you remove Control Manager later, then you must run SetupPatch.exe after removing it to retain Trend VCS functionality. Refer to Removing the Control Manager server for instructions.

2. Run SetupPatch.exe.

## Roll Back to Control Manager 2.5 or 3.0 Server

If upgrading to Control Manager 3.5 is unsuccessful, perform the following steps to roll back to your Control Manager 2.5 or 3.0 system.

---

**Note:** When removing Control Manager 3.5 using the Control Manager uninstallation shortcut, select the keep database option when prompted.

---

**To roll back to Control Manager 2.5 or 3.0:**

1. Collect all Control Manager 2.5 or 3.0 backup files (refer to Table 5-2, “Control Manager 2.5 or 3.0 files that should be backed up,” on page 5-4).
2. Remove Control Manager 3.5 using the Control Manager uninstallation shortcut or the Windows Add/Remove Programs feature.
3. Install Control Manager 2.5 or 3.0. Refer to Control Manager 2.5 or 3.0 Getting Started Guide for instructions.
  - Use the backup authentication information
  - Select **Append new records to existing database** option and specify where the backup Control Manager database is located

---

**Note:** Installing Control Manager 2.5 or 3.0 generates a new public key. Setting the security level too high makes Control Manager agents registered to the original Control Manager 2.5 or 3.0 server re-import the public key to register to the new Control Manager server. With a new public key available, agents cannot match the original public key to the new one, so the agents cannot register to the Control Manager server. To restore the original settings, reinstall all agents to re-register to the new Control Manager 2.5 or 3.0 server.

---

4. Copy and replace the Control Manager files with the Control Manager 2.5 or 3.0 backup files (refer to Table 5-2, “Control Manager 2.5 or 3.0 files that should be backed up,” on page 5-4).
5. Apply Control Manager 2.5 or 3.0 service pack and hot fixes.

## Planning Trend VCS or Control Manager Agent Migration

There are two ways to migrate Trend VCS and Control manager 2.5x agents to Control Manager 3.5 server:

- **Rapid upgrade**

Rapid upgrade works using the following approach::

ORIGINAL SERVER/AGENT	ACTION
<b>Trend VCS 1.8x with Trend VCS 1.8x agents</b>	Upgrades Trend VCS 1.8x agents to Trend VCS 1.86; Trend VCS agents maintain their original folder structure under the <b>Trend VCS agents</b> folder in the Product Directory
<b>Control Manager 2.5 or 3.0 with Control Manager 2.5x agents</b>	Registers Control Manager 2.5x agents to Control Manager 3.5 server; Control Manager agents maintain their original Product Directory structure
<b>Control Manager 2.5 or 3.0 with mixed agents</b>	<p><b>Trend VCS agents:</b> Upgrades Trend VCS 1.8x agents to Trend VCS 1.86; Trend VCS agents maintain their original folder structure under the <b>Trend VCS agents</b> folder in the Product Directory</p> <p><b>Control Manager agents:</b> Registers Control Manager 2.5x agents to Control Manager 3.5 server; Control Manager agents maintain their original Product Directory structure</p>
<b>Control Manager 3.5 with MCP agents</b>	Registers MCP to Control Manager 3.5 server; MCP maintain their original Product Directory structure

TABLE 5-3. Rapid Upgrade

ORIGINAL SERVER/AGENT	ACTION
<p><b>Control Manager 3.5 with mixed agents</b></p>	<p>Trend VCS agents:                      Upgrades Trend VCS 1.8x agents to Trend VCS 1.86; Trend VCS agents maintain their original folder structure under the Trend VCS agents folder in the Product Directory</p> <p>Control Manager agents:                      Registers Control Manager 2.5x agents to Control Manager 3.5 server; Control Manager agents maintain their original Product Directory structure</p> <p>MCP                      Registers MCP to Control Manager 3.5 server; MCP maintain their original Product Directory structure</p>

**TABLE 5-3. Rapid Upgrade**

Trend Micro recommends rapid upgrade for migrating agents in a laboratory setting or in relatively small networks, preferably during test deployments (see *Test Control Manager Deployment at One Location* on page 2-16). However, since you cannot stop the migration once it starts, this method works best for smaller deployments, and the degree of difficulty increases with the size of the network.

- **Phased upgrade**

Trend Micro recommends a phased upgrade for large, single-server Trend VCS 1.8x or Control Manager 2.5x networks; and is essential for multiple-server networks. It 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 3.5 on a server that does not have any previous Trend VCS or Control Manager version installed (preferably without any managed products).
- b. Run the AgentMigrateTool.exe tool on the Trend VCS 1.8x or Control Manager 2.5 server.

You can now consolidate all Trend VCS agents that were originally separated for functional control purposes, as well as Control Manager 2.5 agents, under a single Control Manager 3.5 server. This is practical because Control Manager supports multiple user accounts. To do this, use the phased upgrade procedure described above on all the Trend VCS servers that have to be merged, and migrate their products to a common Control Manager server.

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

## Migration Scenarios Trend VCS 1.8x or Control Manager 2.5x Agents

The following agent migration scenarios are possible:

- Single-server migration

You can use both Rapid and Phased migration in this instance. See *Upgrading to Control Manager 3.5* on page 5-2. Trend Micro recommends using Phased migration for large Trend VCS networks.

- Consolidation of different servers/agents

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

### Trend VCS 1.8x Agent Migration Flow

During Trend VCS 1.8x agent migration, the agent migration tool performs the following:

- Upgrades Trend VCS 1.8x agents to version 1.86
- Removes Trend VCS 1.8x server information from the registry and replaces them with Control Manager 3.5 server information
- Unregisters from the Trend VCS server and registers to the Control Manager 3.5 server

In an event when AgentMigrationTool.exe is unable to complete or finish the Trend VCS 1.8x agent migration, it removes Trend VCS agents from the Control Manager 3.5 server and re-registers them back to the Trend VCS server.

### Control Manager 2.5x Agent Migration Flow

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

- Stops the Trend Micro Infrastructure service
- Obtains the Product Directory information from the Control Manager source server
- Removes the agent information from the Control Manager source database and TMI.cfg



- Retains the Control Manager 2.5x agent version (no upgrade takes place)
- Writes the agent information to the Control Manager 3.5 database and TMI.cfg
- 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 3.5 database and TMI.cfg and then writes them back to the Control Manager source database.

## MCP Agent Migration Flow

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

- Stops the Trend Micro Infrastructure service
- Obtains the Product Directory information from the Control Manager source server.
- Migrates the logs of agents selected, if you enabled the Migrate logs option
- Triggers a ChangeServerSrv.exe at the source server
- ChangeServerSrv.exe requests that the source server informs the Control Manager 3.5 agent to register to the destination server
- Destination server waits for MCP agents to register
- Restarts the Trend Micro Infrastructure service

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

## Migrate Trend VCS, Control Manager 2.x, or MCP Agents

Use AgentMigrateTool.exe to migrate Windows-based agents originally administered by Trend VCS 1.8x, Control Manager 2.5, or Control Manager 3.0 servers.

---

**Note:** Run AgentMigrateTool.exe directly on the destination server — a Control Manager 3.5 server to which you will migrate the agents.

---

**To migrate Trend VCS 1.8x or Control Manager 2.5x or MCP agents:**

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 `AgentMigrateTool.exe`.

---

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

---

3. Click **Set Source** on the main menu.
4. On the Configurations screen under **Source server**, type the **IP address** of the *source server*—a Trend VCS 1.8x or Control Manager 2.x/3.x server hosting the agents that will migrate.
5. Under **System Administrator Account**, specify the administrator **user name** and **password** that is 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 3.5 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` notify migrating agents to use HTTPS to register to Control Manager. If you do not select this option, agents use HTTP to register to Control ManagerThese options apply to agents listed in the Destination list.

---

**Note:** 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 agent before running `AgentMigrateTool.exe`.

The following products use the Control Manager 2.1 agent:

- InterScan eManager 3.0 (all applicable platforms)
  - InterScan eManager 3.02 (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.

## Generate a Migration List

Use `AgentMigrateTool.exe` to generate a migration list.

### To generate a migration list:

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 `AgentMigrateTool.exe`.
3. Click **Generate List** from the main menu.
4. Type the **IP address** of the Control Manager 2.5, 3.x server.
5. At the Save As screen, select a **location** and type a **name** for the migration list (for example, `migrationlistcm25.xml`).
6. Click **Generate**.

Using Windows Explorer, navigate to the directory where `AgentMigrateTool.exe` saves the migration list.

The migration list, which you saved in `*.xml` format, allows you to determine the distribution of different agents on your Control Manager network as well as pick those agents that you will migrate to Control Manager 3.5 servers.

You can use this list during a Control Manager remote agent installation to facilitate the replacement of Trend VCS or older Control Manager agents with newer Control Manager agents.

## Migrate the Control Manager Database

You have two ways to migrate a Control Manager 2.5 or 3.0 database:

- Install Control Manager 3.5 on a Control Manager 2.5 or 3.0 server - this is the recommended method  
The Control Manager 3.5 setup automatically upgrades the database to version 3.5. Refer to Control Manager 2.5x agent migration on [page 5-11](#) for more details.
- Manually transfer Control Manager 2.5 or 3.0 database to Control Manager 3.5 server

## Migrate Control Manager SQL 2000 Database to Another SQL 2000 Server

Modify a number of parameters in TMI.cfg to move a Control Manager database from an SQL 2000 server to another SQL 2000 server.

### To migrate an existing database to another SQL 2000 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:** Backup TMI.cfg to roll back too 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.

# 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 presents the administrative tasks that let you configure the Control Manager network including details on how to:

- *Use the Management Console* on page 6-2
- *Configure Control Manager User Accounts and Groups* on page 6-8
- *Administer Managed Products* on page 6-19
- *Manage Child Servers* on page 6-22
- *Download and Deploy New Components* on page 6-28
- *Monitor the Control Manager Environment* on page 6-44

## Use the Management Console

The management console consists of the following elements:

- **Header menu:** Provides links to the Control Manager online help, the Trend Micro Knowledge Base, Trend Micro Security Information, and the About screen for Control Manager
- **Main menu:** Provides links to the Home, Services, Products, Reports, and Administration menus to administer Control Manager and managed products
- **Navigation menu:** Occupies the left-frame of the management console  
When you select a Main Menu item, the Navigation Menu refreshes to display the available options for the menu selected
- **Tab area:** - provides the Product Directory tabs, parent server, or child server tabs
- **Working area:** - this is where you can administer managed products or child server settings, invoke tasks, or view system status, logs, and reports

Aside from the Navigation Menu options, the Working Area also includes managed product or Child server Tabs when you select Products from the Main Menu.

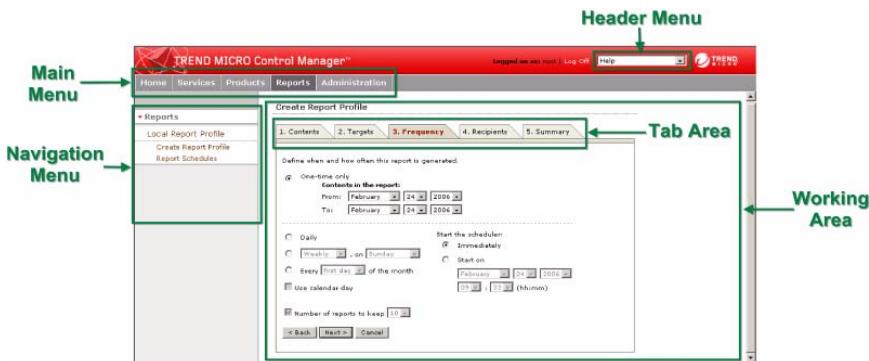


FIGURE 6-1. Control Manager Management Console

<b>HEADER MENU</b>	
<b>Control Manager Help</b>	Provides advanced feature descriptions and detailed configuration information
<b>Support</b>	Provides technical product information and procedures provided by the Trend Micro Support team
<b>Security Info</b>	Provides the latest malware advisories as well as the list of the current top ten security threats
<b>About</b>	Provides the Control Manager version, build number, and copyright information

**TABLE 6-1. Contents of the Control Manager Header menu**

<b>MAIN MENU</b>	
<b>Home</b>	Includes shortcuts to Status Summary tab and available managed products reports
<b>Services</b>	Includes TrendLabs Message Board posts and available services
<b>Products</b>	Includes options to administer Managed Products, Communicators, and Child servers
<b>Reports</b>	Includes options to manage Control Manager managed products and child server reports
<b>Administration</b>	Includes the Command Tracking, Event Center, Update Manager, Logs, User Manager, System Settings, and Tools options

**TABLE 6-2. Contents of the Control Manager Main menu**



## The Function-Locking Mechanism

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

OPTION IN USE	LOCKED OPTION(S)
User Manager	<ul style="list-style-type: none"> <li>• User Manager</li> <li>• Directory Manager</li> </ul>
Directory Manager	<ul style="list-style-type: none"> <li>• User Manager</li> <li>• Directory Manager</li> </ul>
Communicator Scheduler	Communicator Scheduler
Communicator Heartbeat	Communicator Heartbeat
System Settings	System Settings

**TABLE 6-3. Function-Locking Mechanism**

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 "Logon session expired" dialog box appears. Clicking **OK** opens the management console Logon screen.

---

## Access the Management Console

You have two ways to access the management console:

- Locally on the Control Manager server
- Remotely using any compatible browser

**To access the management console locally from the Control Manager server:**

1. Click **Start > Programs > Trend Micro Control Manager > Trend Micro Control Manager**.
2. Provide the user name and password in the **Username** and **Password** fields.
3. Click **Enter**.

**To access the console remotely:**

1. Type the following at your browser's **Address** field to open the Logon page:  
`http://{hostname}/ControlManager`  
Where {hostname} is the Control Manager server's fully qualified domain name (FQDN), IP address, or server name.
2. Provide the user name and password in the **Username** and **Password** fields.
3. Click **Enter**.

Upon opening the console, the initial screen displays 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 cannot access the management console twice using the same user ID and password on the same machine. You can access the management console multiple times on the same computer using unique user IDs. You can also access the management console from different computers using the same user ID and password.

---

## Assign 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 **Directory Security** tab and then click **Server Certificate** to create a server certificate request using the new Certificate Wizard.
  - a. Click **Next**.
  - b. In 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. In 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 **ControlManager** 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 will appear:

*The page must be viewed over a secure channel*

## Access 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://{hostname}:443/ControlManager
```

Where:

{hostname} 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.

## Configure Control Manager User Accounts and Groups

There are four kinds of accounts in Control Manager: Operator, Power User, Administrator, and Root. Control Manager creates the Root account upon installation; you need to create accounts for different types of users.

The root and administrator accounts can view all the functions in the menu, use the available services, and install agents.

Create user groups to simplify sending notifications. For example, you can send email alerts to many Control Manager users at once instead of separate individuals.

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

MENU ITEM	OPERATOR	POWER USER	ROOT/ADMINISTRATOR
<b>HOME</b>			
	•	•	•
<b>SERVICES</b>			
<b>TrendLabs Message Board</b>			•
<b>Outbreak Prevention Services</b>			•
<b>Damage Cleanup Services</b>			•
<b>Vulnerability Assessment</b>			•

**TABLE 6-4. Account User Access**

MENU ITEM	OPERATOR	POWER USER	ROOT/ADMINISTRATOR
<b>PRODUCTS</b>			
Add/Remove Product Agents	•	•	•
Directory Manager	All accounts can use the Directory Manager. However, the account can only access this feature if it has the Edit Directory right.		
Temp	•	•	•
Communicator Scheduler			•
Communicator Heartbeat			•
<b>REPORTS</b>			
Create Report Profile		•	•
Scheduled Reports		•	•
<b>ADMINISTRATION</b>			
Command Tracking	•	•	•
Event Center			•
Update Manager		•	•

TABLE 6-4. Account User Access

MENU ITEM	OPERATOR	POWER USER	ROOT/ADMINISTRATOR
<b>ADMINISTRATION</b>			
Logs - Query or Purge			•
User Manager > My Account	•	•	•
User Manager > User Accounts			•
User Manager > User Groups			•
System Settings			•
Tools			•
Registration			•

TABLE 6-4. Account User Access

## Additional Root Account Privileges

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 is using it.

---

**Note:** Control Manager accounts are for logging into Control Manager only, and not the entire network. Control Manager user accounts are not the same as network domain accounts.

---

## Understanding the User Manager

User Manager is a collection of functions that allow you to create and maintain Control Manager user accounts. Use these functions to assign users clearly defined areas of responsibility - by restricting their access rights to certain managed products, and limiting the actions that they can perform.

---

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

---

## Setting Access Rights

These rights determine the controls available to the user in the Managed Product and Folder menus of the Directory. For example, when you only assign a user the Execute right, then only the options associated with this right will appear on the Product Directory.

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

- View
- Execute
- Configure
- Edit Directory

### View

This allows the user to obtain information from the managed products in the assigned folders. The following managed product and folder options are associated with this right.

- Logs
- Status Summary



- Managed Product Status Summary
- Status Info of <product>

## Execute

This right permits the user to run commands on managed products in assigned folders. The following are associated with this privilege.

- Deploy Now
- Start Scan Now
- Configuration Request
- Product Service

## Configure

This gives the user access to the configuration consoles of the managed products in the assigned folders. Users with this right can see Configuration for <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 assigned folders.

---

**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 will not appear in its menu.

---

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

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

## Add a User Account

Add user accounts to allow others to log on to the Control Manager management console, appear on the recipient list for notifications, or be added to user groups.

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

**To add a user account:**

1. Click **Administration** on the main menu.
2. On the left menu, click **User Accounts**.
3. On the working area, click **Add New User**. The Add New User screen appears.
4. Select the type of user to add.

**To add a Trend Micro Control Manager authenticated user**

- Provide the following information to create an account:
  - **User ID**
  - **Full name**
  - **Password** - you must confirm this in the field provided. You can change this on the My Account screen

The following additional information is optional. You can also set these settings on the My Account screen.

- **Email address**
- **Mobile phone number**
- **Pager number** (precede the pager number with your company's dial out number and a comma ", " [each comma causes a 2 second pause])
- **MSN Messenger address**

**Add an Active Directory authenticated user**

- a. Select Active Directory authenticated user.
- b. Provide the following required information to create an account:
  - **User ID**
  - **Domain:** The domain which the user belongs

---

**Note:** User ID's and domain names can be up to 32 characters in length.

---

5. Click **Next>>**.
6. Click one of the following options on the menu to select an account type: Operator, Power User, or Administrator.

---

**Note:** Enterprise Edition only: For users to take advantage of the cascading management structure, they need to have “Power User” rights or greater.

---

7. Select the check boxes of the rights to assign the privileges 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 is, 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.

---

Go to the Accessible Folders tree. Click the folder where the rights apply.

Carefully organize the Product Directory because you can assign users access to a single point. This means, you can:

- Assign access to a folder, this allows users access to all its sub-folders and managed products
- Restrict a user to a single managed product

8. Click **Apply**.

## Import Active Directory Users

Control Manager supports importing users from pre-established Active Directory lists. Import Active Directory user accounts to allow others to log on to the Control Manager management console, appear on the recipient list for notifications, or be added to user groups. Control manager provides two methods to search for Active Directory users, by user name and by the base distinguished name.

### To add a user account:

1. Access the User Accounts screen.
2. In the working area, click **Import Active Directory Users**. The Add New Active Directory User screen appears.
3. There are two methods available to search for users:
  - **User Name:** Type the name or a partial name for the user in the **User Name** field.

- **Base distinguished name:** Type the distinguished name, the base name, or both to search in the **Base distinguished name** field.
4. Click **Search**. The top ten matches from each domain appear in the User(s) list.
  5. Select the users to add to Control Manager and click the > button. Selected items appear in the **Import List**.
  6. Click the **Next>>** button.
  7. Click one of the following options on the menu to select an account type:  
**Operator, Power User** or **Administrator**.

---

**Note:** **Enterprise Edition only:** For users to take advantage of the cascading management structure, they need to have “Power User” rights or greater.

---

8. Select the check boxes of the rights to assign the privileges to the user. These rights determine what actions the user can perform on managed products.

---

**Note:** Privileges granted to an account cannot exceed those of the grantor. If you reduce an account's rights, you also reduce all of its sub-accounts.

---

9. Go to the Accessible Folders tree and click the folder where the rights apply. Carefully organize the Product Directory, because you can assign users access to a single point.

---

**Note:** You can assign access to a folder, this allows users access to all its sub-folders and managed products.  
You can restrict a user to a single managed product.

---

10. Click **Apply**.

## Edit a User Account

You can change the information of any user account you have added including account information, account type, or folder access rights. However, access rights granted to an account cannot exceed those of the grantor. That is, 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.

**To edit a user account:**

1. Click **Administration** on the main menu.
2. On the left menu, click **User Accounts**.
3. In the working area, click **Edit** beside the account to modify.
4. Modify the account information, and then click **Next>>**.
5. Modify the accessible folders and access rights.
6. Click **Apply**.

When editing accounts, remember:

- Root users can edit all the accounts that exist on the system. Administrator accounts, however, can only edit those that they created themselves.
- An account's rights are a sub-set of those of its grantor; and are adjusted 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 downgrade of rights, child accounts whose privileges are also affected will also be logged out.
- You cannot change an existing account's User ID.

## Disable 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. Click **Administration** on the main menu.
2. On the left menu, click **User Accounts**.
3. On the working area of the Add User or Edit User screen, select the **Disable this account** check box.
4. Click **Next>>**.
5. Click **Apply**.

## Delete a User Account

Permanently remove a user account from accessing the Control Manager network. After you delete a user account, it is removed from any groups it used to belong to and the user no longer receives notifications for those events where the user account was added to the recipient list.

### To delete a user account:

1. Click **Administration** on the main menu.
2. On the left menu, click **User Accounts**.
3. On the working area, click **Delete** beside the account.
4. Click **OK** to delete the account.


## Add 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. Click **Administration** on the main menu.
2. On the left menu, under **User Manager**, click **User Groups**.
3. On the working area, click **Add New Group**.
4. Type a descriptive name for the group in Group name.
5. 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.

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 a "9" and a comma ", " [each comma causes a 2 second pause])

Separate multiple entries with semicolons.

6. Click **Save**.
7. Click **OK**.

## Edit a User Group

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

**To edit a user group:**

1. Click **Administration** on the main menu.
2. On the left menu, under **User Manager**, click **User Groups**.
3. On the working area, click **Edit** beside the group to modify.
4. Change the entries as required.
5. Click **Save**.
6. Click **OK**.



## Delete a User Group

Permanently remove a user group from the Control Manager network. 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. Click **Administration** on the main menu.
2. On the left menu, under **User Manager**, click **User Groups**.
3. On the working area, click **Delete** beside the group to delete.
4. Click **OK** to delete the user group.
5. Click **OK**.

## Administer Managed Products

A **managed product** is a representation of an antivirus, content security, or third party product in the Product Directory. Managed products are the icons (for example,  or ) in the Control Manager management console Product Directory section. These icons represent Trend Micro antivirus and content security products, as well as third-party products.

Indirectly administer the managed products either individually or by groups through the Product Directory. Use the Directory Manager to customize the Product Directory organization.

## Configure Managed Products Using the Product Directory

The Product Directory is a logical grouping of managed products. It allows you to perform the following for administering managed products:

- Configure 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 it affects the following:

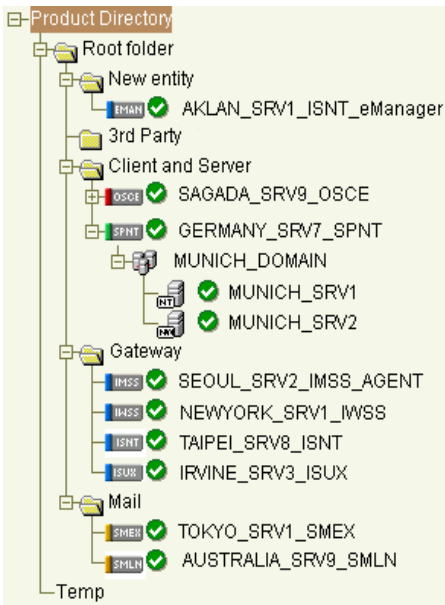
- **User access:** When creating user accounts, Control Manager prompts for the segment of the Product Directory that the user can access. Carefully plan the Product Directory since you can only grant access to a single segment. For



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.

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 (see *Administration Plan* on page

2-8). For example, grant access rights to mail administrators to configure the Mail folder. Refer to the Control Manager *Understanding Directory Manager* online help topic for details on how to arrange the Product Directory.

## Default Folder for Managed Products

Newly registered managed products handled by Control Manager agents usually appear in the **New entity** folder - depending on the user account specified during the agent installation. Control Manager determines the default folder for the managed product by the privileges of the user account specified during the product agent installation.

However, Control Manager segregates managed products handled by Trend VCS agents under the **Trend VCS agents** folder.

## Use the Product Directory Tabs

Use the Product Directory tabs to configure and administer managed products. Control Manager 3.5 makes the following tabs available:

TABS	DESCRIPTION
<b>Product Status</b>	Use this tab to obtain status summaries about individual or groups of managed products The Product Status tab provides managed product-specific or group summaries depending on the element you selected.
<b>Configuration</b>	Use this tab to log on to the product's Web-based console and configure the managed product The Configuration tab is available when configuration options are available to the element you selected.
<b>Tasks -</b>	Use this tab to perform specific functions (such as deploying the latest components) to a managed product or group of managed products or child servers If you initiate a task from the Product Directory folder group or cascading structure parent server-level Tasks tab, Control Manager sends requests to all managed products belonging to that group/level.

TABLE 6-5. Product Directory Tabs

TABS	DESCRIPTION
Logs	Use this tab to query and view product logs If you select a Product Directory managed product, you can only query logs for that specific product. Otherwise, you can query all the products available in the group.

TABLE 6-5. Product Directory Tabs

## Group Managed Products Using Directory Manager

Use the Directory Manager to customize the Product Directory organization to suit your administration model needs (see *Administration Plan* on page 2-8). For example, you can group products by location or product-type - messaging security, Web security, file storage protection, and so on.

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:

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

TABLE 6-6. Advantages and disadvantages when grouping managed products

## Manage Child Servers

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

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

Aside from the parent servers 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:

FEATURE	AVAILABLE IN PARENT	AVAILABLE IN CHILD
Support two-tier cascading structure	Yes	No
Manage Enterprise and Standard edition 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

**TABLE 6-7. Parent and child server feature comparison**

---

**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).

---

## Configure Child Server Using the Cascading Structure Tree

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, spyware/grayware, content security, network viruses, service violations, 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.

---

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

---

## Use the Cascading Structure Tree Tabs

Depending on which item you clicked, the management console provides the following tabs for performing parent server or child server-specific actions:

- **Global Status** (for parent server) / **Product Status** (for child server) - use this tab to obtain status summaries about individual or groups of managed products  
The Product Status tab provides managed product-specific or group summaries depending on the element you selected.
- **Configuration** (for child server) - use this tab to log on to the product's Web-based console and configure the managed product  
The Configuration tab is available when configuration options are available to the element you selected.
- **Global Tasks** (for parent server) / **Tasks** (for child server) - use this tab to perform specific functions (such as deploying the latest components) to a managed product or group of managed products or child servers  
If you initiate a task from the Product Directory folder group or cascading structure parent server-level Tasks tab, Control Manager sends requests to all managed products belonging to that group/level.
- **Global Logs** (for parent server) / **Logs** (for child server) - use this tab to query and view product logs
- **Reports** (for child server) - use this tab to query and view child server product reports

If you select a Product Directory managed product, you can only query logs for that specific product. Otherwise, you can query all the products available in the group.

## Registering or Unregistering Child Servers

Use specific *CasTool.exe Commands* on page 7-3 to change a child server's parent server. The tool allows you to unregister a child server from a parent server and register it to another parent server.

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*, run `CasTool.exe` to 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.

`CasTool.exe` is useful 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. From the Control Manager server, click **Start > Run**.
2. Type `cmd` and then click **OK**.
3. On the Windows command interpreter, go to the Control Manager root directory (for example, `<root>\Program Files\Trend Micro\Control Manager\`).
4. Execute one of the following:
  - `castool /n:{parent server user account} /p:{parent server name:port} /c:"{child server display name}"`

For example:

```
castool /n:root /p:cm.test.com:8080 /c:"child_01"
```

`CasTool.exe` will use the root account to access `http://cm.test.com:8080/download/e2epublic.dat` and download the public key from the parent server. It will then register the child server as **child\_01** in the parent server cascading structure tree.

- `castool /n:{parent server user account} /p:{parent server name:port} /c:"{child server display name}" /s`

For example:

```
castool /n:root /p:cm.test.com:8080 /c:"child_01" /s
```

CasTool.exe will use the root account to access

`http://cm.test.com:8080/download/e2epublic.dat` via HTTPS and download the public key from the parent server. It then registers the child server as **child\_01** in the parent server cascading structure tree.

- `castool /n:{parent server user account} /f:"{local directory}" /c:"{child server display name}"`

For example:

```
castool /n:root /f:"C:\E2EPublic.dat" /c:"child_01"
```

CasTool.exe will use the root account to access and get the public key from the local directory (`C:\E2EPublic.dat`). It will then register the child server as **child\_01** in the parent server cascading structure tree.

CasTool.exe restarts the Control Manager services after executing the register or unregister commands.

#### To unregister a child server using CasTool.exe:

1. From the Control Manager server, click **Start > Run**.
2. Type `cmd` and then click **OK**.
3. On the Windows command interpreter, go to the Control Manager root directory (for example, `<root>\Program Files\Trend Micro\Control Manager\`).
4. Execute `castool /u` (the unregister command).

---


**Note:** You can use the `/d` command to debug the process while CasTool unregisters a child server. If you remove Control Manager 3.5 from a child server, the child server executes the `"castool /u /d"` to unregister itself automatically from a parent server.

---

#### To unregister a child server using the cascading structure Cascading Manager:

1. Click **Products** on the main menu.
2. On the left menu, select **Control Managers** from the list and then click **Go**.
3. On the left menu, click **Cascading Manager**.
4. In the working area, right-click the child server to unregister, and then select **Delete** from the menu.

---

**Note:** Trend Micro recommends using the **Cascading Manager Delete** option only when the child server status is abnormal (  ). Take care when using the Cascading Manager, or else you may accidentally unregister child servers that need to remain registered.

---



## Download and Deploy New Components

Update Manager is a collection of functions that help you update the antivirus and content security components on your Control Manager network.

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

- Pattern files/Cleanup templates - refer to virus pattern files, damage cleanup templates, Vulnerability Assessment patterns, network outbreak rules, and network virus pattern files
- Anti-spam rules - refer to import and rule files used for anti-spam and content filtering
- Engines - refers to virus scan engine, damage cleanup engine, and VirusWall engine for Linux
- Product programs - these are product specific components (for example, Service Pack releases)

---

**Note:** Only registered users are eligible for components update. For more information, see the Control Manager online help [Registering and Activating your Software > Understanding product activation topic](#).

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

---

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

1. Downloading components manually or by schedule
2. Deploying components immediately or by schedule

If you configured your scheduled or manual download to either use a Deployment Plan, or to "deploy immediately", Control Manager deploys components after it completes their download. Otherwise, you will have to perform a manual deployment.

## 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. Manually downloading components 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 settings

**Step 5:** Configure the automatic deployment settings

**To manually download components:**

**Step 1: Create a deployment plan:**

1. Click **Administration** on the main menu.
2. On the left menu under Update Manager, click **Deployment Plan**. The Deployment Plan screen appears.
3. On the working area, click **Add New Plan**.
4. On the Add New Plan screen, type a deployment plan name in the **Plan name** field.
5. Click **Add New Schedule** to provide deployment plan details. The Add New Schedule screen appears.
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**

1. Click **Administration > System Settings**. The System Settings screen appears.
2. Select the **Use a proxy server to download update components from the Internet** checkbox in the Download component proxy settings area.
3. Type the host name or IP address of the server in the **Host name** field.
4. Type a port number in the Port field.
5. Select the protocol:
  - HTTP
  - SOCKS
6. Type a login name and password if your server requires authentication.
7. Click **Save**.

### **Step 3: Select the components to update**

1. Click **Administration > Update Manager > Manual Download**. The Manual Download screen appears.
2. From the Components area select the components to download.
  - a. Click the + icon to expand the component list for each component group. The groups are the following:
    - Pattern files/Cleanup templates
    - Anti-spam rules
    - Engines
    - Product programs
  - b. Select the components to download. To select all components for a group, select:
    - Pattern files/Cleanup templates
    - Anti-spam rules
    - Engines
    - Product programs

**Step 4: Configure the manual download settings**

1. Select the update source:
  - Select **Internet: Trend Micro update server** to download components from the official Trend Micro ActiveUpdate server.
  - Select **Other update source** and 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 of retries and duration between retries for downloading components.

---

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

---

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

4. Click **Download Now** and then click **OK** to confirm. The download response screen appears. The progress bar displays the download status.
5. Click the **Command Details** to view details from the Command Details screen.
6. Click **OK** to return to the Manual Download screen.

## Automatically Downloading Components

Configure scheduled downloading of components to keep your components up-to-date and your network secure. Control Manager 3.5 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.

The Scheduled Download screen displays following information for components currently in your Control Manager system:

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

---

**Tip:** Enable or disable component group or individual component downloads by clicking the icon that appears in the Enabled column of the table.

---

Configuring scheduled downloading of components 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:** Schedule and frequency

**Step 5:** Configure the download settings

**Step 6:** Configure the automatic deployment settings

**To configure scheduled component downloads:****Step 1: Create a deployment plan:**

1. Click **Administration** on the main menu.
2. On the left menu under Update Manager, click **Deployment Plan**. The Deployment Plan screen appears.
3. On the working area, click **Add New Plan**.
4. On the Add New Plan screen, type a deployment plan name in the **Plan name** field.
5. Click **Add New Schedule** to provide deployment plan details. The Add New Schedule screen appears.
6. On the Add New Schedule screen, choose a deployment time schedule by selecting one of 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**

1. Click **Administration > System Settings**. The System Settings screen appears.
2. Select the **Use a proxy server to download update components from the Internet** checkbox in the Download component proxy settings area.
3. Type the host name or IP address of the server in the **Host name** field.
4. Type a port number in the Port field.
5. Select the protocol:
  - HTTP
  - SOCKS

6. Type a login name and password if your server requires authentication.
7. Click **Save**.

### **Step 3: Select the component group or component to download**

1. Click **Administration > Scheduled Download**. The Scheduled Download screen appears.
2. 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 component or component group to configure for download. To download all components for a group, select:
    - Pattern files/Cleanup templates
    - Anti-spam rules
    - Engines
    - Product programs

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

### **Step 4: Configure the component group's or component's schedule and frequency**

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 every minute, hour, day, or week.
3. Use the **Start time** menus to specify the **date** and **time** the schedule starts to take effect.

### **Step 5: Configure the scheduled 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 of retries and duration between retries for downloading components.

---

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

---

### Step 5: Configure 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
2. Select a deployment plan after components download to Control Manager, from the **Deployment plan:** list.
3. Click **Save**.
4. Click **Download Now** and then click **OK** to confirm. The download response screen appears. The progress bar displays the download status.
5. Click the **Command Details** to view details from the Command Details screen.
6. Click **OK** to return to the Manual Download screen.



## Configure 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. Click **Administration** from the main menu, and then click **Scheduled Download** from the left menu under Update Manager to access the Scheduled Download screen.
2. On the working area, click the **Edit** link of the component whose scheduled download schedule and frequency you want to modify.
3. Under **Schedule and frequency**:
  - a. Define the download **schedule**. Select a **frequency**, and use the appropriate drop down menu to specify the desired schedule. You may schedule a download every minute, hour, day, or week.
  - b. Use the **Start time** menus to specify the **date** and **time** the schedule starts to take effect.
4. Click **Save**.

## Configure Scheduled Download Settings

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

### To configure scheduled download settings:

1. Click **Administration** from the main menu, and then click **Scheduled Download** from the left menu under **Update Manager** to access the Scheduled Download screen.
2. On the working area, click the **Edit** link of the component whose scheduled download settings you want to modify.
3. Under **Download settings**:
  - a. Select the **components** to download.
  - b. Under **From**, 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
  - **File path** - specify a location on your network of the latest component source, for example, your company's file server (see *Enable UNC Download* on page 6-39)
- c. 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.
  - d. If 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 (*Configure Proxy Server Connection for Component Download and Trend VCS Agents* on page 6-38) from the System Settings screen.

4. Click **Save**.

Use **Command Tracking** to check whether Control Manager performed the scheduled download at the specified time and date.

## Configure 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. Click **Administration** from the main menu, and then click **Scheduled Download** from the left menu under **Update Manager** to access the Scheduled Download screen.
2. On the working area, click the **Edit** link of the component whose scheduled download automatic deployment settings you want to modify.
3. Under **Automatic deployment**, select the appropriate deployment schedule. The options are:
  - **DO NOT deploy** - click this option if you intend to:
    - Deploy to the managed products individually
    - Test the updated components before deployment
  - **Based on deployment plan** - this option requires that you define an appropriate Deployment Plan by selecting the options from the **Plan used list**

It gives you the greatest control over the update, since you can specify which products Control Manager updates, and in what order.

- **Deploy immediately** - this deploys the updates to all managed products immediately after Control Manager completes the download

4. Click **Save**.

## Configure Proxy Server Connection for Component Download and Trend VCS Agents

Use the System Settings screen to configure proxy server connection for component download and Trend VCS agents.

**To configure proxy server settings:**

1. Click **Administration** on the main menu.
2. On the left menu, click **System Settings**. The System Settings screen appears.
3. On the working area under **Proxy Settings for Component Download** or **Proxy Settings for Trend VCS Agents**, set the proxy server settings:
  - a. If using a proxy server to connect with the Internet:
    - On the working area under **Proxy Settings for Component Download**, click **Use a proxy server to download update components from the Internet**.
    - On the working area under **Proxy Settings for Trend VCS Agents**, click **Use a proxy server to connect to Trend VCS agents**.
  - b. Specify the proxy server **host name** and **port**.
  - c. Select the proxy server protocol—**HTTP** or **Socks**.
  - d. Type the **user name** and **password** used for proxy authentication.
  - e. Click **Save**.

## Enable HTTPS Download

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

**To enable HTTPS download:**

1. Click **Administration** on the main menu.
2. On the left menu, click **System Settings**. The System Settings screen appears.
3. On the working area under **ActiveUpdate settings**, select **Enable HTTPS for the default update download source** or specify your organizations component source server in the **Other Internet source field**.
4. Click **Save**.
5. Do one of the following:
  - On the left menu under **Update Manager**, click **Manual Download**
  - On the left menu under **Update Manager**, click **Scheduled Download**Define a **schedule** for a component by clicking its corresponding **Edit** link. This opens the component's configuration screen, which is divided into three groups: **Schedule and frequency**, **Download settings**, and **Automatic deployment**.
6. On the working area under **Download settings > From** group, select **Internet: Trend Micro update server**.
7. Click **Save**.

**Enable UNC Download**

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

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

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

The **Remote UNC authentication** is any user account from the component source server with permission to share a folder where Control Manager downloads updates.

**To enable UNC download:**

1. Click **Administration** on the main menu.
2. On the left menu, click **System Settings**. The System Settings screen appears.
3. On the working area under ActiveUpdate settings, provide the **local Windows** and **Remote UNC authentication user names** and **passwords**.

4. Click **Save**.
5. Do one of the following:
  - On the left menu under Update Manager, click **Manual Download**.
  - On the left menu under Update Manager, click **Scheduled Download**.

Define a **schedule** for a component by clicking its corresponding **Edit** link. This opens the component's configuration screen, which is divided into three groups: **Schedule and frequency**, **Download settings**, and **Automatic deployment**.

6. On the working area under Download settings > From group, select **File path** and then specify the **shared network folder**.
7. Click **Save**.

## Set "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 set "Log on as batch job" policy:

1. Add **Security Configuration Analysis** in the **Console Root**.
  - a. Click **Start > Run**, type **mmc**, and then click **OK**. A blank console window opens.
  - b. From the Console menu, select **All/Remove Snap-in...**
  - c. On the Add/Remove Snap-in window, click **Add** and then select **Security Configuration Analysis**.
  - d. Click **Add** and then click **OK** to return to the console window.
2. Run **Configure Computer Now** and **Analyze Computer Now**.
  - a. On the left pane, right-click the **Security Configuration and Analysis** scope item and then select **Open database...** from the menu.
  - b. In the Open database window, type the **name** for the security database file and then click **Open**.
  - c. In the Import Template window, select **basicsv.inf** from the security template lists and then click **Open**.

- d. On the left pane, right-click the **Security Configuration and Analysis** scope item and then select **Configure Computer Now...** from pop-up menu.
  - e. Provide the error log **file name**, and then click **OK**.
  - f. On the left pane, right-click the **Security Configuration and Analysis** scope item and then select **Analyze Computer Now...** from pop-up menu.
  - g. Provide the error log **file name**, and then click **OK**.
3. Set **Log on as a batch job** policy.
- a. On the left pane, expand the **Security Configuration and Analysis > Local Policies** scope item.
  - b. Click **User Rights Assignment**.
  - c. On the right pane, double-click **Log on as a batch job**.
  - d. On the Analysis Security Policy Setting window, select **Define this policy in the database**.  
  
If the user account used for local Windows authentication is not in the list, click **Add** to assign **Log on as batch job Database Setting** to a user with administrative privilege and then click **OK**.
  - e. On the left pane, right-click **Security Configuration and Analysis**, click **Save** and then click **Configure Computer Now** to apply the changes.

## Deploy Updated Components

A Deployment Plan allows you to set the order that 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 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

## Create Deployment Plans

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

### To create a new deployment plan:

1. Click **Administration** on the main menu.
2. On the left menu under **Update Manager**, click **Deployment Plan**. The Deployment Plan screen appears.
3. On the working area, click **Add New Plan**.
4. On the Add New Plan screen, type a deployment plan **name** in the plan name field.
5. Click **Add New Schedule** to provide deployment plan details.
6. On the Add New Schedule screen, choose a deployment time **schedule** by selecting one of the following options:
  - **Delay** - after Control Manager downloads the update components, it delays the deployment according to the interval you specify  
Use the menus to indicate the duration, in terms of hours and minutes.
  - **Start at** - this performs the deployment at a specific time  
Use the drop-down 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. On the Add New Plan screen, do one of the following:
  - Click **Add New Schedule** to add another schedule
  - Click **Save** to apply the new deployment plan

## Update All Outdated Components

Updating and deploying new components to managed products with out-of-date components involves two steps.

### To update all out-of-date components:

1. Add managed products with out-of-date components to **Temp**.
  - a. Click **Products** on the main menu.
  - b. On the left menu, select **Managed Products** from the list and then click **Go**. The Product Directory screen appears.
  - c. On the left menu, select the Product Directory **folder**, then in the working area, click the **Product Status** tab.
  - d. At the **Component Status** table, click one of the numeric links indicating the number of **out-of-date** managed products. Depending on the link you clicked, the Virus Pattern Status (Out-of-date), Scan Engine Status (Out-of-date), or Spam Rule Status (Out-of-date) screen shows the computer name, product name, product version, and outdated component version.
  - e. Click **Add to Temp** in the status page. Control Manager organizes the managed products in Temp under folders named after the screen from which you added them. For example, Control Manager places managed products added from the Scan Engine Status (Out-of-date) page under the Scan Engine Status (Out-of-date) folder.

---

**Note:** Clicking **Add to Temp** adds only the managed products on the status screen. If the list of managed products spans multiple screens, click **Add to Temp** on all screens to add all products with outdated components.

---
- f. Click **<<Back** to return to the Status Summary page, and then proceed to the next out-of-date component. Repeat the instructions until Control Manager adds all the out-of-date managed products to Temp.
2. On the working area, click the **Tasks** tab.
3. Select **Deploy <component>** from the Select a task list, and then click **Next**.
4. Click **Deploy Now** to start updating all out-of-date components.

Monitor the progress via Command Tracking. Click the **Command Details** link to view the Deploy Now command details.



## Monitor the Control Manager Environment

Use the Administration main screen to view the state of your Control Manager network.

Select **Administration** on the menu to access the Control Manager network information. The screen provides the following information:

- **System information** - groups all Control Manager server related system information and includes the following:
  - Control Manager server - indicates the host name of the server hosting the Control Manager application
  - Installed version - indicates the version and build number of the Control Manager program
  - Registration - indicates the date you installed the Control Manager program  
If you are using a Control Manager evaluation version, this shows when the evaluation period began. This is useful when monitoring the time remaining in the evaluation period. If you installed or upgraded to a full version of Control Manager, it shows the date you registered the product.
  - Running since - indicates when the Control Manager service was last started
  - Virus pattern file - indicates the version of the virus pattern used by antivirus products
  - Anti-spam rule - indicates the version of the spam rule used by content security products
  - Damage cleanup template - indicates the version of the cleaning template used by Damage Cleanup Services (DCS)
  - Damage cleanup engine - indicates the version of the engine used by DCS
  - Network outbreak rule - indicates the version of the collaborative antivirus rule file used by packet scanning and antivirus products like Trend Micro Network VirusWall 1200
  - Network virus pattern - indicates the version of the network pattern used by packet scanning products
  - Network VirusWall engine - indicates the version of the engine used by packet scanning antivirus products
  - Vulnerability assessment pattern file - indicates the version of the vulnerability pattern used by Vulnerability Assessment Services (VAS)

- Vulnerability assessment engine - indicates the version of the vulnerability engine used by VAS
- Spyware pattern file - indicates the version of the component used to detect hidden but legal program that secretly collects confidential information
- Virus scan engine - indicates the platform, version, and update time of the scan engine used by different managed product and services registered to the Control Manager server
- **Security level** - indicates the security setting that you specified during the Control Manager installation

## Use 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. 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 the Command Tracking later for results.

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

- Date/Time Issued - indicates the date and time when the Control Manager server issued the command to the managed product or child server
- Command - indicates the type of command issued
- Successful - indicates the number of managed products or child servers that completed the command
- Unsuccessful - indicates the number of managed products or child servers that was not able to perform the command
- In Progress - indicates the number of managed products or child servers that currently performs the command
- All - indicates 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.

## Query and View Commands Issued in the Past 24 Hours

Use the Command Tracking Query screen to track and view commands issued over an extended period of time — that is, more than 24 hours.

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

1. Click **Administration** on the main menu.
2. On the left menu click **Command Tracking**.
3. On the working area, click **Query**.
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 their results.  
Click the available link in the **Successful, Unsuccessful, In Progress, or All** column to view their Command Details.

## Use 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:

- Alert - provides warning about viruses and spyware/grayware detected by antivirus and spyware/grayware managed products
- Outbreak Prevention Services - provides information about policy application and update information about Outbreak Prevention Services

- Damage Cleanup Services - provides information about policy application and update information about damage cleanup services-related events
- Vulnerability Assessment - provides "Vulnerability Assessment task completed" event notification
- Statistics - provides statistics on the number of policy violations versus compliances from Network VirusWall devices
- Update - provides antivirus and content security components update result (successful or unsuccessful)
- Unusual - provides information about product option or service activation and deactivation

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:

- Email - messages sent to a mailbox belonging to the organization's email system or to a POP3 account (for example, Yahoo!™ or Hotmail™)
- Windows event log - the Windows Event Viewer application log contains events logged by Control Manager
- SNMP - 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 **MIBs browser** to view SNMP trap notification.

- Pager - an electronic device that accepts messages from a special radio signal
- 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. Otherwise, an off-line MSN Messenger account cannot receive Control Manager notifications.

- 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.

## Enable or Disable Notifications

Enable or disable notifications from the Event Center screen.

### To enable or disable notifications:

1. Click **Administration** on the main menu.
2. On the left menu, click **Event Center**.
3. Do one of the following:
  - Select/clear the event check boxes
  - Select/clear Enable all notifications to activate/deactivate Control Manager notifications
4. Click **Apply**.

## Configure Notification Method

Use the System Settings screen to configure settings used by the selected notification method.

### To configure notification method settings:

1. Click **Administration** on the main menu.
2. On the left menu, click **Event Center**.
3. On the working area under Notification Settings, configure the notification method:

### To set an email notification:

- a. On the working area under **SMTP Server**, type the **hostname** 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, which is a requirement for some SMTP servers.

### To set a pager notification:

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

**To set an MSN Messenger notification:**

- a. On the working area under **MSN notification**, specify the **MSN Messenger email address**. This is the user name used 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**.
  - Specify the proxy server hostname and port.
  - Select the proxy server protocol—Socks 4 or Socks 5.
  - Type the login name and password used for proxy authentication.

**To set an SNMP notification:**

- a. On the working area under **SNMP trap notification**, specify the **Community name**.
  - b. Specify the SNMP trap server **IP address**.
4. Click **Save**.


## Configure Notification Recipients and Test Notification Delivery

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

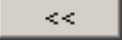
**To configure the notification recipients and test notification delivery:**

1. Click **Administration** on the main menu.
2. On the left menu, click **Event Center**.
3. On the working area, click the **Recipients** link of the event you want to configure.
4. On the Edit Recipients under **Email and Pager Recipient List**, specify or remove the email and pager notification recipients:

**To add recipients from the list:**

- a. Click the user or group from the **Users and groups** list. To select multiple recipients, use the CTRL key.
- b. Click  to add the entry to the **Recipients** list.

**To remove a recipient from the list:**

- a. Click the user or group from the Recipient list. To select multiple recipients, use the CTRL key.
  - b. Click  to remove the entry from the Recipients list.
5. Select the check box of the corresponding **notification method** you prefer:  
Configure the notification method settings via the System Settings screen. Refer to Configure Notification Method.
  6. Provide the **notification message** in the corresponding message fields.
  7. Click **Test** to experiment if your system is able to deliver the notifications.
  8. Click **Save**.

## Configure Virus Outbreak Alert Settings

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

**To configure virus outbreak alert settings:**

1. Click **Administration** on the main menu.
2. On the left menu, click **Event Center**.
3. On the working area, click **Settings** adjacent to the Virus outbreak alert event.
4. On the Edit Virus Outbreak Alert Settings screen, provide the following:
  - Virus count - the number of viruses that triggers an outbreak alert
  - Time period - the period of consideration for virus count parameter
  - Spread - the number of computers infected
5. Click **Save**.

## Configure Special Virus Alert Settings

Configure Control Manager to send notifications whenever it detects a virus on your system. Special virus alert notifications provide an early warning of what could be a potential virus outbreak.

**To configure special virus alert settings:**

1. Click **Administration** on the main menu.
2. On the left menu, click **Event Center**.

3. On the working area, click **Settings** adjacent to the Special virus alert event.
4. On the Edit Special Virus Alert Settings screen, specify the **Notification frequency** (in hours) using the list.
5. Type the **virus names** that you want to monitor. Specify up to 10 viruses.
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 what could be a potential spyware/grayware item.

### To configure special virus alert settings:

1. Access Event Center.
2. On the working area, click **Settings** adjacent to the Special spyware/grayware alert event.
3. On the **Edit Special spyware/grayware Alert Settings**, specify the **Notification frequency** (in hours) using the list.
4. Type the spyware/grayware names that you want to monitor. You can list up to 10 items of spyware/grayware.
5. Click **Save**.

## Use Reports

A Control Manager **report** is an online collection of figures about virus, spyware/grayware, and content security events that occur on the Control Manager network. The Enterprise edition provides the Control Manager reports.

Control Manager 3.5 categorizes reports according to the following types:

- *Local reports* about managed products administered by the parent server  
Local reports do not include reports generated by child servers. Use the Global Report options to view reports about managed products administered by child servers registered to the parent server.
- *Global reports* about managed products administered by child servers as well as the parent server



---

**Note:** You can only configure the **Global Report Profile** option through the *parent server management console*.

---

A **profile** lays out the content (template and format), target, frequency, and recipient of a report. You can view reports in the following file formats:

- **RTF** - rich text format; use a word processor (for example, Microsoft Word™) to view \*.RTF reports
- **PDF** - portable document format; use Adobe Reader to view \*.PDF reports
- **ActiveX™** - ActiveX documents; use a Web browser to view reports in ActiveX format

Control Manager cannot send reports in ActiveX format as email attachments.

- **RPT** - Crystal Report format; use Crystal Smart Viewer to view \*.RPT reports

After generating the report, Report Server launches the default viewer for that report file format. For RPT reports, you must have the Crystal Smart Viewer installed.

## Create Report Profiles

Use the local or global Create Report Profile screen to create report profiles. Creating a report profile requires a number of steps through four screens:

- **Contents:** Select the report profile type and provide a profile name and description
- **Targets:** Select the source of the report data
- **Frequency:** Configure the schedule to generate reports
- **Recipient:** Configure settings for the recipient of the reports

### To create local or global report profile:

#### Step 1: Select the local or global report type:

1. Click **Reports** on the main menu.
2. Take one of the following actions:
  - To create a local report profile, click **Local Report Profile** under Reports.
  - To create a global report profile, click **Global Report Profile** under Reports.
3. On the left menu under Local Report Profile or Global Report Profile, click **Create Report Profile**.

**Step 2: Configure the settings on the Contents screen:**

1. In the working area under the Contents tab, type a name for the report in the **Report name** field to identify the profile on the Local Reports screen.
2. Type a title for the report in the **Report Title** field (optional).
3. Type a description of the report profile in the **Description** field (optional).
4. Specify settings for one of the following:
  - To configure settings for New CM 3.0 reports**
    - a. Select **New CM 3.0 Reports**.
    - b. Select the reports to generate and configure the settings that accompany the report.
  - To configure settings for original CM 3.0 reports**
    - a. Select **CM 3.0 Original Reports**.
    - b. Select the report to generate.
5. Select the output format for the report.
6. Click **Next >** to proceed to the Targets tab.

**Step 3: Configure the settings on the Targets screen:**

1. On the working area under the Targets tab, select the **target** of the local or global report profile:
  - Select the **managed products** or **folders**.

The profile only contains information about the managed products or folders selected.
  - Select the **child servers**.

The profile will only contain information about the child servers selected. Select the parent server to include all child servers' managed products in the profile.

2. If you are creating a report profile for NVW devices, select the machines that the report will include:
  - **All clients:** All clients the selected NVW protects
  - **IP range:** Select the IP range of the clients you want to include in the report
  - **Segment:** Select the IP range and segment of the clients you want to include in the report
3. Click **Next >** to proceed to the Frequency tab.

**Step 4: Configure the settings on the Frequency screen:**

1. On the working area under the Frequency tab, specify **how often** Control Manager generates this report. You have the following options:
  - **One-time only:** Provides information you specified in the From and To dates
  - **Daily:** Contains information from the creation time (12:00 AM yesterday) up to the current time
  - **Weekly or Bi-weekly:** Contains 7 or 14 days worth of information; select the day of the week that will trigger the report server to generate a report
  - **Monthly:** Contains 30 days worth of information; select the day of the month (first, 15th, or last day) that will trigger the report server to generate a report
  - **Use calendar day:** If checked, the start time is 00:00:00 of the first day and the end time is 00:00:00 of the day before generation  
If it is not checked, the start time is the same generation hour of the first day and end time is the generation hour of the day when generation occurs
2. Under **Start the scheduler**, specify **when** the Report Server starts collecting information for this report. Select one of the following:
  - **Immediately:** The report server collects information as soon as you save the report profile
  - **Start at:** The report server collects information at the specified date and time
3. For scheduled reports, click **Number of reports to keep** and then specify the **instance** Control Manager will maintain on the server.

---


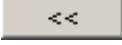
**Note:** Control Manager automatically enables a scheduled report profile. To temporarily disable generating reports, user should navigate to the Local or Global Scheduled

Reports screen, and then check the check box adjacent to the scheduled report profile and click **Disable** to stop schedule.

---

4. Click **Next** > to proceed to the Recipient tab.

**Step 4: Configure the settings on the Recipient screen:**

1. On the working area under the Recipients tab, select **recipients** from the existing Control Manager users and groups.
  - Use  to add recipients from the **Users and groups** list to the Recipient list
  - Use  to remove recipients from the **Recipient** list
2. Click **Send the report as an attachment** to send the report as an attachment. Otherwise, recipients will only receive an email notification about the report being generated.
3. Click **Next** > to proceed to the Summary tab.
4. On the working area under the Summary tab, review the profile settings and then click **Finish** to save the profile.

## Generate On-demand Scheduled Reports

The Report Server generates scheduled reports based on the date and time you specified. When the date and time has not yet commenced, use **Generate** to create scheduled reports on demand.

**To generate on-demand scheduled reports:**

1. Click **Reports** on the main menu.
2. Complete one of the following:
  - To create a local report profile, click **Local Report Profile** on the left menu under **Reports**
  - To create a global report profile, click **Global Report Profile** on the left menu under **Reports**
3. On the working area under the **Available Reports** column, click the corresponding **View** link.
4. On the Available Reports for {profile name} under **Generate a Monthly report starting from**, specify the **starting month, day, and year**.

5. Click **Generate**.

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 Report** link adjacent to the report becomes available.

## View Generated Reports

Aside from sending and then viewing reports as email attachments, you can also use the Local Report Profile or Global Report Profile screen to view the available local or global reports.

### To view reports:

1. Click **Reports** on the main menu.
2. Do one of the following:
  - To create a local report profile, click **Local Report Profile** on the left menu under Reports
  - To create a global report profile, click **Global Report Profile** on the left menu under Reports
3. On the working area under the **Available Reports** column, click the corresponding **View** link.  
On the Available Reports for {profile name}, you can sort reports according to **Submission Time** or **Stage Completion Time**.
4. Under the **Status** column, click **View Report**.  
The default program used to open the file format opens.

## Using Tools

Control Manager 3.5 provides a number of tools to help you with specific configuration tasks.

Control Manager houses tools at the following locations:

- `<root>:\Control Manager`
- `<root>:\Control Manager\WebUI\download\tools\`

This chapter provides instructions on how to use the following Control Manager tools:

- *Agent Migration Tool (AgentMigrateTool.exe)* on page 7-2
- *Cascading Management Structure Tool (CasTool.exe)* on page 7-2
- *IIS Restoration Tool (SetupPatch.exe)* on page 7-5
- *Web Server and Port Configuration Tool (CMWebCfg.bat)* on page 7-6
- *Using the Control Manager MIB File* on page 7-7
- *Using the NVW 1.x SNMPv2 MIB File* on page 7-7
- *Using the NVW Enforcer SNMPv2 MIB File* on page 7-8
- *Use the NVW System Log Viewer* on page 7-8
- *Use the NVW 1.x Rescue Utility* on page 7-8

## Agent Migration Tool (AgentMigrateTool.exe)

The Agent Migration tool provided in Control Manager 3.5 Standard or Enterprise edition performs two essential functions:

- Generate a Migration List (see *Generate a Migration List* on page 5-14), that identifies all agents used by managed products administered by a Control Manager 2.5, 3.0, or 3.5 server

The migration list, which is saved in \*.xml format, allows you to determine the distribution of different agents on your Control Manager network as well as choose those agents that you will migrate to Control Manager 3.5 servers.

Use this list during a Control Manager remote agent installation to facilitate the replacement of Trend VCS or older Control Manager agents with newer Control Manager agents.

- Migrate agents administered by a Trend VCS 1.8x, Control Manager 2.5x, 3.0, or Control Manager 3.5 server (see *Migrate Trend VCS, Control Manager 2.x, or MCP Agents* on page 5-12)

Run AgentMigrateTool.exe directly on the destination server.

---

**Note:** 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 9-2).

---

## Cascading Management Structure Tool (CasTool.exe)

CasTool.exe is a command-line program that lets you register or unregister a child server.

Use CasTool.exe to balance the load of your Control Manager parent servers and to allow child server unregistration and registration from one parent server to another.

**To run CasTool .exe:**

1. From the Control Manager server, click **Start > Run**.
2. Type `cmd` and then click **OK**.
3. On the Windows command interpreter, go to the Control Manager root directory (for example, `<root>\Program Files\Trend Micro\Control Manager\`).

Refer to `CasTool .exe` commands for the list of commands you can execute.

## CasTool .exe Commands

The following are the commands you can execute using `CasTool .exe`:

COMMAND	USAGE
<code>castool /p:{parent server name:port}</code>	<p>To specify the parent server that the child server will register to.</p> <p>For example:  <code>castool /p:SAGADA_SRV1:2061</code></p> <p>Use <code>/p</code> with other CasTool child server registration commands. Do not use it separately.</p>
<code>castool /n:{parent server user account}</code>	<p>To specify the user account to register a child server to a parent server.</p> <p>{parent server user account} must exist on the parent server and should not be deleted. Otherwise, the child server cannot communicate to the parent server.</p> <p>For example:  <code>castool /n:root</code></p> <p>Trend Micro suggests the use of the parent server root account created during the Control manager installation.</p> <p>Use <code>/n</code> with other CasTool child server registration commands. Do not use it separately.</p>

**TABLE 7-1. CasTool .exe commands**



COMMAND	USAGE
castool /c:"{child server display name}"	<p>To specify the name of the Control Manager child server displayed on the parent server's management console cascading structure tree.</p> <p>{child server display name} can be a maximum of 64 characters and must contain letters, numbers, or the following characters: "_", "-".</p> <p>For example: castool /c:"TOKYO_CHILD1"</p> <p>Use /c with other CasTool child server registration commands. Do not use it separately.</p>
castool /f:"{local directory}"	<p>To specify the location of the public key in the local directory. The directory can be a local folder, mapped drive, or shared network drive. It must be accessible from the child server.</p> <p>For example: castool /f:"c:\e2epublic.dat"</p> <p>Use /f with other CasTool child server registration commands. Do not use it separately.</p>
castool /u	<p>To unregister a child server from the parent server.</p> <p>Use /u with the CasTool debug command.</p>
castool /e	<p>To forcibly unregister a child server from the parent server.</p> <p>Use /e with the CasTool debug command.</p>

TABLE 7-1. CasTool.exe commands

COMMAND	USAGE
castool /s	<p>To specify that an HTTPS connection exists between parent and child server. The command retrieves the E2EPublic.dat key from the parent server.</p> <p>For example:  castool /n:root /p:cm.test.com:8080 /c:"child_01" /s</p> <p>CasTool.exe will use the root account to access https://cm.test.com:8080/download/e2epublic.dat via HTTPS and download the public key from the parent server. It will then register the child server as child_01 in the parent server cascading structure tree.</p> <p>Use /s with CasTool registration commands. Do not use it separately.</p>
castool /d	<p>To enable CasTool.exe debugging.</p> <p>CasTool.exe saves debug logs in &lt;root&gt;:\Program Files\Trend Micro\Control Manager\debuglog folder.</p> <p>Use /d with CasTool registration and unregistration commands. Do not use it separately.</p>

**TABLE 7-1. CasTool.exe commands**

## IIS Restoration Tool (SetupPatch.exe)

Use SetupPatch.exe to restore the Internet Information Server (IIS) settings of the Trend VCS 1.8x or Control Manager 2.5x server. Use this tool if you:

- Made an unsuccessful attempt to upgrade from Trend VCS to Control Manager  
Run this tool to revive Trend VCS functions.
- Migrated from Trend VCS to Control Manager, then removed Trend VCS  
The Trend VCS removal routine modifies the IIS settings and disables Control Manager. Run this tool to restore Control Manager.

**To use SetupPatch.exe:**

1. Using Windows Explorer™, go to the **Tools** folder of the Control Manager installation CD.
2. Double-click **SetupPatch.exe**.
3. Click **Start** to begin the repairs. The tool's user interface shows the modified settings.
4. Click **Exit** to close the program.

---

**Note:** Run SetupPatch.exe on the server where you wish to restore Trend VCS 1.8x or Control Manager 2.5x functions.

---

## Web Server and Port Configuration Tool (CMWebCfg.bat)

Use CMWebCfg.bat to automatically renew the `m_strWebServer_HostName` and `m_uiWebServer_Port` values in `systemconfiguration.xml`. These parameters represent the Web server address and HTTP port that Control Manager uses, which you specified during the Control Manager installation.

**To use CMWebCfg.bat:**

1. From the Control Manager server, click **Start > Run**.
2. Type `cmd` and then click **OK**.
3. On the Windows command interpreter, go to the Control Manager root directory (for example, `<root>\Program Files\Trend Micro\Control Manager\`).
4. Type and run the following command:  
`CMWebCfg {new Web server hostname} {new Web server port}`

Where:

`{new Web server hostname}` is the new Web server IP address or hostname  
`{new Web server port}` is the new Web server port

## Using the Control Manager MIB File

Download and use the Control Manager MIB file with an application (for example, HP™ OpenView) that supports SNMP protocol.

### To use the Control Manager MIB file:

1. Access the Control Manager management console.
2. Click **Administration** on the main menu.
3. On the left-hand menu under Administration, 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.
3. On the left-hand menu under Administration, 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.
3. On the left-hand menu under Administration, 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.

## Use 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. Click **Administration** on the main menu.
3. On the left-hand menu under Administration, click **Tools**.
4. On the working area, click **NVW System Log Viewer**.
5. Using the log viewer, import logs from the Network VirusWall device.

## Use the NVW 1.x Rescue Utility

Uploading 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.



# 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:

- *Remove a Control Manager Server* on page 8-2
- *Remove a Windows-based Control Manager Agent* on page 8-2
- *Manually Removing Control Manager* on page 8-6



## Remove 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 it.

---

**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 re-verify their connection after an 8-hour period

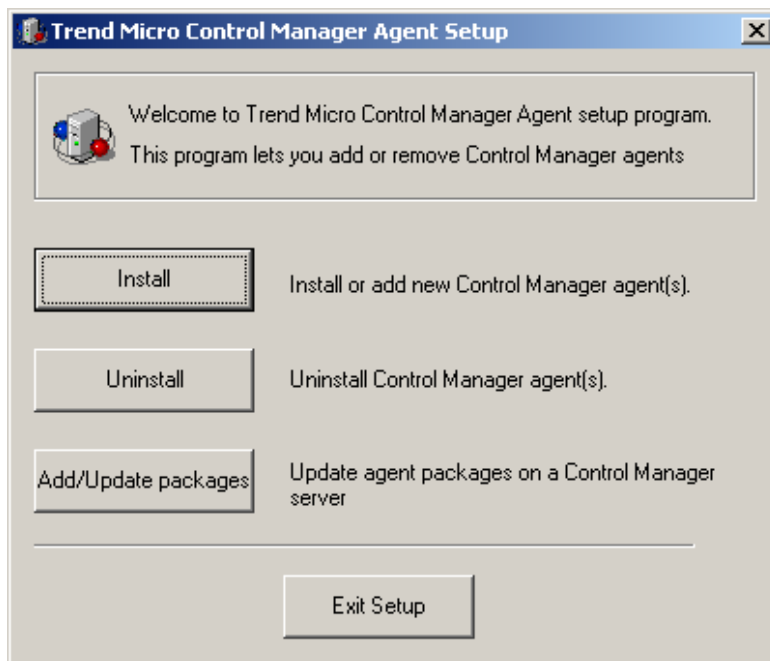
## Remove a Windows-based Control Manager Agent

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 machine.

**To remove a Windows-based Control Manager agent:**

1. On the Control Manager management console main menu, click **Products**.
2. Click **Add/Remove Product Agents**.
3. Click the **Use this** for obtaining, installing, and removing Control Manager agent-update packages link to download the setup package. Save it in any convenient location on your server.
4. Using Microsoft Explorer, go to the location where you saved the agent setup program.
5. Double-click the `RemoteInstall.exe` file. The Control Manager Agent setup screen appears.

**FIGURE 8-1. Trend Micro Agent setup program**

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

7. Click **Next**. The Control Manager source server logon screen appears.



**FIGURE 8-2. Control Manager source server logon**

8. Specify, and provide Administrator-level logon credentials for the Control Manager server that contains the agent package. Type the following information:
  - **Host name**
  - **User name**
  - **Password**
9. Click **Next**. Select the product whose agent to remove from the list box.

10. 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.

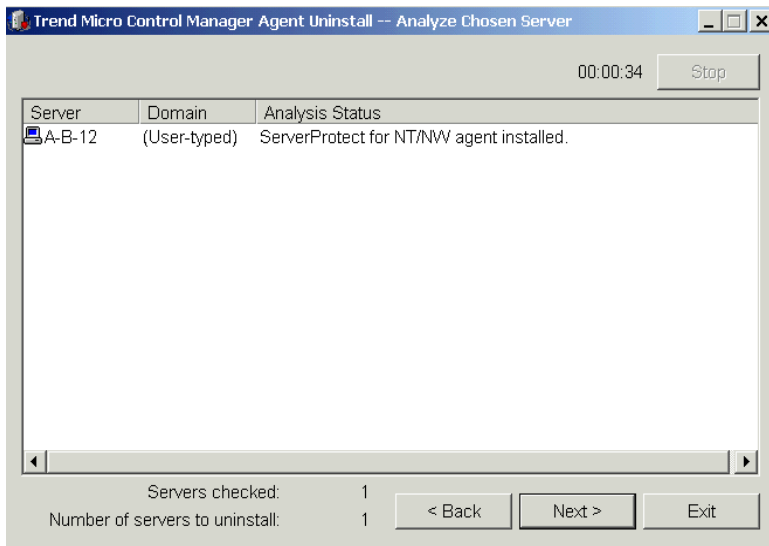
Alternatively, you can double-click on a server to add it to the left list.

**To specify a server name directly:**

- a. Enter 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**.

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



**FIGURE 8-3. Analyze Chosen Control Manager**

14. 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.
15. Click **OK**, and then at the Removing Agents screen, click **Exit**.

## 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 machine, 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. Stop the IIS and Control Manager Services.
2. Remove IIS Settings.
3. Delete Control Manager-related Files/Registry Keys.
4. Remove Crystal Reports.

## Stop the IIS and Control Manager Services

You can perform this action from either the Services screen or the command prompt.

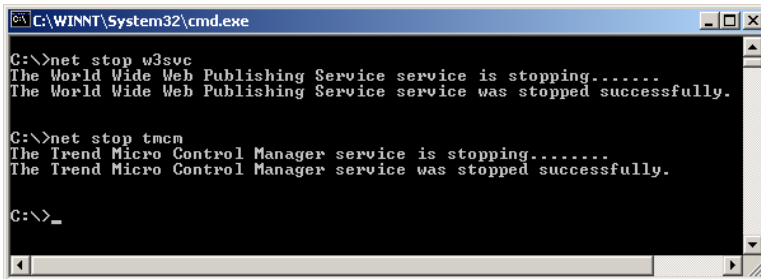
**To stop IIS and Control Manager services from the Services screen:**

1. Click **Start > Programs > Administrative Tools > Services** to open the Services screen.
2. Right-click the following services, and then click **Stop**:
  - IIS Admin Service
  - Trend Micro Control Manager

### 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:\WINNT\System32\cmd.exe

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 8-4.** View of the command line with the necessary services stopped

## Remove IIS Settings

### To remove IIS settings:

1. From the Control Manager server, click **Start > Run**.
2. In the **Open** box, type:  
`%SystemRoot%\System32\mmc.exe %SystemRoot%\System32\Inetsrv\iis.msc`
3. On the left menu, double-click the server name to expand the console tree.
4. Double-click the IIS Web site you set during installation.
5. Delete the following virtual directories:
  - ControlManager
  - TVCSDownload
  - Viewer9
  - TVCS
  - Jakarta
6. Right-click the IIS Web site you set during installation.
7. Click **Properties**.
8. Click the **ISAPI Filter** tab.

**9.** Delete the following ISAPI filters:

- TmcmRedirect
- CCGIRedirect

**10.** Click **OK**.

## Delete Control Manager-related Files/Registry Keys

Delete all files under the Control Manager folder in the following default location:

C:\Program files\Trend Micro\Control Manager

Using Regedit.exe, delete the following keys from the Windows registry:

- HKEY\_LOCAL\_MACHINE\SOFTWARE\TrendMicro\TVCS\...
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TMC
- HKEY\_LOCAL\_MACHINE\SOFTWARE\TrendMicro\TMI\...
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TMI
- HKEY\_LOCAL\_MACHINE\SOFTWARE\TrendMicro\CommonCGI
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\TMC
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro Infrastructure\...
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\TrendCCGI
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro\_NTP

Delete all the Damage Cleanup Services registry keys at the following location:

- HKEY\_LOCAL\_MACHINE\SOFTWARE\TrendMicro\DamageCleanupService\...

## Remove Crystal Reports

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, and then click **Remove**. This automatically removes the Crystal Reports related files.



## Remove the Trend Micro Management Infrastructure

You can manually remove the Trend Micro Management Infrastructure (TMI) — the communication backbone of the Control Manager system — in three steps:

1. Stop the TMI service.
2. Delete TMI-related files.
3. Delete relevant registry keys.

### Stop the TMI Service

You can stop the TMI service from the Services screen or the command prompt.

#### To stop the TMI service from the Services screen:

1. Click **Start > Programs > Administrative Tools > Services** to open the Services screen.
2. Right-click the **Trend Micro Management Infrastructure** service, and then click **Stop**.

#### To stop the TMI service from the command prompt:

Run the following command at the command prompt:

```
net stop "TrendMicro Infrastructure"
```

---

**Note:** You must include the quotation marks in the above command.

---

### Delete TMI-related Files

Delete all files under the TMI folder. By default this is located at:

```
C:\Program files\Trend Micro\COMMON\TMI
```

### Delete Relevant Registry Keys

Using `Regedit .exe`, delete the following keys from the Windows registry:

- HKEY\_LOCAL\_MACHINE\SOFTWARE\TrendMicro\TMI\ . . .
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TMI
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro\Infrastructure\ . . .

## Remove the Common CGI Modules

Manual removal of the Common CGI modules (CCGI) involves the following steps:

1. Stop the IIS and CCGI services.
2. Delete CCGI-related files.
3. Delete relevant registry keys.
4. Remove Windows Installer settings.

## Stop the IIS and CCGI Services

You can stop these services from either the Services screen or the command prompt.

**To stop the IIS and CCGI services from the Services screen:**

1. Click **Start > Programs > Administrative Tools > Services** to open the Services screen.
2. Right-click the following services, and then click **Stop**.
  - IIS Admin Service
  - Trend Micro Common CGI

**To stop IIS and CCGI services from the command prompt:**

Run the following commands at the command prompt:

- `net stop w3svc`
- `net stop TrendCCGI`

## Delete CCGI-related Files

Delete files under the CCGI folder. By default this folder is located at:

```
C:\Program files\Trend Micro\COMMON\ccgi
```

## Delete Relevant Registry Keys

Using `Regedit.exe`, delete the following keys from the Windows registry:

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\CommonCGI`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendCCGI`

## Remove Windows Installer Settings

Use the Windows Installer Cleanup Tool. This tool can be easily obtained from the Microsoft Web site ([www.microsoft.com](http://www.microsoft.com)). Remember to download the tool for Windows NT.

### To remove Windows Installer settings:

1. Run the Windows Installer Cleanup Tool, `Msicuu.exe`.
2. Select **TrendCommonCCGI(All Users)**, and then click **Remove**.

## Remove the Database Components

If you used the Microsoft Data Engine (MSDE) 2000 SP3 for your Control Manager database, you may want to remove it after removing the other components of the Control Manager system.

---

**Note:** If you have upgraded from a previous version of Control Manager, and originally used the MSDE database, then the MSDE database would not have been upgraded to MSDE 2000 SP3.

---

Trend Micro recommends using the Windows Add/Remove programs feature. But if that method is unsuccessful, you can remove MSDE manually as follows:

1. Stop the MSDE service.
2. Stop the SQL Service Manager.
3. Delete MSDE-related files.
4. Delete relevant registry keys.
5. Restart your server.

## Stop the MSDE Service

You can stop the service from either the Services screen or the command prompt.

### To stop the MSDE service from the Services screen:

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

**To stop the MSDE service from the command prompt:**

- Run the following command at the command prompt:

```
net stop MSSQLServer
```

**Stop the SQL Service Manager**

1. Right-click the SQL Server  icon in the Windows tray.
2. Click **Exit**.

**Delete MSDE-related Files**

Remove all files under the Control Manager MSDE folder. By default this folder is located at:

```
C:\Program files\Trend Micro\MSDE2000
```

```
C:\Program files\Trend Micro\MSDE2000MSSQL
```

```
C:\Program files\Microsoft SQL Server
```

**Delete Relevant Registry Keys**

Using `Regedit.exe`, delete the following keys from the Windows registry:

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\MSSQLServer
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Microsoft SQL Server 2000
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\MSSQLServer



# 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 includes the following topics:

- *Before Contacting Technical Support* on page 9-2
- *Contacting Technical Support* on page 9-2
- *TrendLabs™* on page 9-3
- *Other Useful Resources* on page 9-3

## 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](mailto: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 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 in Paris, Munich, Manila, Taipei, Tokyo, and Irvine, CA. ensure a rapid response to any virus outbreak or urgent customer support issue, anywhere in the world.

The TrendLabs modern headquarters, in a major Metro Manila IT park, 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](http://www.trendmicro.com/en/security/trendlabs/overview.htm)

## Other Useful Resources

Trend Micro offers a host of services via its Web site, [www.trendmicro.com](http://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





## System Checklists

Use the checklists in this appendix to record relevant system information as a reference.

### 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	

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
HTTP port		
HTTPS port		
NetBIOS (host) name	yourserver	
SQL-based Control Manager database information		
SQL version	SQL 7.0	
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	
Proxy server for Trend VCS Agent		
IP address	10.1.177.225	
Fully Qualified Domain Name (FQDN)	firewall.company.com	
NetBIOS (host) name	firewall	
SMTP server information (Optional; for email notifications)		
IP address	10.1.123.225	
Fully Qualified Domain Name (FQDN)	mail.company.com	
NetBIOS (host) name	mailserver	
SNMP Trap information (Optional; for SNMP Trap notifications)		

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
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	
MCP UPD heartbeat	10323	
Entity emulator	10329	

---

**Note:** Control Manager requires the exclusive use of ports 10319 and 10198.

---

## Agent Installation Checklist

The following information is used during agent installation.

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
Control Manager server Administrator account User ID	root	
Encryption key location	C:\MyDocuments\E2EPulic.dat	

---

**Note:** You can use any User ID in lieu of the Root account User ID. 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

# Version Comparison Checklist

## Trend Virus Control System and Trend Micro Control Manager Product Features

FEATURES	TVCS	CONTROL MANAGER						
	1.84	2.0	2.1	2.5	3.0 ENT	3.0 STD	3.5 ENT	3.5 STD
Agent interfaces with the Products	●	●	●	●	●	●	●	●
Automatic component (for example, patterns/rules) update	●	●	●	●	●	●	●	●
Cascading management structure					●		●	
Single sign-on (SSO) for managed products which support SSO							●	●
Spyware/grayware detection, reporting, and cleanup							●	●

FEATURES	TVCS	CONTROL MANAGER						
	1.84	2.0	2.1	2.5	3.0 ENT	3.0 STD	3.5 ENT	3.5 STD
Component download granularity							●	●
Configure multiple download sources							●	●
Central database for all virus log and system events	●	●	●	●	●	●	●	●
Centralized, web-based, virus management solution for the enterprise	●	●	●	●	●	●	●	●
Child server monitoring					●		●	
Child server reporting					●		●	
Child server task issuance					●		●	
Command Tracking		●	●	●	●	●	●	●
Communicator Heartbeat		●	●	●	●	●	●	●
Communicator Scheduler		●	●	●	●	●	●	●
Configuration by Group				●	●	●	●	●
Consistent managed product and Control Manager UI				●	●	●	●	●
Damage Cleanup Services					●	●	●	●
Deployment Plans		●	●	●	●	●	●	●
Directory Manager			●	●	●	●	●	●
Enhanced Security Communication	●	●	●	●	●	●	●	●
Event Center		●	●	●	●	●	●	●
Control Manager MIB files (previously called HP OpenView MIB)		●	●	●	●	●	●	●
Improved Navigation			●	●	●	●	●	●

FEATURES	TVCS	CONTROL MANAGER						
	1.84	2.0	2.1	2.5	3.0 ENT	3.0 STD	3.5 ENT	3.5 STD
Improved User Interface			●	●	●	●	●	●
InterScan Web Security Service integration					●	●	●	●
Trend Micro InterScan for Cisco Content Security and Control Security Services Module (ISC CSC SSM) integration							●	●
LDAP for storing Product Tree objects and attributes	●							
Logging Enhancements							●	●
Manage antivirus and content security products	●	●	●	●	●	●	●	●
Manage services					●	●	●	●
Managed product reporting	●			●	●		●	
MDSE or Microsoft SQL 7/2000		●	●	●	●	●	●	●
MSN Messenger notification					●	●	●	●
Notification and Outbreak Alert	●	●	●	●	●	●	●	●
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	●				●		●	



FEATURES	TVCS	CONTROL MANAGER						
	1.84	2.0	2.1	2.5	3.0 ENT	3.0 STD	3.5 ENT	3.5 STD
Remote and Local Agent Installation	●	●	●	●	●	●	●	●
Remote management	●	●	●	●	●	●	●	●
Secure communication between Server and Agents		●	●	●	●	●	●	●
Support HTTPS communication between server, agents, and managed products							●	●
SSL support for ActiveUpdate					●	●	●	●
SSL support for management console					●	●	●	●
Trend Micro Network VirusWall 1200 integration					●	●	●	●
Trend Micro Network VirusWall 2500 integration							●	●
Trend Micro Product Registration server integration					●	●	●	●
TrendLabs Message Board					●	●	●	●
Supports Trend VCS agents	●	●	●	●	●	●	●	●
Support Control Manager agents 2.x agents		●	●	●	●	●	●	●
Support Control Manager agents 3.5 agents							●	●
User Manager			●	●	●	●	●	●
Vulnerability Assessment					●	●	●	●
Work-hour control		●	●	●	●	●	●	●

# Index

## Symbols

"Log on as batch job" policy 6-40

## A

access rights

- Configure 6-12
- Edit Directory 6-12
- Execute 6-12
- setting 6-11
- View 6-11

activating

- Control Manager 3-14, 3-33
- Damage Cleanup Services 3-14–3-15
- Outbreak Prevention Services 3-14–3-15
- services 3-14
- Vulnerability Assessment 3-14–3-15

activating Control Manager 3-35

Activation Code 3-35

Activation Codes 3-14

adding

- user accounts 6-12
- user groups 6-17

address, checklist A-1

Administration Plan 2-8

- centralized management 2-8
- decentralized management 2-8

Administrator's Guide i-x

AG. See Administrator's Guide

agent 4-5

- Control Manager
  - installation 4-12
  - setup program *See RemoteInstall.exe*
- installation 4-6
  - checklist A-4
  - programs 4-7
- InterScan Messaging Security Suite 4-7
- package *See RemoteInstall.xml*
- Trend VCS
  - installation 4-20
  - setup program. *See CMAgentsetup.exe*

Agent Migration Tool 7-2

- migrating agents 7-2

migration list 7-2

AgentMigrateTool.exe. See Agent Migration Tool

agents

- installation tool 4-5
- installing Control Manager 4-3
- NetScreen Firewall 4-25
- obtaining packages 4-9
- obtaining required files 4-7
- preparing for installation 4-4
- remote installation 4-5
- removing Windows-based 8-2
- verifying successful installation 4-27

audience i-xi

## B

back up. See backing up Control Manager 2.5 or 3.0 information

## C

calling CasTool.exe 7-3

cascading management structure

- child servers 6-22
- feature comparison 6-23
- parent server 6-23

Cascading Management Structure Tool 7-2

commands 7-3

/c 7-4

/d 7-5

/f 7-4

/n 7-3

/p 7-3

/s 7-5

cascading structure tree tabs 6-24

CasTool.exe commands 7-3

CasTool.exe. See Cascading Management Structure Tool

CCGI *See Common CGI*

checklist

- agent installation A-4
- ports A-3
- server address A-1

child servers

- configuring 6-23
- managing 6-22
- registering 6-25

- tab 6-24
- unregistering 6-26
- CMAgentSetup.exe 4-6, 4-21
- CMWebCfg.bat 7-6
- CMWebCfg.bat. See Web Server and Port Configuration Tool
- command prompt
  - Common CGI, stopping service from 8-11
  - Control Manager, stopping service from 8-8
  - Trend Micro Management Infrastructure, stopping service from 8-10
- Command Tracking 6-45
  - query and view commands 6-46
- Common CGI
  - command prompt, stopping service from 8-11
  - location, files 8-11
  - registry key 8-11
  - remove 8-11
- comparison
  - cascading management structure 6-23
  - Enterprise edition and Standard edition 1-7
- components
  - downloading 6-28
  - updating out-of-date items 6-43
- configuring
  - child servers 6-23
  - MCP two-way communication 4-28
    - Linux 4-29
  - proxy server connection for component download and Trend VCS agents 6-38
  - scheduled download automatic deployment settings 6-37
  - scheduled download settings 6-36
  - user accounts 6-8
- Control Manager 1-1
  - accounts 6-8
  - activating 3-14, 3-33, 3-35
  - Administrator's Guide i-x
  - agent 1-9
    - installation 4-12
  - antivirus and content security components 6-28
  - architecture 1-8
  - basic features 1-2
  - command prompt, stopping service from 8-8
  - configuring accounts 6-8
  - deployment. See deployment architecture and strategy
  - how many 2-2
  - installation steps 3-10
  - installing 3-1, 3-11
  - installing agents 4-3–4-4
  - latest documentation i-x
  - mail server 1-9
  - managed product 6-19
  - manually removing 8-6
  - migrating database 5-15
  - notifications 6-47
  - PDF documentation i-xi
  - preparing for agent installation 4-4
  - registering 3-14, 3-33
  - remove manually 8-7
  - removing overview 8-1
  - removing server 8-2
  - removing Windows-based agent 8-2
  - report server 1-9
  - report types 6-51
  - reports 6-51
  - security levels 3-18, 3-21
  - server 1-8
  - SQL database 1-8
  - system requirements 3-2, 4-2
  - test deployment. See test deployment
  - Trend Micro Infrastructure 1-9
  - Trend Micro Management Communication Protocol 1-9
  - understanding remote installation 4-5
  - updating 6-28
  - verifying agent installation 4-27
  - verifying installation 3-32
  - Web server 1-9
  - Web-based management console 1-10
  - where to install 2-14
- Control Manager 2.5x agent migration flow 5-11
- Control Manager 3.5 agent migration flow 5-12
- Control Manager agent for NetScreen Firewall 4-25
  - Certificate Name 4-26
    - determine Certificate Name 4-26
    - installing the agent 4-26
- Control Manager agents 4-3
- convention

- document i-xii
- creating
  - deployment plans 6-42
  - user groups 6-17
  - users 6-12
- D**
- Damage Cleanup Services
  - activating 3-14–3-15
- database recommendations 2-7
- deleting
  - user accounts 6-17
  - user groups 6-18
- deploying 6-41
  - deployment plans 6-41
  - sample 6-42
- deployment architecture and strategy 2-10
  - multiple-site deployment 2-12
  - multi-site deployment 2-12
  - single-server deployment 2-10
  - single-site deployment 2-10
- deployment plan
  - creating 6-42
  - default plans 6-42
- Directory Manager 6-22
  - grouping managed products 6-22
- disable notifications 6-48
- disabling
  - user accounts 6-16
- documentation i-ix
- downloading
  - enable HTTPS 6-38
  - enable UNC 6-39
  - set proxy server settings 6-38
- downloading and deploying components 6-28
- downloading components
  - manually 6-29
  - scheduled download 6-32
- E**
- E2EPublic.dat *See encryption key*
- editing
  - user accounts 6-15
  - user groups 6-18
- email 6-47
- enable notifications 6-48
- encryption key
  - agent, installation 4-20
  - obtaining 4-7
  - obtaining the 4-7
  - purpose 4-7
- enterprise
  - multiple site 2-2
  - single-site 2-2
- Enterprise edition
  - features 1-7
- Event Center 6-46
  - Alert 6-46
  - Damage Cleanup Services 6-47
  - Outbreak Prevention Services 6-46
  - Statistics 6-47
  - Unusual 6-47
  - Update 6-47
  - Vulnerability Assessment 6-47
- F**
- flow
  - migrating Control Manager 2.5x agent 5-11
  - migrating Control Manager 3.5 agent 5-12
  - migrating Trend VCS 1.8x agent 5-11
- G**
- generating on-demand scheduled reports 6-55
- global reports 6-51
- grouping managed products or child servers 2-13
- H**
- how many
  - Control Manager servers 2-2
- HTTPS
  - enable HTTPS download 6-38
- I**
- IIS Restoration Tool 7-5
  - using SetupPatch.exe 7-6
- initializing CasTool.exe. *See calling CasTool.exe*
- Insatllation Guide
  - about i-xi
- installation
  - agent
    - Control Manager 4-12

- InterScan Messaging Security Suite 5.1 4-25
- Trend VCS agent 4-20
- installing
  - Control Manager 3-1, 3-11
  - Control Manager agents 4-3
  - MCP agents 4-4
  - steps 3-10
  - TVCS and Control Manager 2.x agents 4-1
  - verifying Control Manager server 3-32

## K

- Knowledge Base i-ix
  - URL i-ix

## L

- local reports 6-51
- location
  - Common CGI files 8-11
  - Microsoft Data Engine files 8-13
  - Trend Micro Management Infrastructure files 8-10

## M

- managed products 6-19
  - configuring 6-19
  - default folder 6-21
  - tabs 6-21
  - using the Product Directory 6-19
- Management Communication Protocol
  - see MCP 1-3
- management console
  - access HTTPS 6-7
- manual
  - remove
    - Common CGI 8-11
    - MSDE 8-12
    - Trend Management Infrastructure 8-10
- manually
  - remove Control Manager 8-7
- manually uninstalling 8-6
- MCP
  - about 1-3
  - configuring two-way communication 4-28
    - Linux 4-29
  - one-way communication 1-6
  - two-way communication 1-6
  - verifying connection method 4-29

- MCP agents 4-3
  - installing 4-4
- MCP and Control Manager
  - communication 4-29
- MIB file
  - Control Manager 7-7
  - NVW 1.x SNMPv2 7-7
  - NVW Enforcer SNMPv2 7-8
- MIBs browser 6-47
- Microsoft
  - Data Engine
    - location, files 8-13
- migrating 5-8
  - Control Manager 2.5x agent migration flow 5-11
  - Control Manager 3.5 agent migration flow 5-12
  - Control Manager SQL 2000 5-15
    - database 5-15
    - different servers/agents 5-11
    - generate a migration list 5-14
    - phased upgrade 5-9
    - rapid upgrade 5-8
    - scenarios 5-11
    - single-server migration 5-11
    - steps 5-12
    - strategy 5-8
    - Trend VCS 1.8x agent migration flow 5-11
  - migration list 5-14
- minimum system requirements 3-2
- monitoring
  - security level 6-45
  - system information 6-44
- monitoring the Control Manager environment 6-44
- MSDE 2000 i-viii

## N

- NetScreen Firewall 4-25
- network traffic
  - plan 2-2
  - source
    - log traffic 2-3
    - logs 2-3
    - Product registration traffic 2-5
    - Trend Micro Management Infrastructure policies 2-4
  - sources 2-3

- traffic frequency 2-5
- notifications 6-47
  - configure recipients 6-49
  - configuring 6-48
  - enabling or disabling 6-48
  - special spyware/grayware alert settings 6-51
  - special virus alert settings 6-50
  - test notification delivery 6-49
  - virus outbreak alert settings 6-50
- NVW 1.x Rescue Utility 7-8
- NVW System Log Viewer 7-8
- O**
- obtaining
  - agent packages 4-9
  - encryption key 4-7
- ODBC
  - drivers 2-7
  - settings, Control Manager 8-12
- off-hour period 2-5
- OfficeScan
  - Trend VCS agent for 4-21
- on-demand scheduled reports 6-55
- one-way communication 1-6
- online help i-ix
- Outbreak Prevention Services i-viii
  - activating 3-14–3-15
- P**
- pager 6-47
- parent and child server feature comparison 6-23
- parent server 6-23
- performance, penalty 2-2
- phased upgrade 5-9
- plan
  - administration 2-8
  - data storage 2-6
  - network traffic 2-2
  - server distribution 3-2
- port
  - checklist A-3
- preface i-i
- preparing
  - Control Manager agent installation 4-4
- Product Directory tabs 6-21
- profiles. See report profiles
- proxy server
  - communicating with Trend VCS agents 3-26
  - connecting to the Internet 3-25
- proxy settings 6-38
- public encryption key 4-7–4-8
- Q**
- querying commands 6-46
- R**
- rapid upgrade 5-8
- readme file i-ix
- recommended system requirements 3-4
- register online 3-14
- registering
  - Control Manager 3-14, 3-33
- registering a child server 6-25
- Registration Key 3-15, 3-35
- registry key
  - Common CGI 8-11
  - Microsoft Data Engine 8-13
  - Trend Micro Management Infrastructure 8-10
- Remote Agent Setup tool 4-12
- RemoteInstall.exe 4-5, 4-12
- RemoteInstall.xml 4-10
- remove
  - manual
    - Control Manager 8-7
    - Microsoft Data Engine 8-12
    - Trend Management Infrastructure 8-10
- removing
  - Control Manager manually 8-6
  - Control Manager server 8-2
  - Control Manager Windows-based agent 8-2
- renew product maintenance 3-36
- reports 6-51
  - global 6-51
  - local 6-51
  - on-demand scheduled 6-55
- report profiles 6-52
  - ActiveX 6-52
  - Contents 6-53
  - creating 6-52
  - Frequency 6-54

- PDF 6-52
- Recipient 6-55
- RPT 6-52
- RTF 6-52
- Targets 6-53
  - viewing generated reports 6-56
- rolling back
  - to Control Manager 2.5 or 3.0 server 5-7
  - to Trend VCS 1.8x server 5-6
- root account 6-10
- root-level share 4-22
- running SetupPatch.exe. See using SetupPatch.exe

## S

- scheduled component download 6-33
- scheduled reports 6-55
- security levels 3-20
- server
  - address, checklist A-1
- server distribution plan 2-2
- setting
  - access rights 6-11
- setting "Log on as batch job" policy 6-40
- SetupPatch.exe. See IIS Restoration Tool
- single-sign on 1-6
- sizing recommendations 3-5
- Small Network Management Protocol. See SNMP
- SNMP 6-47
- SolutionBank-see Knowledge Base i-ix
- SQL
  - Service Manager 8-13
- SSO
  - see single-sign on 1-6
- Standard edition
  - features 1-7
- support operating systems
  - Control Manager agents 3-2
  - Control Manager server 3-2
- system requirements 3-2, 4-2
  - minimum 3-2
  - recommendations 3-5
  - recommended 3-4

## T

- tabs

- cascading structure tree 6-24
- Product Directory 6-21
- test deployment 2-16
  - tasks 2-16
- TMI 2-5
- TMI See *Trend Micro Management Infrastructure*
- tool
  - AgentMigrateTool.exe 7-2
  - CasTool.exe 7-2
  - CMWebCfg.bat 7-6
  - Control Manager MIB file 7-7
  - NVW 1.x Rescue Utility 7-8
  - NVW 1.x SNMPv2 MIB file 7-7
  - NVW Enforcer SNMPv2 MIB file 7-8
  - NVW System Log Viewer 7-8
  - SetupPatch.exe 7-5
- traffic plan
  - network 2-2
  - network sources 2-3
- traffic, network 2-2
- Trend Micro Management Infrastructure 2-6
  - command prompt, stopping service from 8-10
  - location, files 8-10
  - registry key 8-10
  - remove 8-10
- Trend VCS
  - agent
    - installation 4-20
- Trend VCS 1.8x agent migration flow 5-11
- Trend VCS agents 4-3
- Trigger Application 6-47
- TVCS and Control Manager 2.x agents
  - installing 4-1
- two-way communication 1-6

## U

- UNC 6-39
- understanding
  - Control Manager remote installation 4-5
- unregistering a child server 6-26
- Update Manager 6-28
- updating components 6-28, 6-43
- upgrading 5-2
  - backing up Control Manager 2.5 or 3.0 information 5-4

- considerations 5-2
- Control Manager 2.5 or 3.0 servers 5-3
- Trend VCS 1.8x servers 5-3
- URLs
  - Knowledge Base i-ix
- user accounts
  - adding 6-12
  - deleting 6-17
  - disabling 6-16
  - editing 6-15
- user groups
  - adding 6-17
  - deleting 6-18
  - editing 6-18
- User Manager 6-11
- users
  - adding accounts 6-12
  - adding groups 6-17
  - deleting accounts 6-17
  - deleting groups 6-18
  - disabling accounts 6-16
  - editing accounts 6-15
  - editing groups 6-18
- V**
- verifying
  - agent installation 4-27
  - Control Manager server installation 3-32
  - MCP communication 4-29
- version
  - agent package 4-11
- viewing commands 6-46
- viewing generated reports 6-56
- Vulnerability Assessment
  - activating 3-14–3-15

**W**

- who should read this document
  - audience i-xi
- Windows event log 6-47
- work-hour policy 2-4
- World Virus Tracking 3-16



