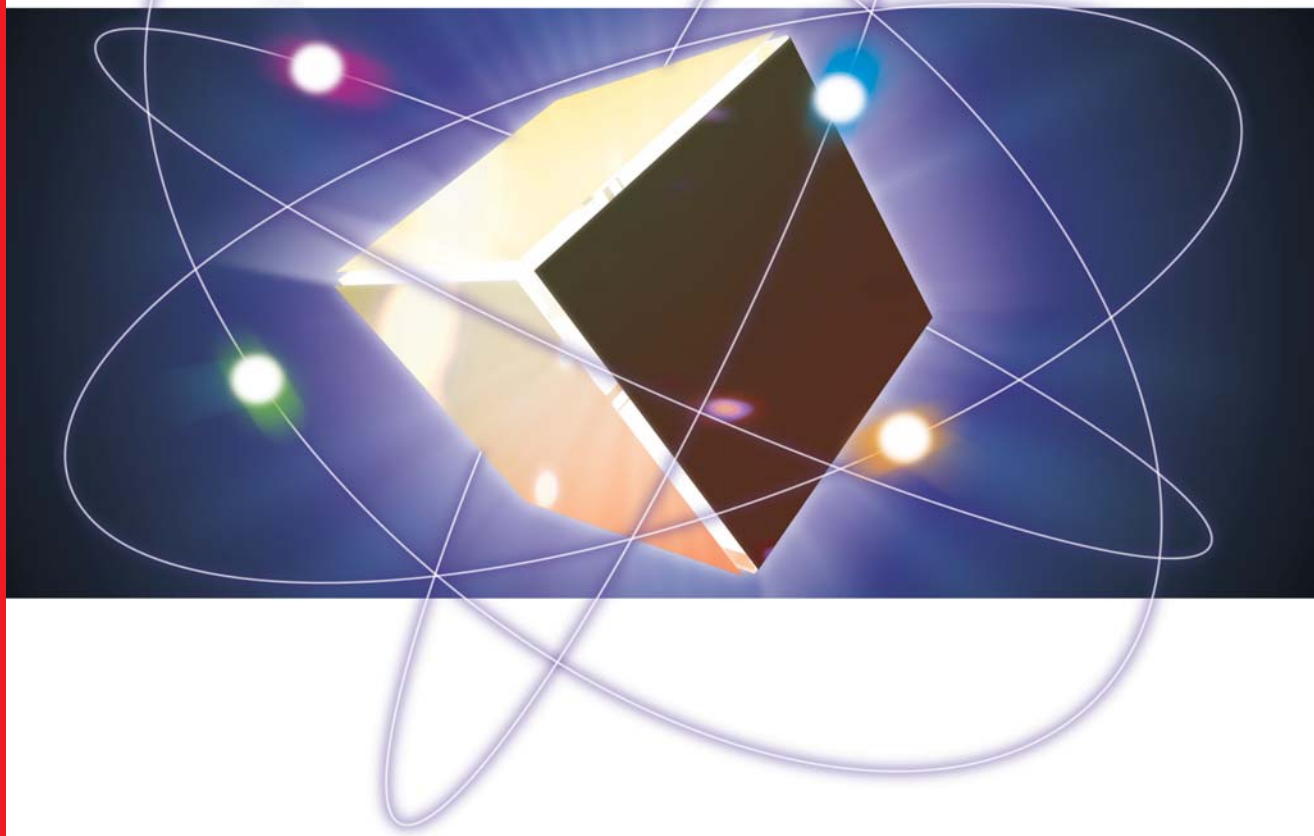
TREND MICRO
Control Manager™ 3

Enterprise Virus Outbreak and Content Security Management

Administrator's Guide



TREND MICRO™

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

www.trendmicro.com/download/documentation/

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

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. CMEM32570/51128

Release Date: March 2006

The Getting Started 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 12-2 for technical support information and contact details. Detailed information about how to use specific features within the software are available in the online help file and online Knowledge Base at Trend Micro's Web site.

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

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

Contents

Preface

What's New in This Version 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..... vi
Secure Sockets Layer (SSL) Support Management Console and ActiveUpdate vii
Increased Managed Product Support..... vii
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 Administrator's Guide x
Audience xi
Document Conventions..... xi

Chapter 1: Introducing Trend Micro Control Manager™

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 1-5
One-way Communication 1-6
Two-way Communication 1-6
Single Sign-on (SSO) Support 1-6
Cluster Node Support 1-6
Control Manager Standard and Enterprise Editions 1-7
Control Manager Architecture 1-9

Chapter 2: Planning and Implementing the Control Manager Deployment

Identifying Deployment Architecture and Strategy 2-2
Understanding Single-Site Deployment 2-2
Understanding Multiple-Site Deployment 2-5
Installation Flow 2-9
Supported Operating Systems 2-9
Compatible Antivirus and Content Security Products 2-11
Testing Control Manager at One Location 2-13
Server Distribution Plan 2-15
Understanding Administration Models 2-15
Understanding Control Manager Server Distribution 2-16
Single-Server Topology 2-16
Multiple-Server Topology 2-16
Network Traffic Plan 2-17
Understanding Control Manager Network Traffic 2-17
Sources of Network Traffic 2-17
Traffic Frequency 2-17
Logs 2-17
Trend Micro Management Infrastructure Heartbeat 2-18
File Sizes 2-18
Updating the ScanMail and InterScan Family of Products 2-20
Updating the eManager Family of Products 2-21
Updating OfficeScan Corporate Edition and ServerProtect 2-21
Protocols 2-21
Sources of Network Traffic 2-22
Log Traffic 2-22

Trend Micro Management Infrastructure Policies 2-23
Trend Micro Management Communication Protocol Policies 2-23
Product Registration Traffic 2-24
Deploying Updates 2-24
Understanding Deployment Updates 2-24
About ScanMail and InterScan Family of Product Updates 2-25
About the eManager Family of Product Updates 2-26
About OfficeScan Corporate Edition and ServerProtect Updates 2-26
Data Storage Plan 2-27
Understanding Control Manager Data Storage 2-28
Database Recommendations 2-28
ODBC Drivers 2-28
Authentication 2-28
Web Server Plan 2-29
Web Server Configuration 2-29

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

System Requirements 3-2
Minimum System Requirements 3-2
Recommended System Requirements 3-3
Installing a Control Manager Server 3-8
Verifying Successful Installations 3-31
Verify a Successful Control Manager Server Installation 3-31
Post-installation Configuration 3-32
Register and Activate Control Manager 3-32
Configure User Accounts 3-32
Download the Latest Components 3-33
Set Notifications 3-33
Registering and Activating Your Software 3-33
Activate Control Manager 3-34
Convert to the Full Version 3-34
Renew Your Product Maintenance 3-35

Chapter 4: Installing Control Manager Agents

About Control Manager Agents 4-2
Prepare for Control Manager Agent Installation 4-3
Understanding Control Manager Agent Remote Installation 4-4
RemoteInstall.exe 4-5
CMAgentSetup.exe 4-5
Performing the Installation 4-5
Step One: Obtain Required Files 4-6
Step Two: Obtain Agent Packages (Optional) 4-7
Step Three: Install the Agents 4-10
Install Windows-Based Agents 4-11
Installing Control Manager Agents with the Remote Agent SetupTool 4-14
Installing Trend VCS Agents 4-22
Installing Control Manager Agents for InterScan Messaging Security Suite 5.1 for Windows 4-27
Install the Trend VCS Agent for OfficeScan Corporate Edition 4-27
Installing the Trend VCS Agent on Remote OfficeScan Servers 4-28
Change Agent Logon Credentials for Remote OfficeScan Servers 4-30
Installing the Trend VCS Agent Locally 4-31
Change Agent Logon Credentials for its Host Server 4-33
Install Control Manager Agent for InterScan VirusWall for UNIX 4-34
Registering the InterScan VirusWall Agent with a Control Manager Server 4-34
Install Trend VCS Agent for ScanMail for Lotus Notes 4-35
Signing the ScanMail Databases 4-35
Setting Agent Restrictions 4-36
Enabling the ScanMail Agent 4-36
Install the Control Manager Agent for NetScreen™ Firewall 4-37
Verify a Successful Agent Installation 4-39

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 5-7
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 5-12
Control Manager 2.5x Agent Migration Flow 5-13
MCP Agent Migration Flow 5-13
Migrate Trend VCS, Control Manager 2.x, and MCP Agents 5-14
Generate a Migration List 5-16
Migrate the Control Manager Database 5-16
Migrate Control Manager SQL 2000 Database to Another SQL 2000 Server 5-17

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
Log Off from the Management Console 6-7
Configure Control Manager User Accounts and Groups 6-8
Additional Root Account Privileges 6-10
Understanding the User Manager 6-10
Setting Access Rights 6-11
View 6-11
Execute 6-11
Configure 6-11
Edit Directory 6-12
Add a User Account 6-12

Import Active Directory Users 6-16
Edit a User Account 6-18
Disable a User Account 6-19
Delete a User Account 6-19
Add a User Group 6-20
Edit a User Group 6-22
Delete a User Group 6-23
Administer Managed Products 6-23
Configure Managed Products Using the Product Directory 6-23
Default Folder for Managed Products 6-25
Use the Product Directory Tabs 6-26
Group Managed Products Using Directory Manager 6-26
Manage Child Servers 6-27
Configure Child Server Using the Cascading Structure Tree 6-28
Use the Cascading Structure Tree Tabs 6-28
Registering or Unregistering Child Servers 6-29
Download and Deploy New Components 6-32
Understanding Update Manager 6-36
Understanding Manual Downloads 6-36
Manually Download Components 6-37
Configure Scheduled Download Exceptions 6-46
Understanding Scheduled Downloads 6-47
Configure Scheduled Downloads and Enable Scheduled Component Downloads 6-47
Configure Scheduled Download Settings 6-54
Configure Scheduled Download Automatic Deployment Settings 6-55
Configure System Settings 6-56
Configure Proxy Server Connection for Component Download and Trend VCS Agents 6-59
Enable HTTPS Download 6-59
Enable UNC Download 6-60
Set "Log on as batch job" Policy 6-60

Chapter 7: Monitoring the Control Manager Network

View Summary Screens in Control Manager 7-2
Use Command Tracking 7-4
Understanding Command Details 7-5
Details for the Individual Products or Services 7-6
Query and View Commands Issued in the Past 24 Hours 7-6
Use Event Center 7-9
Customizing Notification Messages 7-11
Enable or Disable Notifications 7-14
Configure Notification Method 7-15
Configure Notification Recipients and Test Notification Delivery 7-16
Configure Virus Outbreak Alert Settings 7-18
Configure Special Spyware/Grayware Alert Settings 7-18
Configure Special Virus Alert Settings 7-19
Configure Network Virus Alert Settings 7-20
Configure Potential Vulnerability Attack Detected Settings 7-21
Work With Logs 7-22
Server Logs 7-22
Client Logs 7-22
Open Access Log and Server Event Logs 7-25
Query Access or Server Event Logs 7-27
Save Logs to a *.CSV file 7-28
Open <log type> (Purge Settings) 7-28
Configure Purge Log Settings 7-29
Use Reports 7-30
Local Reports 7-30
Global Reports 7-30
Understanding Report Templates 7-31
Understanding Report Profiles 7-37
Create Report Profiles 7-37
Review Report Profile Settings 7-43
Enable Scheduled Report Profiles 7-44
Disable Scheduled Report Profiles 7-44
Modify Scheduled Report Profiles 7-44
Delete Report Profiles 7-45

Generate On-demand Scheduled Reports 7-45
View Generated Reports 7-46
Delete Reports 7-46

Chapter 8: Administering Managed Products

Understanding Communicators 8-2
Understanding Agents 8-3
Understanding Managed Products, Communicators, and Child Servers Connection Status Icons 8-5
Understanding the Control Manager Security Levels 8-6
Understanding the Connections Tree 8-8
Using Communicator Scheduler 8-9
Using Communicator Heartbeat 8-9
MCP Heartbeat 8-10
Using the Schedule Bar 8-11
Determining the Right Heartbeat Setting 8-12
Access Communicators 8-12
View Communicators Connection Status Details 8-12
View Communicators and Communicators Status 8-13
Access Communicator Scheduler 8-14
Set Communicator Schedules 8-14
Modify the Default Communicator Schedule 8-15
Access Communicator Heartbeat 8-15
Set Communicator Heartbeat 8-15
Restart Control Manager Services 8-16
Modify the Control Manager External Communication Port 8-16
Modify the Security Level 8-18
Modify the Communicator Heartbeat Protocol 8-18
Configure MCP for Two-way Communication 8-19
Verify the Communication Method Between MCP and Control Manager 8-21
Understanding Managed Products 8-22
Understanding Product Directory 8-22
Accessing a Managed Product's Default Folder 8-23
Access Product Directory 8-24
Manually Deploy New Components Using the Product Directory 8-25

View Managed Products Status Summaries 8-25
Configure Managed Products 8-26
Issue Tasks to Managed Products 8-27
Query and View Managed Product Logs 8-28
Recover Managed Products Removed From the Product Directory 8-29
Change Agent Connection Re-Verification Frequency 8-30
Search for Managed Products, Product Directory Folders or Computers 8-31
Refresh the Product Directory 8-32
Understanding Directory Manager 8-32
Using the Directory Manager Options 8-33
Access Directory Manager 8-33
Create Folders 8-34
Renaming Folders or Managed Products 8-34
Move Folders or Managed Products 8-34
Delete User-Defined Folders 8-35
Understanding Temp 8-36
Using Temp 8-36
Access Temp 8-36
Adding Managed Products to Temp 8-36
Removing Managed Products from Temp 8-38
Managing Third Party Products 8-39
Understanding the Control Manager Agent for NetScreen™ Firewall 8-39
Install the Control Manager Agent for NetScreen™ Firewall 8-40
Updating NetScreen-Global PRO Settings 8-41
Managing Child Servers 8-42
Understanding the Parent Server and Child Server Communication 8-44
Registering or Unregistering Child Servers 8-45
Using CasTool.exe Commands 8-46
Use CasTool.exe 8-48
Register a Child Server 8-48
Unregister a Child Server 8-49

Debug CasTool.exe 8-50
Access the Cascading Structure Tree 8-51
View the Cascading Structure Status Summaries 8-51
Configure Log Upload Settings 8-52
Enable or Disable Child Server Connection 8-53
Issue a Task to Child Servers 8-54
Query and View Child Server Logs 8-54
View Child Server Reports 8-56
Refresh the Cascading Tree 8-57
Renaming a Child Server Alias 8-57
Recover Child Servers Accidentally Removed from the Cascading Manager 8-58
Understanding the Control Manager Database 8-58
Understanding the db_ControlManager Tables 8-59
Backing Up db_ControlManager Using osql 8-62
Restore Backup db_ControlManager Using osql 8-63
Backing Up db_ControlManager Using the SQL Server Enterprise Manager 8-64
Restore backup db_ControlManager Using SQL Server Enterprise Manager 8-65
Shrink db_controlmanager_log.ldf Using SQL Server Enterprise Manager 8-66
Shrink db_ControlManager.mdf and db_ControlManager.ldf Using SQL Commands 8-67

Chapter 9: Using Trend Micro Services

Understanding Trend Micro Services 9-2
Understanding Enterprise Protection Strategy (EPS) 9-3
Highlighting the Value of EPS 9-4
Introducing TrendLabs Message Board 9-5
Participating in the World Virus Tracking Program 9-5
Introducing Outbreak Prevention Services 9-6
Understanding Outbreak Prevention Services 9-6
Benefits of Outbreak Prevention Services 9-7
Activate Outbreak Prevention Services 9-7
View Outbreak Prevention Services Status 9-8

Preventing Virus Outbreaks and Understanding the Outbreak Prevention Mode 9-9
Understanding Outbreak Prevention Policies 9-10
Access the Outbreak Prevention Services Settings Screen 9-10
Update Outbreak Prevention Policies 9-11
Start Outbreak Prevention Mode 9-12
Edit an Outbreak Prevention Policy 9-13
Set Automatic Outbreak Prevention Mode 9-14
Configure Outbreak Prevention Mode Download Settings 9-16
Stop Outbreak Prevention Mode 9-16
View Outbreak Prevention Mode History 9-17
Outbreak Prevention Mode Tutorial 9-18
Outbreak Prevention Mode Introduction 9-18
What is the Threat? - Identifying the Source of the Outbreak 9-18
What Can My System Do Now? - Evaluating Existing Policies 9-19
Virus Covered by Existing Policies 9-19
Virus Not Covered by Existing Policies 9-20
How Do I Protect My System? 9-20
What Follow-Up Procedures Should I Use? 9-22
Using Vulnerability Assessment 9-22
Possible Actions 9-23
Available Details 9-24
Performing a Vulnerability Assessment 9-25
Features and Benefits of Vulnerability Assessment 9-26
Four Main Stages of the Vulnerability Assessment Process 9-26
Activating Vulnerability Assessment 9-29
Downloading Updates 9-29
Configuring Vulnerability Assessment 9-30
Running a Vulnerability Assessment Task 9-31
View Current Task 9-31
Run a Task Now 9-33

Run a Scheduled Task 9-33
Viewing Results 9-34
Understanding Results 9-35
What do the Results Mean? 9-35
What is a Vulnerability? 9-35
What is the Security Risk? 9-35
Resolving Security Risks 9-36
Maintaining Network Security 9-37
Understanding Enforcement 9-38
Understanding Manual Assessment 9-39
Using the Manual Vulnerability Assessment Tool 9-40
Using the Network VirusWall Manual Assessment Page 9-41
View Security Summary 9-42
Search for a Machine 9-43
Select Machines 9-44
Create a Task 9-46
Edit a Task 9-50
Delete a Task 9-54
Set Task Actions 9-54
Enable Damage Cleanup Services for a Vulnerability Assessment Task 9-56
Set Global Enforcements and Exceptions 9-57
View Tasks 9-60
View a Current Task 9-61
Use the Vulnerability Assessment History 9-63
View Task History 9-64
View Result Summary 9-67
Result Summary Actions 9-68
Viewing the Top Ten Vulnerabilities 9-69
View Machine Status 9-69
Create a query 9-71
View Query Results 9-72
Generate Comparative Reports 9-72
View Comparative Reports Results 9-73
Account Management Tool Tutorial 9-74

Chapter 10: Using Control Manager Tools

Agent Migration Tool (AgentMigrateTool.exe) 10-2
Cascading Management Structure Tool (CasTool.exe) 10-2
CasTool.exe Commands 10-3
IIS Restoration Tool (SetupPatch.exe) 10-5
Web Server and Port Configuration Tool (CMWebCfg.bat) 10-6
Using the Control Manager MIB File 10-7
Using the NVW 1.x SNMPv2 MIB File 10-7
Using the NVW Enforcer SNMPv2 MIB File 10-8
Use the NVW System Log Viewer 10-8
Use the NVW 1.x Rescue Utility 10-8

Chapter 11: Removing Trend Micro Control Manager

Remove a Control Manager Server 11-2
Remove a Windows-Based Control Manager Agent 11-2
Manually Removing Control Manager 11-6
Remove the Control Manager Application 11-7
Stop the IIS and Control Manager Services 11-7
Remove IIS Settings 11-8
Delete Control Manager-related Files/Registry Keys 11-8
Remove Crystal Reports 11-9
Remove the Trend Micro Management Infrastructure 11-9
Stop the TMI Service 11-9
Delete TMI-related files 11-10
Delete relevant registry keys 11-10
Remove the Common CGI modules 11-10
Stop the IIS and CCGI services 11-10
Delete CCGI-related files 11-11
Delete Relevant registry keys 11-11
Remove Windows Installer Settings 11-11
Remove the Database Components 11-11
Stop the MSDE Service 11-12
Stop the SQL Service Manager 11-12
Delete MSDE-related Files 11-12
Delete Relevant Registry Keys 11-13

Chapter 12: Getting Support

Before Contacting Technical Support 12-2
Contacting Technical Support 12-2
TrendLabs™ 12-3
Other Useful Resources 12-3

Chapter 13: Troubleshooting and FAQs

Troubleshooting 13-2
General Troubleshooting 13-2
Troubleshooting MCP 13-14
Troubleshooting Reporting 13-15
Troubleshooting the Cascading Environment 13-15
Troubleshooting Installation 13-17
Troubleshooting Update Manager 13-19
FAQs 13-21
General FAQs 13-21
Directory Manager FAQs 13-24
Active Directory Accounts FAQs 13-25
Reporting FAQs 13-25
Agent Migration Tool FAQs 13-26
Update and Deploy Components FAQs 13-27
Product Registration FAQs 13-28
Installation FAQs 13-28

Appendix A: Appendix

System Checklists A-1
Server Address Checklist A-1
Ports Checklist A-3
Agent installation checklist A-4
Control Manager Conventions A-5
Control Manager Core Process and Configuration Files A-5
Control Manager Communication and Listening Ports A-7
Trend Virus Control System and Trend Micro
Control Manager Product Features A-8

Index

Preface

This Administrator's Guide introduces Trend Micro Control Manager™ 3.5, guides you through the installation planning and steps, and walks you through 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 Administrator's Guide* on page x
- *Audience* on page xi
- *Document Conventions* on page xi

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 7-9).

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. TMCM 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
Online Help	Web-based documentation that is accessible from the Control Manager™ management console. The online help contains explanations of Control Manager™ components and features, as well as procedures needed to configure Control Manager.
Knowledge Base	The Knowledge Base is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following Web site: *http://esupport.trendmicro.com/support*
Readme file	The Readme file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues and product release history.
Installation Guide	Printed documentation provided in the package contents and PDF form that is accessible from the Trend Micro Enterprise CD or downloadable from the Trend Micro Web site. The Installation Guide contains detailed instructions of how to install Control Manager and configure basic settings to get you "up and running".
Administrator's Guide	PDF documentation that is accessible from the Trend Micro Solutions CD for Control Manager™ or downloadable from the Trend Micro Web site. 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. See *About this Administrator's Guide* for a summary of the chapters available in this book.

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 Administrator's Guide

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

TASK	DESCRIPTION
Pre-Installation	**Chapter 1:** Provides an overview of the Control Manager, product architecture, and a description of all features
	Chapter 2: Provides deployment and product application information and Trend Micro recommendations on the optimal deployment of Network VirusWall 300 devices
Installation	**Chapter 3:** Provides first-time installation procedures for Control Manager 3.5 server
	Chapter 4: Provides installation procedures for older Control Manager agents
	Chapter 5: Provides information and procedures for upgrading to Control Manager 3.5 from previous versions
Post Installation	**Chapter 6:** Provides information on basic Web console navigation, creating and importing users, updating the server and managed products
	Chapter 7: Provides information on interpreting and monitoring the Control Manager environment, such as, configuring notifications, generating reports, and collecting logs
	Chapter 8: Provides information on managing the Control Manager network and managed products
	Chapter 9: Provides information on using Control Manager services, such as, EPS, OPS, and Vulnerability Assessment
	Chapter 10: Provides information on using Control Manager tools, such as, Agent Migration tool and Cascading Management Structure Tool
	Chapter 11: Provides information on removing Control Manager from your computer
	Chapter 12: Provides information about contacting Trend Micro if you have questions or need support
	Chapter 13: Provides information for troubleshooting on issues encountered using Control Manager 3.5
Appendices	• *System Checklists*

TABLE PREFACE-3. Administrator's 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 Getting Started Guide) uses the following conventions.

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

TABLE PREFACE-4. Control Manager Documentation Conventions

Chapter 1

Introducing Trend Micro Control Manager™

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 Standard and Enterprise Editions* on page 1-7
- *Control Manager Architecture* on page 1-9

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.

FEATURE	DESCRIPTION
Centralized configuration	Using the Product Directory and cascading management structure, these functions allow you to coordinate virus-response and content security efforts from a single management console This helps ensure consistent enforcement of your organization's virus 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

TABLE 1-1. Control Manager Features

FEATURE	DESCRIPTION
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.

TABLE 1-1. Control Manager Features

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 new features:

- Reduced network loading and package size
- NAT and firewall traversal support
- HTTPS support
- One-way and two-way communication support
- Single sign-on (SSO) support
- 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 data types are integer, unsigned integer, Boolean, and floating point.
- **Faster parsing speed:** With a fixed binary format, each data item can be easily parsed one by one. Compared to XML, the performance is several times faster.
- **Improved design flexibility:** Design flexibility 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 TMCM 2.5/3.0 agents, one pre-condition is assumed. The server relies on the fact that the agent can be reached by initiating a connection from server to the agent. This is a so-called two-way communication product, since both sides can initiate network connection with each other. This assumption breaks

when agent sits behinds a NAT device (or TMCM 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 TMCM server sitting behind a NAT device). One common work-around is that a specific mapping relationship is established on the NAT device to direct it to automatically route the in-bound request to the respective agent. However, this solution needs user involvement and it does not work well when large-scale product deployment is needed.

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

HTTPS Support

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

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

Using MCP, Control Manager has three security levels:

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

One-way and Two-way Communication Support

MCP supports one way and two-way communication.

One-way Communication

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

Two-way Communication

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

Single Sign-on (SSO) Support

Through MCP, Control Manager 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

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 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
Child server reporting	N/a	Yes
Trend Micro Product Registration server support	Yes	Yes
HTTPS management console	Yes	Yes

TABLE 1-2. Feature comparison between Enterprise and Standard editions

FEATURE	STANDARD	ENTERPRISE
HTTPS ActiveUpdate	Yes	Yes
Trend Micro Network VirusWall and InterScan Web Security Service integration	Yes	Yes
MSN Messenger notification	Yes	Yes

TABLE 1-2. 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. Refer to Table 1-3, “Control Manager Components,” on page 1-9 for a list of components Control Manager uses.

COMPONENT	DESCRIPTION
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.

TABLE 1-3. Control Manager Components

COMPONENT	DESCRIPTION
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.
Agents	Receives commands from the Control Manager server and sends status information and logs to the Control Manager server The Control Manager agent is an application installed on a managed product server that allows Control Manager to manage the product. Agents interact with the managed product and Communicator. An agent serves as the bridge between managed product and communicator. Hence, 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.

TABLE 1-3. Control Manager Components

Chapter 2

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:

- *Identifying Deployment Architecture and Strategy* on page 2-2
- *Installation Flow* on page 2-9
- *Supported Operating Systems* on page 2-9
- *Compatible Antivirus and Content Security Products* on page 2-11
- *Testing Control Manager at One Location* on page 2-13
- *Server Distribution Plan* on page 2-15
- *Network Traffic Plan* on page 2-17
- *Sources of Network Traffic* on page 2-22
- *Deploying Updates* on page 2-24
- *Data Storage Plan* on page 2-27
- *Web Server Plan* on page 2-29

Identifying Deployment Architecture and Strategy

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

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

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

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

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

Understanding Single-Site Deployment

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

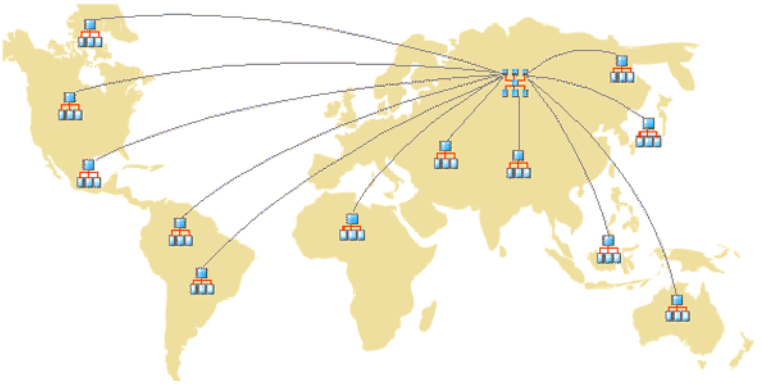


FIGURE 2-1. A single-server deployment using Enterprise Control Manager parent server and mixed child servers

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

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

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 put these servers on your network to optimize communication and management.

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

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 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.

Locate where your Windows servers are, 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 that will host Control Manager, consider the following:

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

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

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

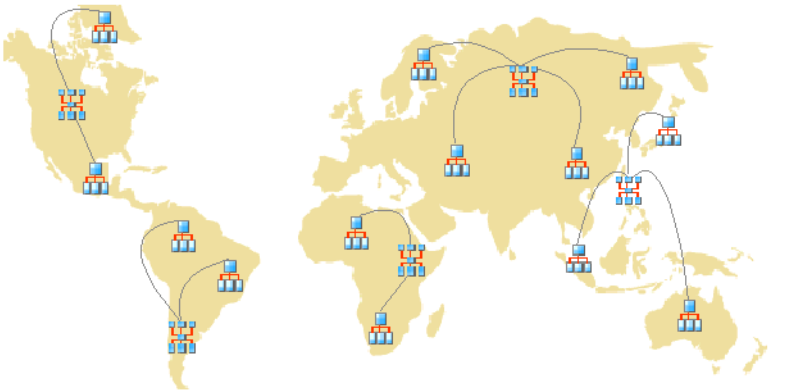
Depending on your network topology, you may need to perform additional site-specific tasks.

Understanding Multiple-Site Deployment

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

Given the uniqueness of each network, exercise judgment as to how many Control Manager servers would be optimal 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 if you want to administer managed product or child servers and access the Control Manager management console using Internet Explorer over the Internet.



nb

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

Consider the following for multi-site deployment:

- Group managed products or child servers
- Determine the number of sites
- Determine the number of managed products and child servers
- Plan for network traffic
- Plan for an optimal server-managed products/cascading structure ratio

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

Group Managed Products or Child Servers

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

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

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

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.

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

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

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

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

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

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.

Locate where your Windows servers are, 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 that will host Control Manager, consider the following:

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

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

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

Decide Where to Install the Control Manager Server

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

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

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

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

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

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

Installation Flow

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

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

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

Step 3: Installing Control Manager agents.

Supported Operating Systems

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

Control Manager Server

- Microsoft(TM) Windows(TM) 2000 Server + SP 1~4
- Windows 2000 Advanced Server + SP 1~4
- Windows 2003 + SP 1, Standard Edition, Enterprise Edition

Control Manager Agents

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

TABLE 2-2. Control Manager Agents Supported Operating Systems

Compatible Antivirus and Content Security Products

The following chart shows the products that are compatible with Control Manager and whether they support Outbreak Prevention Services (OPS) or Damage Cleanup Services (DCS).

Product	Version	Control Manager Agent			Services (OPS, DCS) Support
		MCP	CM 2.x	TVCS	
Storage Security					
ServerProtect	Version 5.5 or later		Yes		Fully supported
	Version 5.0 to 5.35			Trend VCS 1.86 or 1.84 agent only	Not supported
ServerProtect for Linux	Version 2.50	Yes			OPS (file blocking only)
Access Node Security					
OfficeScan Corporate Edition	Version 5.5 or later		Yes		HTTP-based version only
	Version 3.52 to 5.02			Trend VCS 1.86 or 1.84 agent only	Not supported
Web Security					
InterScan VirusWall for Windows NT	Version 3.51 or later			Trend VCS 1.86 or 1.84 agent only	Not supported
InterScan VirusWall for Unix	Version 3.6 or later			Trend VCS 1.84	Not supported

TABLE 2-3. Compatible Antivirus and Content Security Products

Product	Version	Control Manager Agent			Services (OPS, DCS) Support
		MCP	CM 2.x	TVCS	
Web Security					
InterScan WebProtect for ICAP	Version 1.5 or later		Yes		Fully supported
InterScan Web Security Suite	Version 1.0 or later		Yes		OPS support, no DCS support
Anti-Spyware Enterprise Edition 1	Version 5.0 or later		Yes		Fully supported
InterScan for Cisco CSC SSM	Version 5.0 or later	Yes			Fully supported
Messaging Security					
InterScan Messaging Security Suite for Windows	Version 5.1 or later		Yes		Fully supported
InterScan Messaging Security Suite for UNIX	Version 5.1 or later		Yes		Fully supported
InterScan eManager	Version 3.5x or later		Yes		Fully supported
ScanMail for Microsoft Exchange	Version 3.8 and 6.0 or later		Yes	Can also use Trend VCS 1.86 agents	Fully supported if Control Manager agents are used
	Versions 3.52, 3.7, and 5.1			Trend VCS 1.86 or 1.84 agent only	Not supported

Table 2-3. Compatible Antivirus and Content Security Products

PRODUCT	VERSION	CONTROL MANAGER AGENT			SERVICES (OPS, DCS) SUPPORT
		MCP	CM 2.x	TVCS	
MESSAGING SECURITY					
ScanMail for Lotus Notes	Version 2.6 or later		Yes		Fully supported
	Version 1.8x to 2.51			Trend VCS 1.86 or 1.84 agent only	Not supported
ScanMail eManager	Version 5.0 or later		Yes		Fully supported
NETWORK SECURITY					
Network VirusWall 1200 1.x	N/a		Yes		Fully supported
Network VirusWall 2500 1.x	N/a		Yes		Fully Supported
Network VirusWall Enforcer 2500	N/a	Yes			Fully Supported
FIREWALLS					
NetScreen-Global PRO	Version 3.11		Yes		Fully supported

TABLE 2-3. Compatible Antivirus and Content Security Products

Testing Control Manager at One Location

Trend Micro recommends conducting a pilot deployment before performing a full-scale deployment. A pilot deployment provides an opportunity for feedback to determine how features work and the level of support likely needed after full deployment.

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

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

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

A Control Manager test deployment consists of the following tasks:

Preparing for the Test Deployment

Complete the following activities during the preparation stage:

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

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

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

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

Selecting a Test Site

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

Creating a Rollback Plan

Create a disaster recovery or rollback plan (for example, how to rollback to Control Manager 2.x or Trend VCS 1.8x server) in case there are some difficulties with the installation or upgrade. This process should take into account local corporate policies, as well as IT resources.

Beginning the Test Deployment

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

Evaluating the Test Deployment

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

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

Server Distribution Plan

Understanding Administration Models

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

Follow one of these administration models:

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

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

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

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

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

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

Understanding Control Manager Server Distribution

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

Note: Since Control Manager supports multiple user accounts, segregation that was necessary for Trend Virus Control System (Trend VCS) is no longer necessary. For information about upgrading Trend VCS servers, see Upgrading Trend VCS 1.8x servers.

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.

Single-Server Topology

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

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

Multiple-Server Topology

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

For information on the traffic that a Control Manager network generates, see Understanding Control Manager network traffic.

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.

Understanding Control Manager Network Traffic

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

Sources of Network Traffic

The following Control Manager sources generate network traffic:

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

Traffic Frequency

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

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

Logs

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

Trend Micro Management Infrastructure Heartbeat

By default, the Trend Micro Infrastructure (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.

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

File Sizes

Sizes for the following Control Manger network traffic sources include:

- **Logs:** Agents send logs to the Control Manager server in XML format. The table below shows the file sizes (as of December 2003) of each XML file, according to product.

PRODUCT	XML FILE SIZES				
	VIRUS/ SPYWARE/ GRAYWARE LOG	SECURITY LOG	WEB SECURITY LOG	EVENT LOG	STATUS LOG
InterScan eManager	N/a	2KB	N/a	3KB	4KB
InterScan Messaging Security Suite	2K	3KB	N/a	1.5KB	1.5KB
InterScan Web Security Suite	1.8KB	N/a	1.31KB	1KB	1.73KB
InterScan WebProtect	1.8KB	N/a	1.31KB	1KB	1.73KB
OfficeScan Corporate Edition	4KB	N/a	N/a	3KB	2KB
ScanMail eManager	N/a	4KB	N/a	3KB	6KB
ScanMail for Microsoft Exchange	2KB	N/a	N/a	1KB	2KB
ScanMail for Lotus Notes	2KB	3KB	N/a	1KB	2KB
ServerProtect	2KB	N/a	N/a	4KB	6KB

TABLE 2-4. Control Manager 2.x Agent Log Size

PRODUCT	XML FILE SIZES				
	VIRUS/ SPYWARE/ GRAYWARE LOG	SECURITY LOG	WEB SECURITY LOG	EVENT LOG	STATUS LOG
InterScan for Cisco CSC SSM	1KB	2KB	2KB	2KB	2KB
Network VirusWall Enforcer 2500	1KB	2KB	2KB	2KB	2KB
ServerProtect	1KB	2KB	2KB	2KB	2KB

TABLE 2-5. MCP Agent Log Size

- **MCP policies:** Heartbeat, emergency, and command messages are all 1KB in size.
- **Trend Micro Management Infrastructure policies:** Heartbeat, emergency, and prohibited messages are all 1KB in size (as at December 2003).
- **Downloading and deploying updates:** Component updates are the most bandwidth-intensive operation in a Control Manager network.

Updating the ScanMail and InterScan Family of Products

The following table shows the size of the components deployed to these products. Note, however, that the size of the files here are approximations (as at December 2003).

COMPONENT	SIZE (IN COMPRESSED FORM)	
Virus pattern file	If the system is updated regularly (incremental update)	430 to 550KB
	If the system is updated either for the first time or infrequently	3.1MB
Scan engine		411KB

TABLE 2-6. ScanMail and InterScan Files

Updating the eManager Family of Products

Anti-spam rules are approximately 48KB (as at December 2003).

Updating OfficeScan Corporate Edition and ServerProtect

The following table shows the size of the components deployed to these products. Note, however, that the size of the files here are approximations (as at December 2003).

COMPONENT	SIZE (IN COMPRESSED FORM)	
Virus pattern file	If the system is updated regularly (incremental update)	430 to 550KB
	If the system is updated either for the first time or infrequently	3.1MB
Scan engine		411KB
	OfficeScan Corporate Edition	815KB
	ServerProtect	840KB

TABLE 2-7. OfficeScan Corporate Edition and ServerProtect Files

Protocols

Control Manager uses the UDP and TCP protocols for communication.

Sources of Network Traffic

Log Traffic

Constant sources of network traffic in a Control Manager network are '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 security threats.
Security	Violations reported by content security products.
Web Security	Violations reported by web security products.
Event	Miscellaneous events (for example, component updates, and generic security violations).
Status	The environment of a managed product. The Status tab of the Product Directory displays this information.
Network Virus	Viruses detected in network packets.
Performance Metric	Used for previous product versions.
URL Usage	Violations reported by Web security products
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

TABLE 2-8. Control Manager Log Traffic

For detailed information about the types of logs that are available for managed products, see Understanding logs.

Trend Micro Management Infrastructure Policies

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

- **Communicator Heartbeat:** 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. There are two types of information, however, that do not follow the Communicator Scheduler:
  - Emergency messages
  - Prohibited messages

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

Trend Micro Management Communication Protocol Policies

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

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

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

Product Registration Traffic

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

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

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

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

Deploying Updates

Understanding Deployment Updates

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

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

Step 2: Deploy these components to the managed products.

Control Manager deploys update components to managed products, including:

- Pattern files/Cleanup templates

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

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

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

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

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

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

The actual bandwidth usage will vary with the actual managed products. The following sections list differences among different Trend Micro products:

- About the ScanMail and InterScan family of products
- About the eManager family of products
- About OfficeScan Corporate Edition and ServerProtect

About ScanMail and InterScan Family of Product Updates

The ScanMail and InterScan family of products are antivirus applications that protect your email systems and Internet gateway, respectively.

If you regularly update these products, you only need to deploy incremental virus patterns – which only contain the virus signatures that are absent from the pattern file currently used by the program. If the products are fresh installations, or are not updated regularly, deploy full virus patterns.

The following table shows the size of the updates deployed to these products. File sizes are approximations (as at December 2003).

COMPONENT	SIZE (IN COMPRESSED FORM)
Virus pattern file	500 to 900KB- If the system is updated regularly (incremental update)
	3 to 3.5MB- If the system updated either for the first time or infrequently
Scan engine	411KB

About the eManager Family of Product Updates

The eManager family of content security products relies on anti-spam rules to identify unwanted email messages. For additional information on anti-spam rules, see Understanding the antivirus and content security components.

Trend Micro usually updates anti-spam rules at least twice a day.

Control Manager can obtain updated versions of these anti-spam rules from the Trend Micro update server and deploy them to managed eManager products. These files will be approximately 300 to 600KB in size in compressed form (as at December 2003).

About OfficeScan Corporate Edition and ServerProtect Updates

OfficeScan Corporate Edition and ServerProtect are antivirus products that protect desktop machines and network servers respectively. Both are composed of:

- Client applications that perform the actual antivirus function
- A management server (Information Server for ServerProtect; OfficeScan Server for OfficeScan) for controlling the clients

The management server serves as the update server for its clients. It contains the different incremental update patterns, as well as the full pattern, and the different scan engines required by the following client platforms:

OfficeScan clients

- Windows XP/2000/NT Professional
- Windows Me/98/95

ServerProtect Normal Servers

- Windows 2003/2000/NT
- Novell NetWare

When Control Manager deploys updates to these products, it is actually deploying complete update sites – incremental update technology is not used. As a result, updating these products is comparatively more resource intensive than other Trend Micro products.

The following table shows the size of the updates deployed to these products. File sizes are approximations (as at December 2003).

COMPONENT	SIZE (IN COMPRESSED FORM)
Virus pattern file	3.5 to 4MB- Incremental patterns (7 patterns)
	3 to 3.5MB- Full pattern
Scan engine	815KB- OfficeScan
	840KB- ServerProtect

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.

Understanding Control Manager Data Storage

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.

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 rather than Windows authentication.

Web Server Plan

Web Server Configuration

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

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

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

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

Where:

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

  Pattern/vsapi.zip

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

Chapter 3

Installing Trend Micro Control Manager for the First Time

This chapter guides you through installing Control Manager server 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 3-8
- *Verifying Successful Installations* on page 3-31
- *Post-installation Configuration* on page 3-32
- *Registering and Activating Your Software* on page 3-33

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 Control Manager 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.

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

HARDWARE SPECIFICATIONS	MINIMUM REQUIREMENTS
CPU	Intel™ Pentium™ III Processor 450MHz or higher
Memory	256MB RAM
Disk space	• 450MB for Control Manager Standard Version • 500MB for Control Manager Enterprise Version • 300MB for MSDE 2000 (Optional)

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

SOFTWARE SPECIFICATIONS	MINIMUM REQUIREMENTS
Operating system	• Microsoft™ Windows™ Server 2003 Standard • Microsoft Windows Server 2003 Enterprise • Microsoft Windows 2000 Server • Microsoft Windows 2000 Advanced Server with Service Pack 3
Web server	Microsoft Internet Information Server (IIS) 4.0 or higher
Database	• Microsoft Data Engine (MSDE) 1.0 / 2000 (2000 + SP3 is recommended) • Microsoft SQL Server 7.0 • Microsoft SQL Server 2000 (2000 + SP3 is recommended)
Others	• SQL ODBC driver 3.7 or higher • Windows Installer (included in Control Manager package)
Management console	• Browser- Microsoft Internet Explorer 5.5 with SP2 or higher • Java VM- Microsoft Version 5.0.0.3805 or higher • JRE 1.4.2 or 1.5.0

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

Please refer to the URL below 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: • Control Manager agents: 1000 • TVCS agents: 500 • OSCE 6.5 clients: 2000 • Total above: 2000	• Intel Pentium III 450MHz or equivalent • 256MB • MSDE (local)

TABLE 3-4. Control Manager recommended system requirements

CONTROL MANAGER SERVER	ENVIRONMENT	RECOMMENDATION
Single/Child	Number of: • Control Manager agents: 1500 • TVCS agents: 500 • OSCE 6.5 clients: 5000 • Total above: 5000	• Intel Pentium III 1GHz or equivalent • 512MB RAM • SQL Server (local)
Parent	Number of: • Control Manager agents: 10000 • TVCS agents: 2500 • OSCE 6.5 clients:10000 • Total above: 10000 • Child Control Manager servers: 50	
Single/Child	Number of: • Control Manager agents: 2000 • TVCS agents: 500 • OSCE 6.5 clients: 10000 • Total above: 10000	• Intel Pentium III 1GHz or equivalent • 1GB RAM • SQL Server (remote)
Parent	Number of: • Control Manager agents: 20000 • TVCS agents: 5000 • OSCE 6.5 clients:100000 • Total above: 100000 • Child Control Manager servers: 100	

TABLE 3-4. Control Manager recommended system requirements

CONTROL MANAGER SERVER	ENVIRONMENT	RECOMMENDATION
Single/Child	Number of: • Control Manager agents: 5000 • TVCS agents: 1000 • OSCE 6.5 clients: 10000 • Total above: 15000	• Intel Pentium 4 2GHz or equivalent • 2GB RAM • SQL Server (remote)
Parent	Number of: • Control Manager agents: 50000 • TVCS agents: 10000 • OSCE 6.5 clients:200000 • Total above: 200000 • Child Control Manager servers: 200	

TABLE 3-4. Control Manager recommended system requirements

NUMBER OF MANAGED PRODUCTS	NUMBER OF CPUS	CPU SPECIFICATIONS	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.

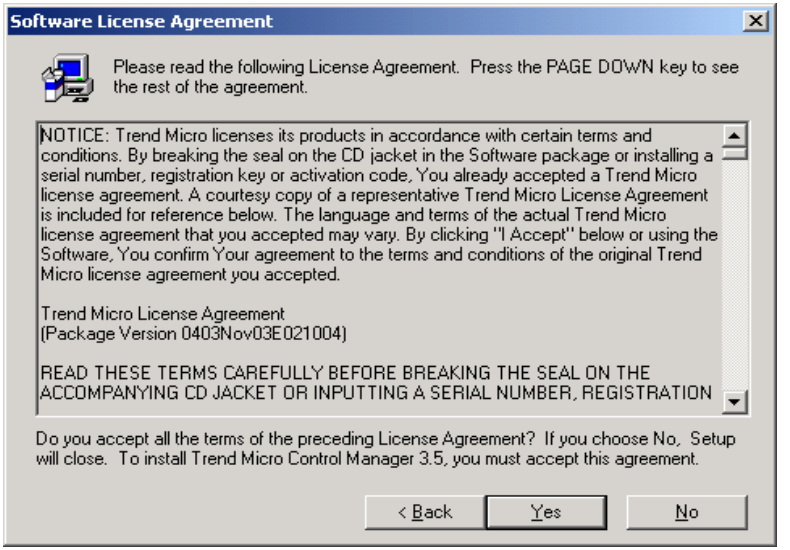


FIGURE 3-1. Choose Yes to agree with the License Agreement

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.

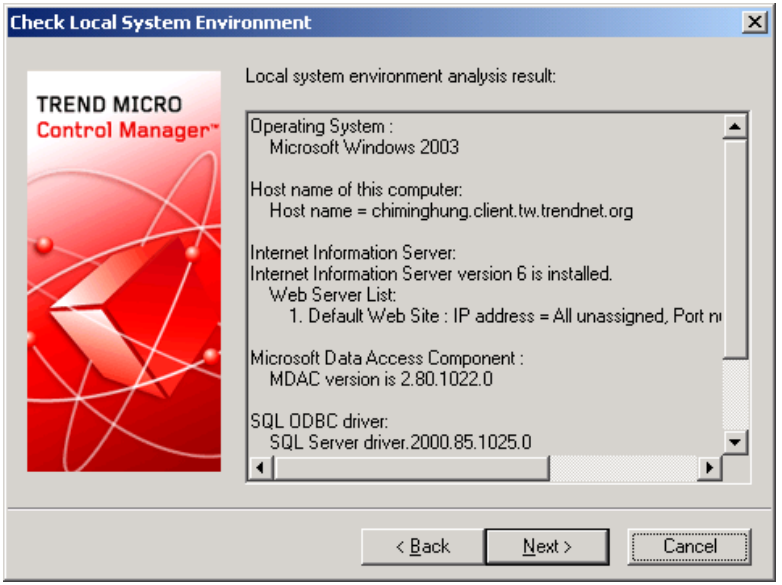


FIGURE 3-2. Displays local system environment information

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

FIGURE 3-3. Enter your name and company

4. Type your name and company.

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

FIGURE 3-4. Register online to obtain an Activation Code

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.

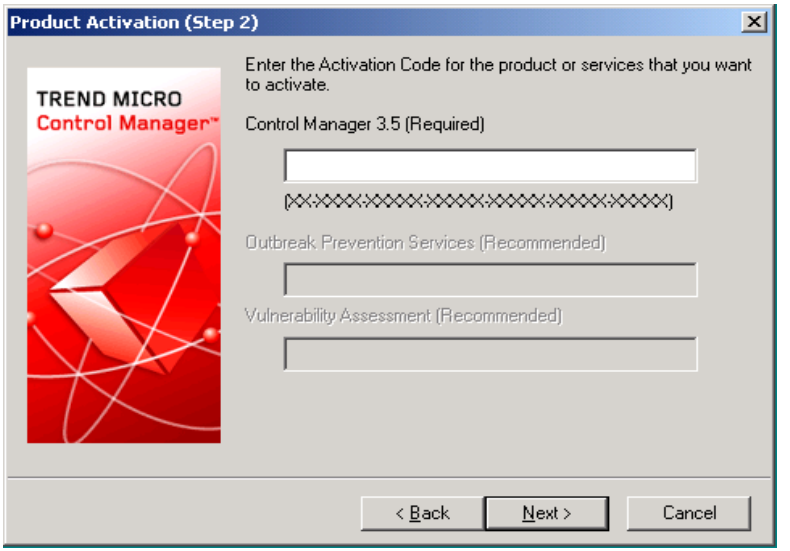


FIGURE 3-5. Enter the Activation Code to activate Control Manager and services

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.

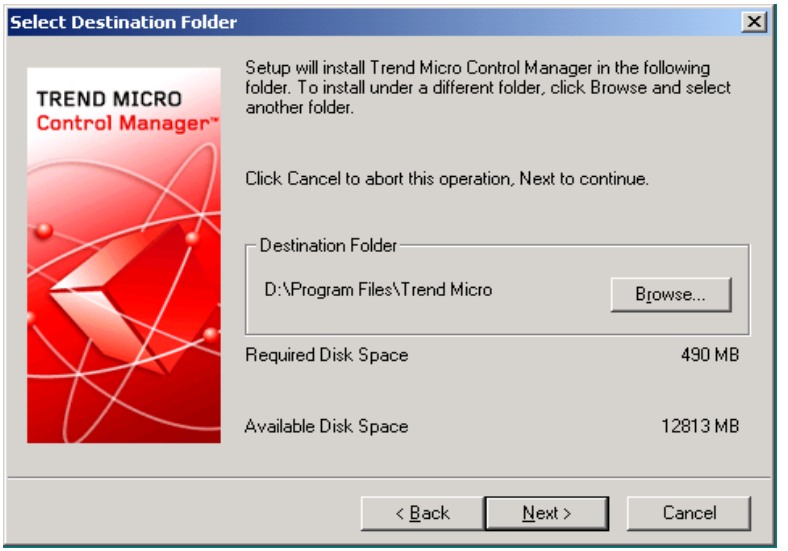


FIGURE 3-7. Select a destination folder

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

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

---

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

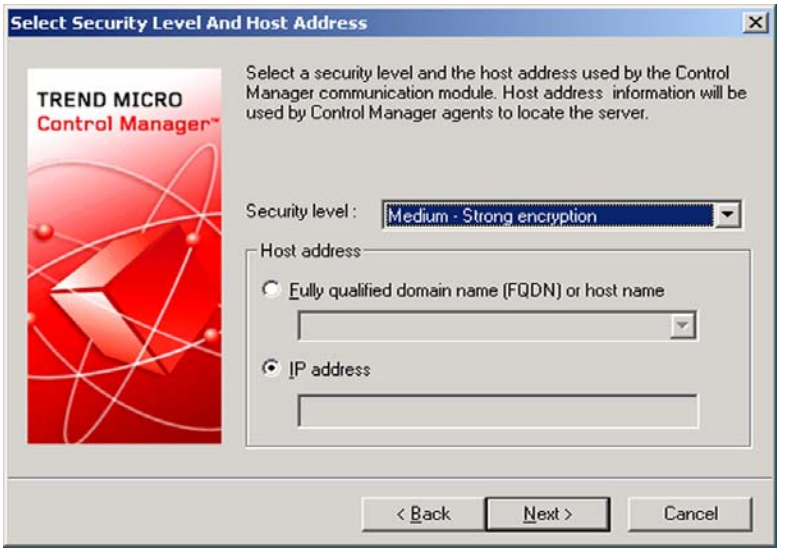


FIGURE 3-8. Select a security level

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.

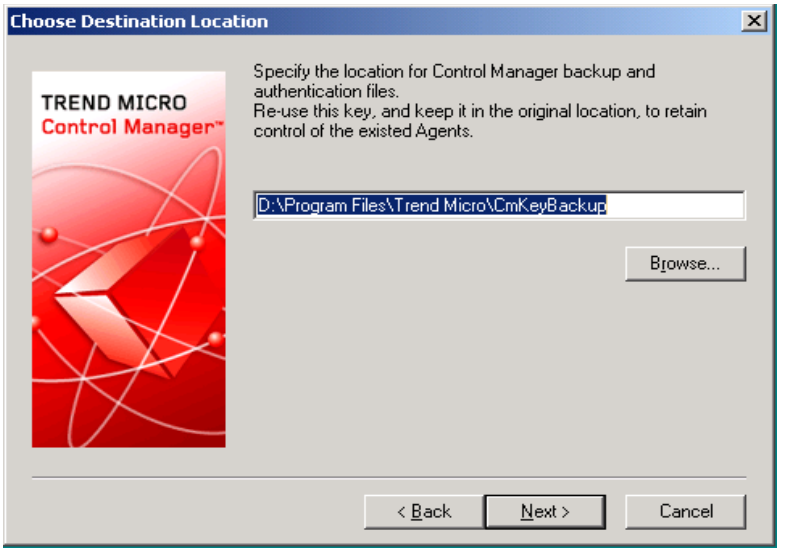


FIGURE 3-9. Choose a destination location for backup and authentication files

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.

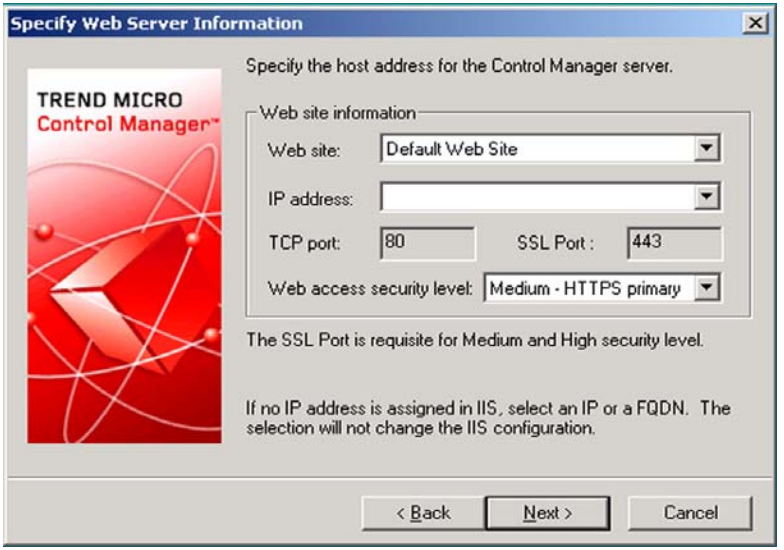


FIGURE 3-10. Specify Web server information

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

Step 3: Choose and configure database information

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

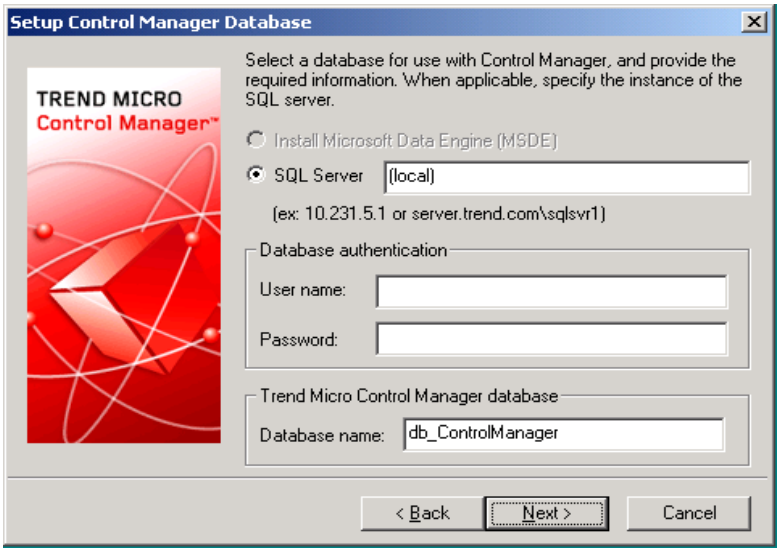


FIGURE 3-11. Choose the Control Manager database

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:

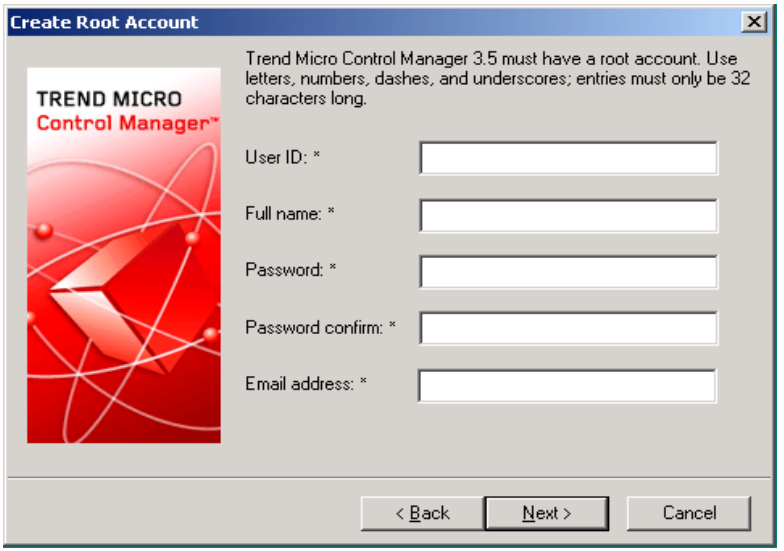


FIGURE 3-12. Enter information for the Control Manager root account

2. Provide the following required account information:
   - User ID
   - Full Name
   - Password
   - Password confirmation
   - Email address

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

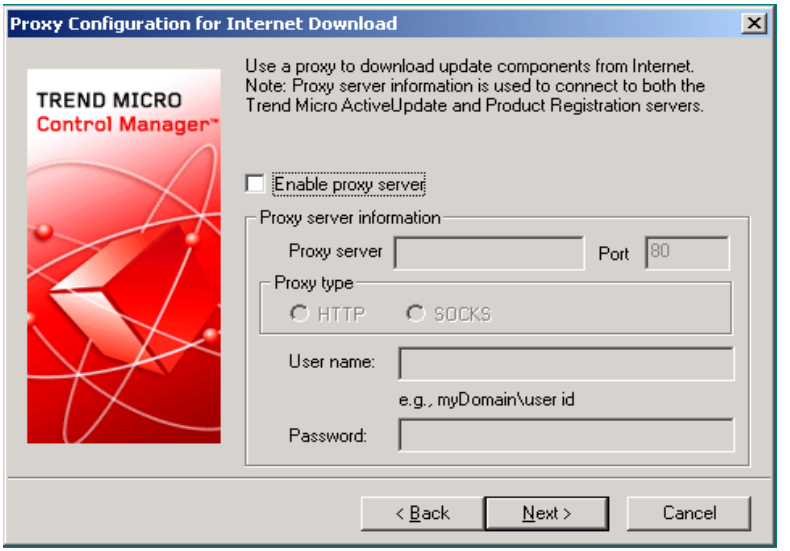


FIGURE 3-13. Enable proxy server

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.

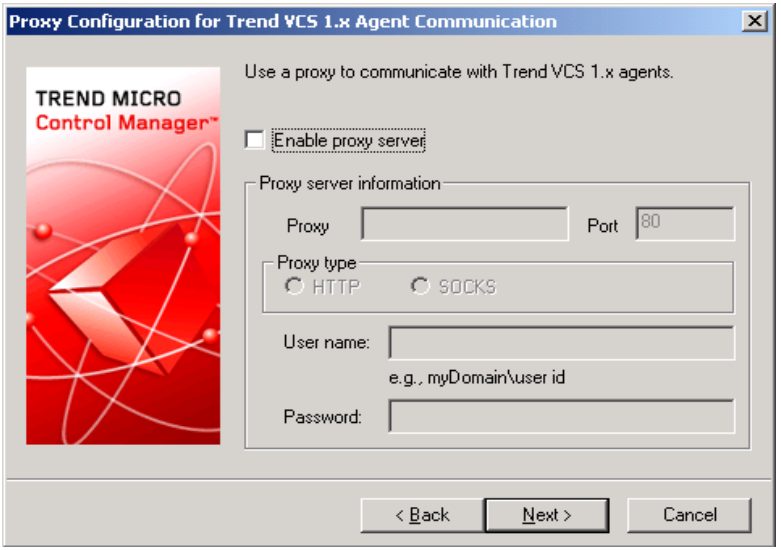


FIGURE 3-14. Enable proxy server to communicate with Trend VCS 1.x agents

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.

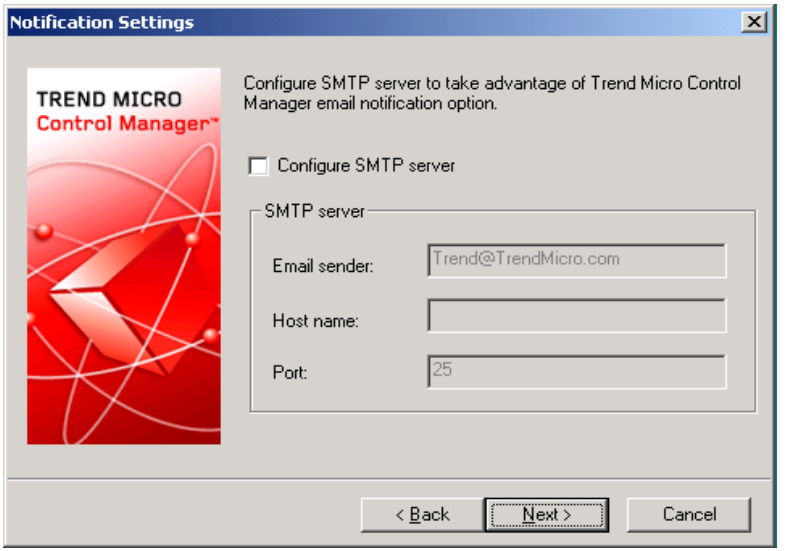


FIGURE 3-15. Configure SMTP options

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.

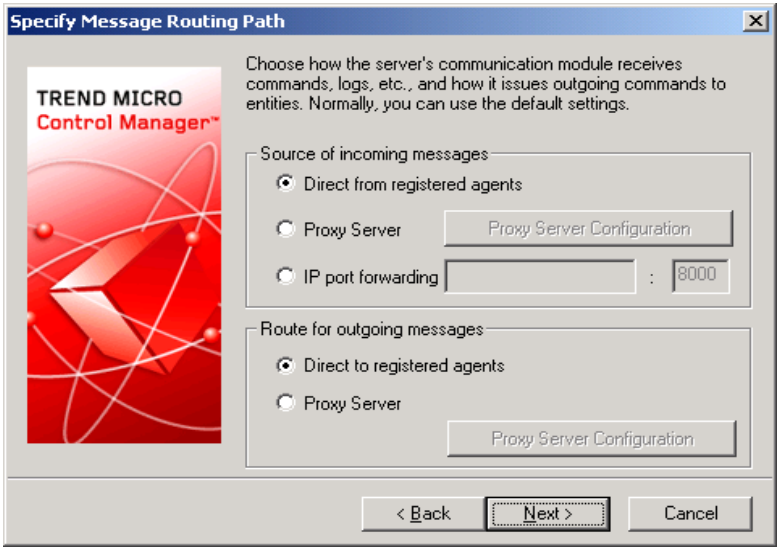


FIGURE 3-16. Define routes for messages or requests

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 6-59.
- **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 6-59.

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

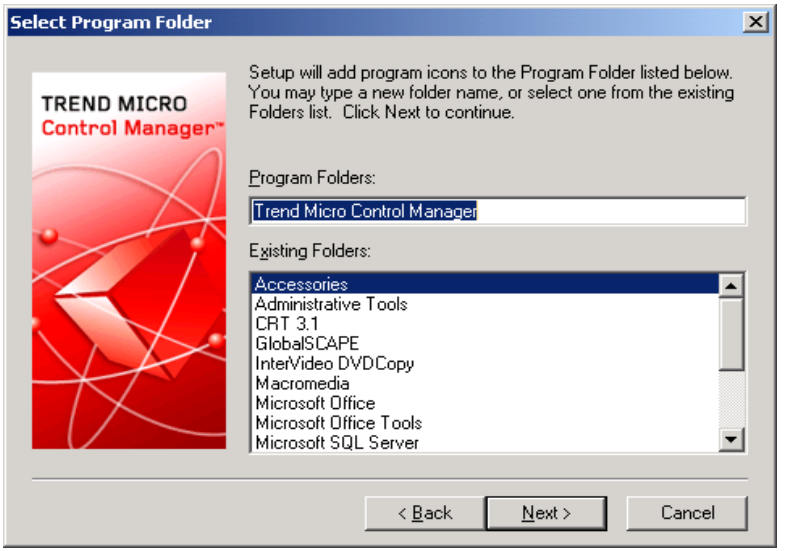
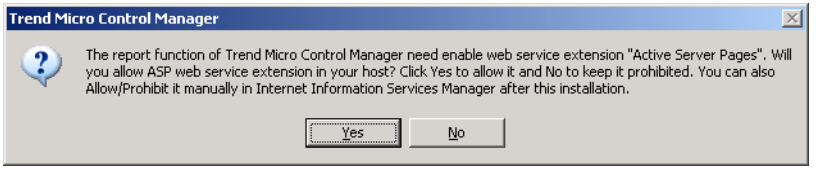


FIGURE 3-17. Select program folder

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

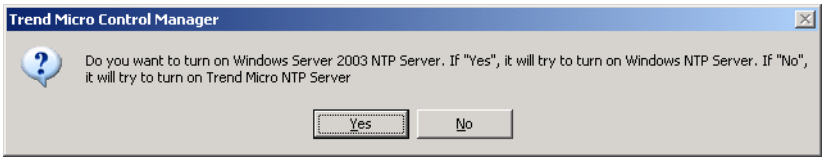
Note: Steps 7 to 10 appear only on Windows 2003 server installations.

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.

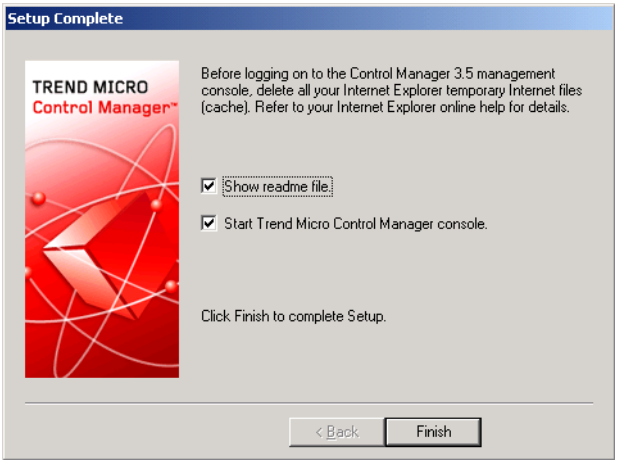


FIGURE 3-18. Setup complete

Verifying Successful Installations

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

Verify a Successful Control Manager Server Installation

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

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

- `Common\TMI`
- `Common\CCGI`
- `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`
- `EntitiyEmulator.exe`
- `LogRetriever.exe`
- `CmdProcessor.exe`
- `UIProcessor.exe`
- `ReportServer.exe`
- `NTPD.exe`
- `DCSprocessor.exe`
- `Casprocessor.exe`

Post-installation Configuration

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

1. Register and activate Control Manager
2. Configure user accounts
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. For more information, see *Registering and Activating Your Software* on page 3-33.

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

For more information, see *Configure Control Manager User Accounts and Groups* on page 6-8.

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**). For more information, see *Download and Deploy New Components* on page 6-32.

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**). For more information, see *Use Event Center* on page 7-9

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**.
4. 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**.

Chapter 4

Installing Control Manager Agents

This chapter details the installation of Control Manager agents for various Trend Micro products. The major topics covered in this chapter are the following:

- *About Control Manager Agents* on page 4-2
- *Prepare for Control Manager Agent Installation* on page 4-3
- *Understanding Control Manager Agent Remote Installation* on page 4-4
- *Performing the Installation* on page 4-5
- *Verify a Successful Agent Installation* on page 4-39

About Control Manager Agents

Control Manager uses agents to manage products on your network. Control Manager now supports three 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 TMI 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.

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 agent, 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 installs one Communicator on each machine, and the Communicator installs 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 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.

MCP agents install with their managed product. You do not need to perform a separate installation for MCP agents. Refer to your managed product's documentation for more information on installing MCP agents with managed products.

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

Note: You need administrator rights for the target servers you want access.

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

- The products for which agents will be installed
- 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. See What happens if I delete the User ID that I used for registering a product? for more information.*

- The location of the public encryption key of the Control Manager you want to register the agent with. Only 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 Control Manager Agent Remote Installation

The Control Manager 3.5 server supports Trend Virus Control System 1.8x and Control Manager 2.5x agents for remote deployment.

There are two agent remote installation programs:

- `RemoteInstall.exe`
- `CMagentSetup.exe`

Tip: Remote installation is the preferred installation method for deploying agents on large numbers of product servers. This capability allows you to install agents without being physically at the target server.

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 perform the installation.

After a fresh Control Manager installation, Control Manager servers do not contain agent packages — the antivirus or content security product uploads and stores their agents 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 1: Obtain required files

Step 2: Obtain agent packages (Optional)

Step 3: 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**.

Note: 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 will be registered 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.

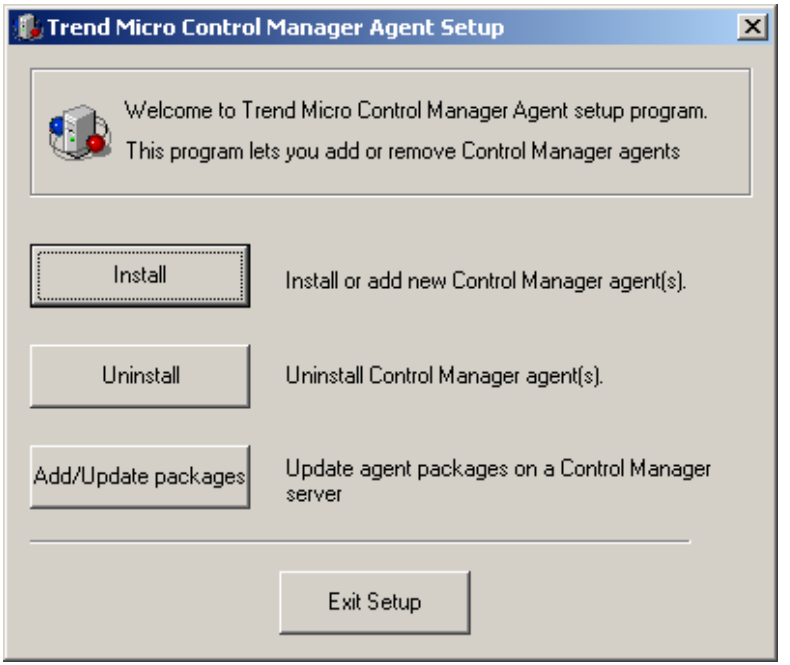


FIGURE 4-1. Control Manager Agent Setup screen

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

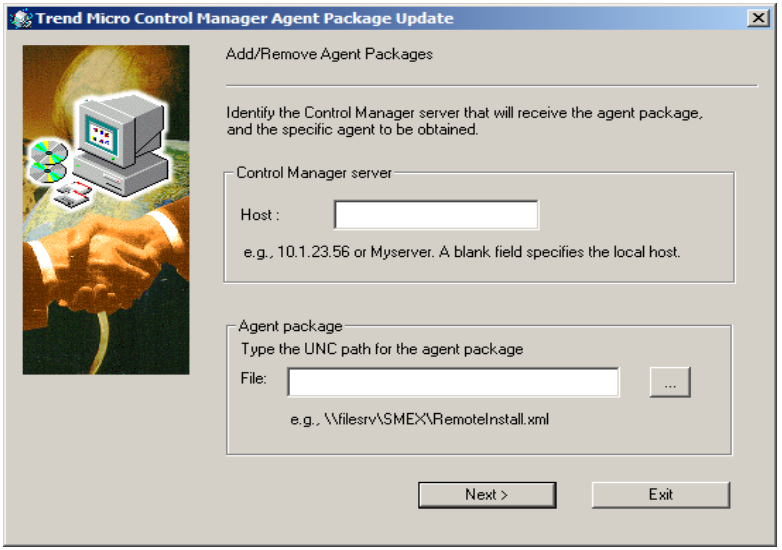


FIGURE 4-2. Identify the Control Manager server and the agent

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 ellipsis button (. . .), locate the package, and then click **Open**.

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

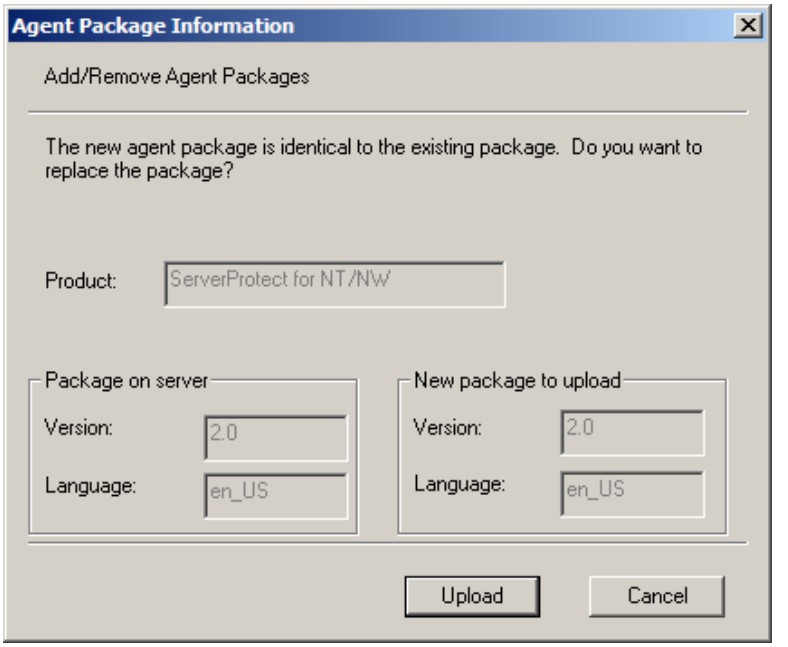


FIGURE 4-3. Agent package information

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.

The table below indicates the locations of each agent in the Enterprise Security

CD (Based on January 2004 Enterprise Security CD):

PRODUCT	PATH
Control Manager agent (general)	disk1\programs\Control Manager\Agent\Control Manager
Trend VCS agent (general)	disk1\programs\Control Manager\Agent\Tvcs
ScanMail for Notes	disk2\programs\ScanMail for Notes NT\cmagent
ScanMail for Microsoft Exchange 2000	disk1\programs\ScanMail for Exchange 2000\cmagent
OfficeScan Corporate Edition	disk1\programs\OfficeScan\cmagent
ServerProtect for Windows	disk1\programs\ServerProtect NT\English\CMAgent
NetScreen Firewall Management Module	disk1\programs\NetScreen Firewall Management Module
ScanMail eManager	disk1\programs\ScanMail eManager for SMEX ESE-2000\cmagent
InterScan eManager for Windows	disk2\programs\InterScan eManager NT\cmagent
InterScan Messaging Security Suite for Windows	disk1\programs\InterScan Messaging Security Suite\cmagent
InterScan Web Security Suite Solaris	disk3\programs\InterScan Web Security Suite Solaris\English
InterScan Messaging Security Solaris	disk3\programs\InterScan Messaging Security Solaris\English
InterScan Messaging Security Linux	disk3\programs\InterScan Messaging Security Linux\English

TABLE 4-1. Enterprise Security Agents

Install Windows-Based Agents

To install Trend VCS agents:

1. Using MS Explorer, go to the location where you saved the agent setup program.

2. Double-click the CMagentsetup.exe file.
3. Click **Install** to begin installation. 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. Click **Next**.
5. Select the product for which you want to install agents. Click **Next** to continue.
   - If you selected the Trend VCS agent for OfficeScan, see *Install the Trend VCS Agent for OfficeScan Corporate Edition* on page 4-27.
   - If you perform a remote agent installation, proceed to **step 6** of this topic
   - If you perform a local installation, proceed to **step 11** of this topic
6. On the Select Servers to Install screen, select the servers where the agents are to be installed. There are two ways to do this:

   To select from the list:

   a. At the left-hand 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-hand list box, then click **Add**. The chosen server appears on the right-hand 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-hand list.

   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-hand list box.

   To remove servers from the list, select a server from the right-hand list box, then click **Remove**. To remove all servers, click **Remove All**.
7. Click **Next** to continue.
8. 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.

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

Tip: Share at least one drive or folder on the target server.

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-enter 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, the setup program prompts for another set of credentials.

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

9. Click **OK** at the dialog box that opens after completion of server analysis. 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 **OK** in the dialog box that opens, then **Next** to start the actual agent installation.
11. At the Proxy Information screen, select the **Yes, connect through a proxy server** check box if you intend to use a proxy for Server-Agent communication.
12. Provide the address of the proxy server used by your Control Manager server; you can use either its IP address, or its Fully Qualified Domain Name (FQDN) -- provided the agent's server can resolve the FQDN. Afterwards, Click **Next**.

Note: Do not select this option if you have configured the Internet Information Service on your Control Manager server to use NT Challenge/Response authentication.

13. The Control Manager Server Information screen opens. Provide the following information on this screen:
    - **Host name (or IP Address):** This is the host name or IP address of your Control Manager server
    - **TCP Port:** This is the port used by the WWW service of your Microsoft Internet Information Service
14. At the Agent Information screen provide the following:

- **Site:** Provide a site name for the agents. This will appear as a sub-folder name under the Trend VCS Agents folder in the Directory

Tip: A useful system for this would be to specify a name that reflects the agent's geographical location (for example, New_York, Tokyo, Manila).

- **Relative destination directory:** This determines the placement of the Trend VCS Agent files on the server. This directory is relative to the shared folder you specified earlier.

The Installing Agents screen opens. The table shows the installation status of the agents.

15. After the installation, click **OK** in the dialog box that opens. Click **Exit** to end the setup, or Next to install agents for other applications.

    If you clicked **Next**, a dialog box opens. Click **Yes** to install other agents, otherwise click **No**.

16. Click **Finish** at the final screen.

Installing Control Manager Agents with the Remote Agent SetupTool

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.

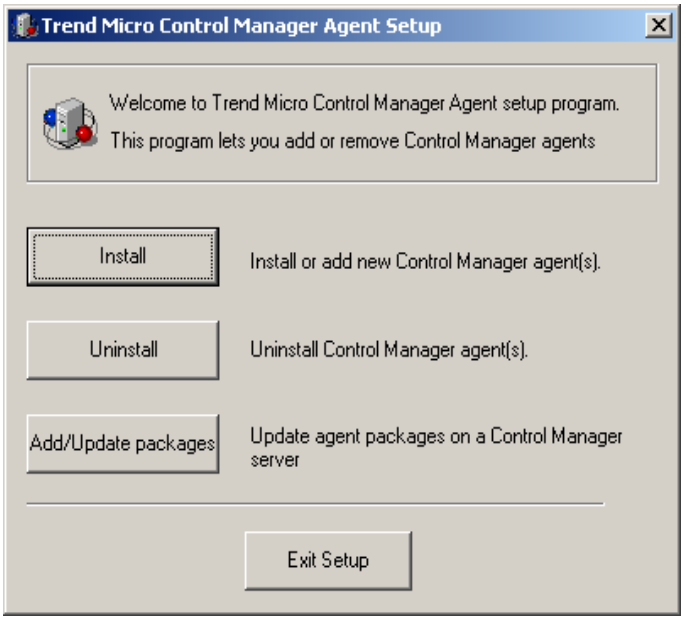


FIGURE 4-4. Control Manager Remote Agent Setup

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.

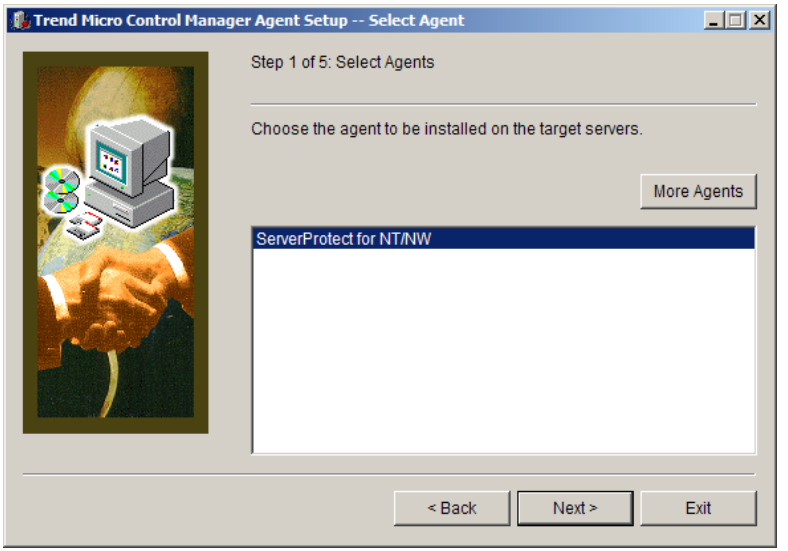


FIGURE 4-6. Choose the agent to install on the target server

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 4-7

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

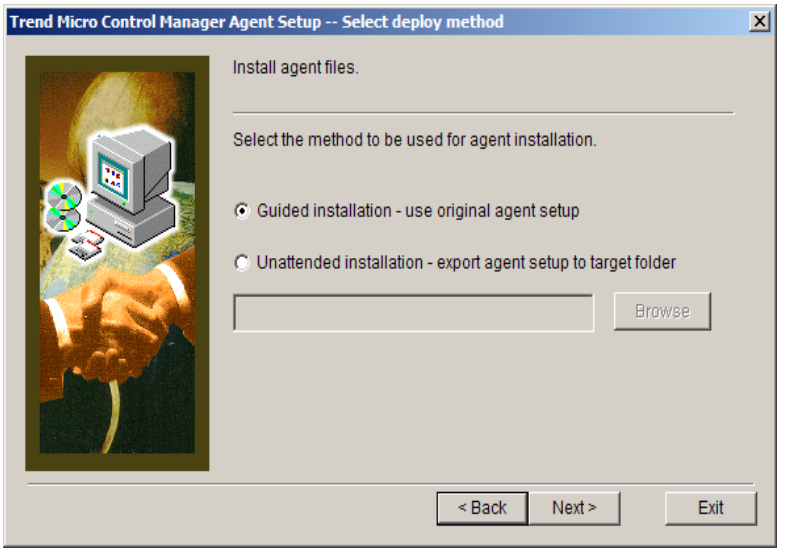


FIGURE 4-7. Select the agent installation method

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

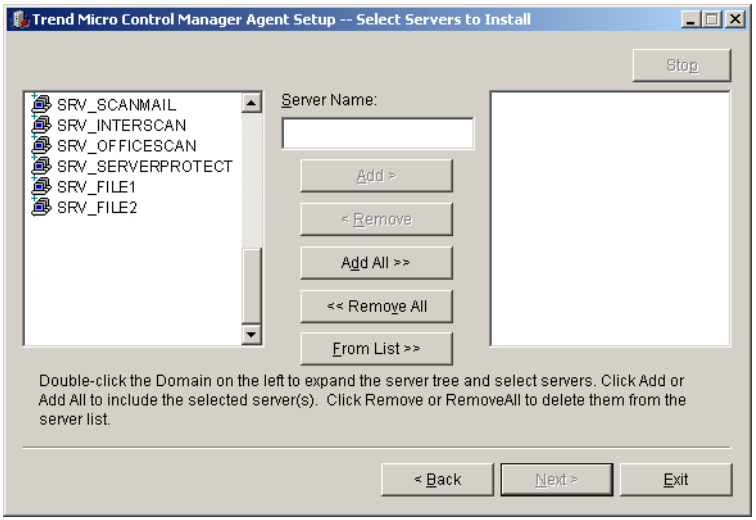


FIGURE 4-8. Select servers to install

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 Trend VCS Migration tool generates the migration list. For additional information about this list, see *Cascading Management Structure Tool (CasTool.exe)* starting on page 10-2.

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.

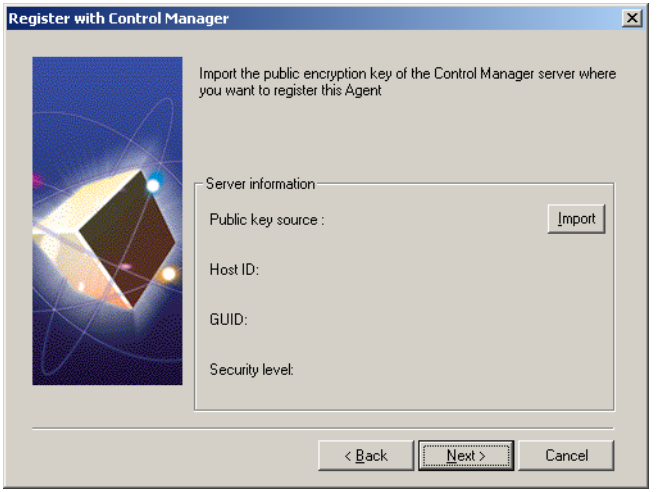


FIGURE 4-9. Encryption key selection screen

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 versions 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.

8. 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.

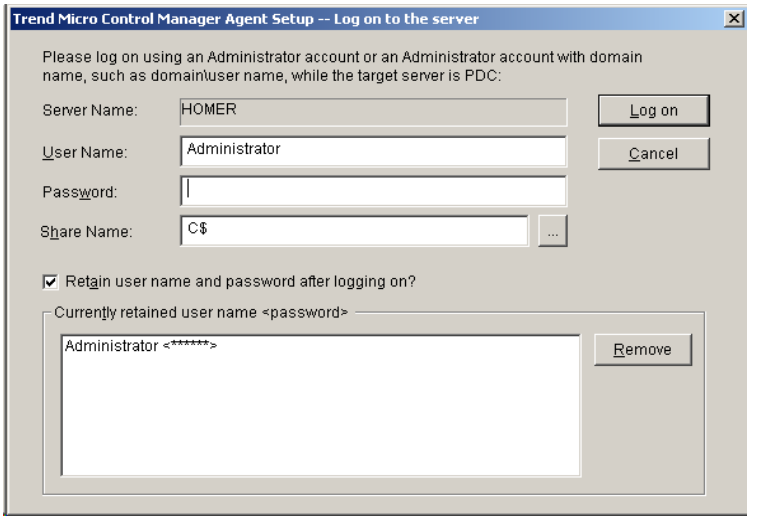


FIGURE 4-10. Logon credentials screen for agent installation

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.

---

9. 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.

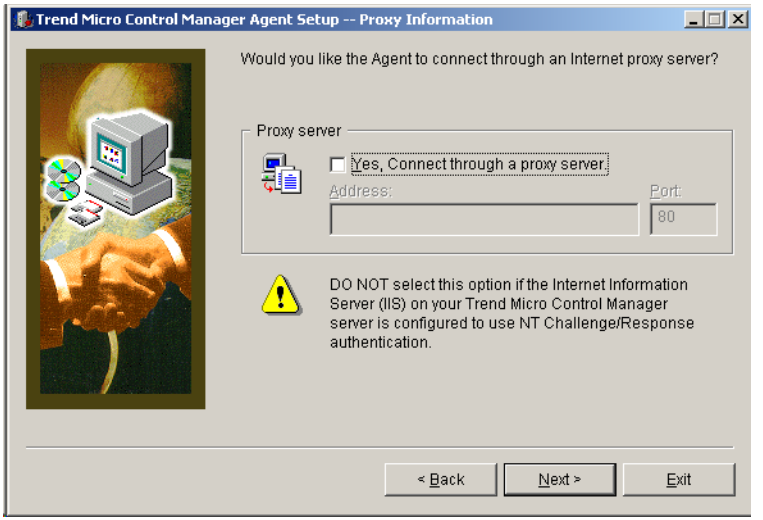


FIGURE 4-11. Trend VCS agent proxy screen

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 Agents 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.

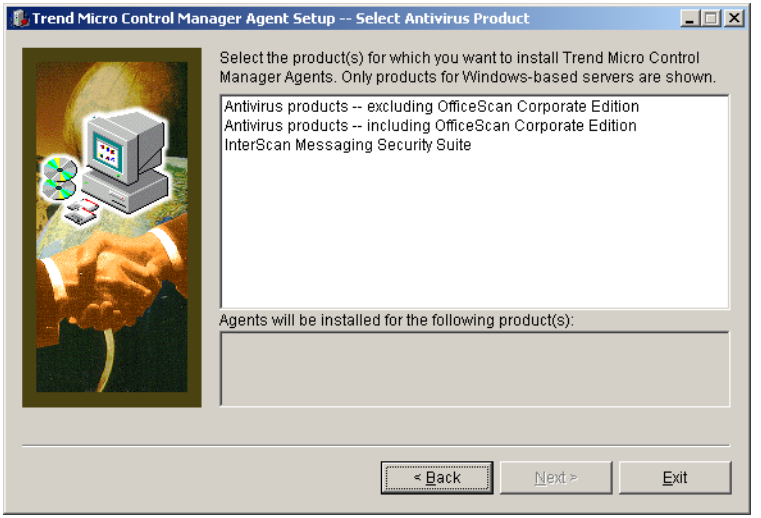


FIGURE 4-12. Select Antivirus Product screen; note inclusion of IMSS in the selection

To install this agent, see *Installing Trend VCS Agents* on page 4-22, and follow the procedure until step 10. Afterwards, see *Installing Control Manager Agents with the Remote Agent SetupTool* on page 4-14, and use the procedure starting on step 14.

Install the Trend VCS Agent for OfficeScan Corporate Edition

OfficeScan Corporate Edition versions 3.5x to 5.02 use the Trend VCS agent.

Note: Later versions of the product use the Control Manager agent for OfficeScan. For installation information about this agent, refer to the OfficeScan documentation.

You can install this agent on the OfficeScan server itself, or a separate server on your network. The installation procedure is identical for both the HTTP-based and file-based versions of the OfficeScan server.

If you have installed OfficeScan on a Windows 2000/NT server, you can install the agent on the same server. However, if you have installed OfficeScan on a NetWare server, you must install the agent on a separate Windows 2000/NT server.

After selecting OfficeScan Corporate Edition from the list of agents, the setup program adds the following steps to the normal procedure:

1. The OfficeScan Agent Setup Mode screen appears. This screen offers you two options:
   - Install Trend VCS agent to remote OfficeScan server(s)
   - Install Trend VCS agent to this local computer
2. Click **Next** to continue. The Agent Topology for OfficeScan screen opens. This screen provides a graphical explanation of the topology you selected.
3. Click **Next** to continue. The procedures for installing remotely or locally are the following:
   - Installing the Trend VCS agent on remote OfficeScan servers
   - Installing the Trend VCS agent locally

Installing the Trend VCS Agent on Remote OfficeScan Servers

If you are using HTTP-based OfficeScan versions exclusively, Trend Micro recommends installing the Trend VCS agent directly on the OfficeScan server for better agent performance.

Clicking **Next** on the screen in **Step 2**, above, returns you to the normal agent installation procedure, proceed with the following steps:

1. At the Select Servers to Install screen, select the servers where the agents are to be installed. There are two ways to do this:

   To select from the list:

   a. At the left-hand 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-hand list box, then click **Add**. The chosen server appears on the right-hand 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-hand list.

To type 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-hand list box.

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

2. Click **Next** to continue.

3. 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.

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

Tip: Share at least one drive or folder on the target server.

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-enter 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, the setup program prompts for another set of credentials.

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

---

4. Click **OK** at the dialog box that opens after completion of server analysis. 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.

5. Click **OK** in the dialog box that opens, then **Next** to start the actual agent installation.

6. At the Proxy Information screen, select the **Yes, connect through a proxy server** check box if you intend to use a proxy for Server-Agent communication.

7. Provide the address of the proxy server used by your Control Manager server; you can use either its IP address, or its Fully Qualified Domain Name (FQDN) -- provided the agent's server can resolve the FQDN. Afterwards, Click Next.

Note: Do not select this option if you have configured the Internet Information Service on your Control Manager server to use NT Challenge/Response authentication.

8. The Control Manager Server Information screen opens. Provide the following information on this screen:
   - **Host name (or IP Address):** This is the host name or IP address of your Control Manager server
   - **TCP Port:** This is the port used by the WWW service of your Microsoft Internet Information Service
9. At the Agent Information screen provide the following:
   - **Site:** Provide a site name for the agents. This will appear as a sub-folder name under the Trend VCS Agents folder in the Directory

Tip: A useful system for this would be to specify a name that reflects the agent's geographical location (for example, New_York, Tokyo, Manila).

   - **Relative destination directory:** This determines the placement of the Trend VCS Agent files on the server. This directory is relative to the shared folder you specified earlier.
10. The Installing Agents screen opens. The table shows the installation status of the agents. After the installation, click **OK** in the dialog box that opens. Click **Exit** to end the setup, or **Next** to install agents for other applications.
11. If you clicked **Next**, a dialog box opens. Click **Yes** to install other agents, otherwise click **No**.
12. Click **Finish** at the final screen.

Change Agent Logon Credentials for Remote OfficeScan Servers

The following instructions only apply to the Trend VCS agent for OfficeScan. This agent is used for OfficeScan versions 3.5x to 5.02.

Why change the password?

The agent must have administrative-level access to the server that hosts it. The host server can either be the OfficeScan server itself, if the agent is installed on the OfficeScan machine, or a separate server, if the Agent remote-manages OfficeScan.

These credentials are initially provided during agent installation. If the account originally provided is modified at the host server, the changes must also be applied to the agent.

To change the password:

1. Click **Products** on the main menu.
2. At the Product Directory on the left-hand menu, click the OfficeScan managed product.
3. Click the **Configuration** tab.
4. Click **Change Agent logon credentials for remote OfficeScan servers**.
5. Click **Next**.
6. Provide the following information in the appropriate fields:
   - **User ID**
   - **Password:** You must confirm this in the Confirm password field
7. Click Apply to save the changes.

Installing the Trend VCS Agent Locally

This option works with both file-based and HTTP-based OfficeScan servers. Clicking **Next** in **Step 2**, above, starts the installation procedure below.

Note: For this option, the agent setup program must be run on the Windows 2000 / NT server where the agent is to be installed.

---

1. Select the OfficeScan servers that the agent will manage. There are two ways to do this:

   To select from the list:

   a. At the left-hand 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-hand list box, and then click **Add**. The chosen server appears on the right-hand 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-hand list.

To type 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-hand list box.

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

2. Click **Next** to continue.
3. Provide logon credentials for the target OfficeScan server, and locate the OfficeScan.ini file.

   a. Type an Administrator-level user name and password in the appropriate fields. Re-type the password in the confirmation field.

   b. Type the root directory share (for example, C$) of the drive that contains the OfficeScan.ini file. This enables the **Browse** button.

   c. Click **Browse**, to go to the location of the OfficeScan.ini file. Select the file, and then click **Open**. The browse screen closes, and the path of the ini file appears in the grayed-out field on the lower part of the screen.

4. Click **Next**. This starts server analysis.
5. Click **Next** in the Server Analysis and Installation List screens.
6. At the Agent Server User Account screen, provide an Administrative-level user name and password for the agent server. Click **Next**.
7. At the Proxy Information screen, select the **Yes**, connect through a proxy server check box if you intend to use a proxy for Server-Agent communication.
8. Provide the address of the proxy server used by your Control Manager server; you can use either its IP address, or its Fully Qualified Domain Name (FQDN) -- provided the agent's server can resolve the FQDN. Afterwards, click **Next**.

Note: Do not select this option if you have configured the Internet Information Service on your Control Manager server to use NT Challenge/Response authentication.

---

9. The Control Manager Server Information screen opens. Provide the following information on this screen:
   - **Host name (or IP Address):** This is the host name or IP address of your Control Manager server
   - **TCP Port:** This is the port used by the WWW service of your Microsoft Internet Information Service
10. At the Agent Information screen provide the following:
   - **Site:** Provide a site name for the agents. This will appear as a sub-folder name under the Trend VCS Agents folder in the Directory

---

Tip: A useful system for this would be to specify a name that reflects the agent's geographical location (for example, New_York, Tokyo, Manila).

   - **Relative destination directory:** This determines the placement of the Trend VCS Agent files on the server. This directory is relative to the shared folder you specified earlier.
11. The Installing Agents screen opens. The table shows the installation status of the agents. After the installation, click **OK** in the dialog box that opens. Click **Exit** to end the setup, or **Next** to install agents for other applications.
12. If you clicked **Next**, a dialog box opens. Click **Yes** to install other agents, otherwise click **No**.
13. Click **Finish** at the final screen.

Change Agent Logon Credentials for its Host Server

The following instructions only apply to the Trend VCS agent for OfficeScan. This agent is used for OfficeScan versions 3.5x to 5.02.

Why change the password?

The agent must have administrative-level access to the server that hosts it. The host server can either be the OfficeScan server itself, if the agent is installed on the OfficeScan machine, or a separate server, if the Agent remote-manages OfficeScan.

These credentials are initially provided during agent installation. If the account originally provided is modified at the host server, the changes must also be applied to the agent.

To change the password:

1. Click **Products** on the main menu.
2. At the Product Directory on the left-hand menu, click the OfficeScan managed product.
3. Click the **Configuration** tab.
4. Click **Change Agent logon credentials for its host server**.
5. Click **Next**.
6. Provide the following information in the appropriate fields:
   - **User ID**
   - **Password:** You must confirm this in the Confirm password field
7. Click **Apply** to save the changes.

Install Control Manager Agent for InterScan VirusWall for UNIX

InterScan VirusWall for Unix installs a variant of the Trend VCS agent, using its own installation routine.

To install the agent:

1. Run the InterScan VirusWall installation script.
2. Choose **1**. Install InterScan VirusWall sub-system.
3. Choose **6**. Modify option of InterScan VirusWall for TVCS.
4. Type "**y**".
5. Choose **9**. Start Installation.

Registering the InterScan VirusWall Agent with a Control Manager Server

You must register the InterScan VirusWall agent with a Control Manager server. You can do either the InterScan VirusWall management console, or the installation script.

Using the Web-based management console:

1. After installing the Trend VCS Agent for InterScan VirusWall, do the following open the InterScan Web-based management console.
2. Choose T**VCS Registration** from the left-hand menu.

3. Click **Register**.

Using the Installation Script:

1. From the UNIX machine where you have installed InterScan VirusWall, run or re-run the InterScan installation program and then choose option **3**.
2. Type a Site name for the InterScan machine and the IP address of the Control Manager server. To make InterScan appear under the same folder in the Product Directory, use the same Site name that was specified in previous iterations of the agent installation program.

Install Trend VCS Agent for ScanMail for Lotus Notes

ScanMail for Lotus Notes versions 2.5x use Trend VCS agents.

The ScanMail for Lotus Notes Agent database, smsolar.nsf (or ntf) must be signed and set up from within Notes before it is accessible from the Control Manager console. You must also set Notes' own Agent restrictions so the database can Run restricted LotusScripts agents.

Read the documentation that came with ScanMail for Lotus Notes, or Notes' own documentation for complete instructions on setting up the ScanMail Agent database after you install it. In addition to signing the database (explained below), Trend Micro recommends you restrict access to the database.

Signing the ScanMail Databases

If you are running Notes version 4.5.1 or above under Windows NT, you need to sign the Agent database (smsolar.nsf). We recommend that you sign using the server id, and specify Sign every design note and Update existing signatures only.

To sign the ScanMail databases:

1. Switch to the Notes server id for the ScanMail machine.
2. From the main menu, click **File > Tools > Server Administration** and select the **ScanMail server**. Click **Database Tools**.
3. Type **smsolar.nsf** in the **Filename:** field.
4. Select **Sign a Database** from the list of available Tools, and select the **Sign every design notes** radio button and **Update existing signatures only** check box.
5. Click **Sign**, then **No** if asked to sign all cross-certifications.

6. Click **Done** to complete the operation.

Setting Agent Restrictions

ScanMail uses LotusScript agents to support Web browser access to the configuration screens and to perform other routine "housekeeping" tasks. For this reason, the Notes id used when ScanMail was installed must be set to Run restricted LotusScripts agents.

Do this in the Address Book by adding the id (typically server id) to the Who can field for Agent Manager > Agent Restrictions > Run restricted LotusScript agents.

1. From the Notes Workspace, double-click the **Address Book** and then bring up the configuration document for the server where ScanMail is installed (via Server > Servers).
2. Locate and click **Agent Manager** to expose the Agent Restrictions options.
3. If no drop-down list appears, double-click **Run restricted LotusScript agents**, otherwise just click the drop-down list to display the contents of the Address Book.
4. Select the appropriate server id and click **Add**.
5. Click **OK**. Close and save your changes to the Address Book.

Note: The Notes error, "Error validating user's agent execution access" may indicate that an inappropriate Notes id was specified for Run restricted LotusScript agents.

---

6. ScanMail uses Notes' own password scheme for restricting database access.

   To set up Notes HTTP passwords, open the Address Book and choose the Person or Group you will grant access to. Type a password in the **HTTP password** field, then close and save your changes. (For additional information regarding HTTP passwords, please consult your Notes documentation.)
7. Stop and restart the Notes HTTP server (for example from the Notes console enter tell HTTP quit and then load HTTP).

Enabling the ScanMail Agent

The Notes HTTP task must be running on the Notes server where the ScanMail agent is installed to access the agent from the Control Manager management console.

In addition, several ScanMail options exist that are unique to Control Manager. They include:

- The option to turn the ScanMail Agent ON or OFF
- The ability to configure how often the ScanMail Agent reports new log data to the Trend VCS server
- The choice of whether to automatically replicate virus pattern files to all ScanMail Notes servers in the cluster

Edit the Notes Control Manager configuration by highlighting the appropriate Server or Group and clicking Configuration above the Server Tree. Click Control Manager Configuration.

Note: If you are using Control Manager to automatically deploy virus pattern updates, disable replication of the smencycl.nsf database.

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 to 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.

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.

Chapter 5

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 5-16

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 an Enterprise edition to Standard edition	n/a	No

TABLE 5-1. Considerations when upgrading to Control Manager 3.0

Trend Micro recommends that you install Control Manager 3.5 on a separate server, rather than upgrading Trend VCS 1.x, Control Manager 2.5, or Control Manager 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 10-5).

  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 servers to version 3.5 servers:

- 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 3.0 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 2.5/3.0 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 *Back up db_ControlManager using SQL Enterprise Manager / osql* 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`

Serial number information	`Cfg_dm_tms_sn value in \Program files\Trend Micro\COMMON\TMI\TMI.cfg`

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

CONTROL MANAGER 2.5/3.0 INFORMATION	LOCATION
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 2.5/3.0 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\TMCM HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TMI HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MSDE HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDE HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMCM HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro_NTP HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro Infrastructure\. . . HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendCCGI HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSSQLServer

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.

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 **Keep existing Database and append new records** 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 packs 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 3.0 server:

- **Rapid upgrade**

  Rapid upgrade works using the following approach:

ORIGINAL SERVER/AGENT	ACTION
Trend VCS 1.8x with Trend VCS 1.8x 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
Control Manager 2.5 or 3.0 with Control Manager 2.5x agents	Registers Control Manager 2.5x agents to Control Manager 3.5 server; Control Manager agents maintain their original Product Directory structure
Control Manager 2.5 or 3.0 with mixed agents	**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 **Control Manager agents:** Registers Control Manager 2.5x agents to Control Manager 3.5 server; Control Manager agents maintain their original Product Directory structure
Control Manager 3.5 with MCP agents	Registers MCP to Control Manager 3.5 server; MCP maintain their original Product Directory structure

TABLE 5-3. Rapid Upgrade

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

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 *Testing Control Manager at One Location* on page 2-13). 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/3.0/3.5 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 Control Manager 3.5 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:

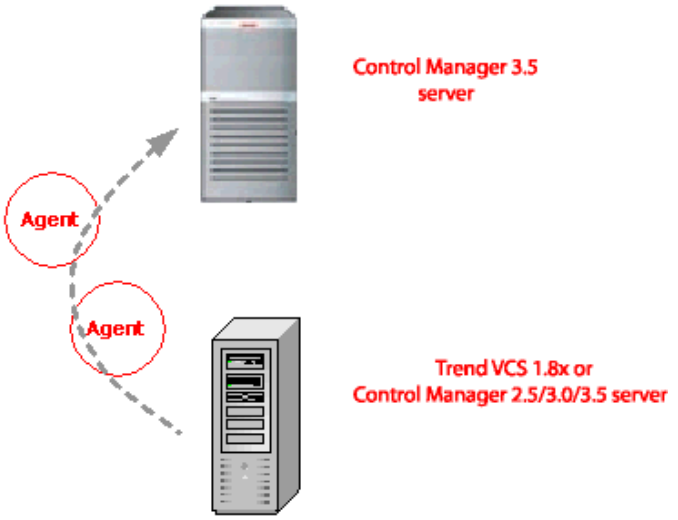


FIGURE 5-1. Migration of agents belonging to a single server

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

- Consolidation of different servers/agents:

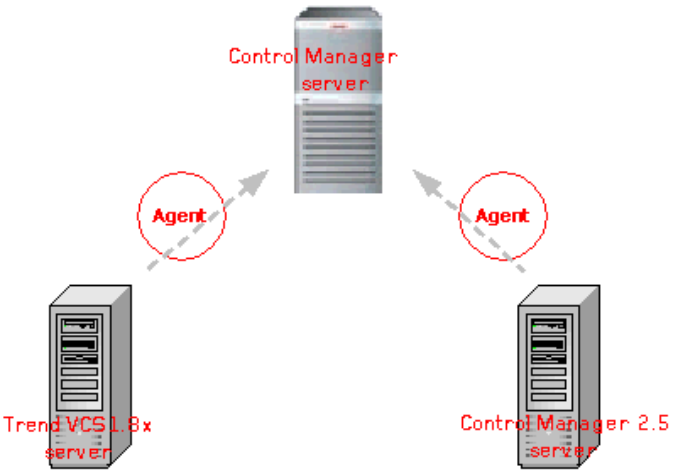


FIGURE 5-2. Migration of agents belonging to multiple servers

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:

1. Upgrades Trend VCS 1.8x agents to version 1.86
2. Removes Trend VCS 1.8x server information from the registry and replaces them with Control Manager 3.5 server information
3. 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:

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

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

MCP Agent Migration Flow

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

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

Migrate Trend VCS, Control Manager 2.x, and MCP Agents

Use `AgentMigrateTool.exe` to migrate Windows-based agents originally administered by Trend VCS 1.8x, Control Manager 2.5, Control Manager 3.0 server, or Control Manager 3.5 server. When migrating agents Trend VCS and 2.5x agents migrate first, then MCP migrates.

If an agent migration is unsuccessful, the following occurs:

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

Migrated logs will not shows logs unless the agents are registered to the destination server. Destination CM server will purge migrated logs when purge is triggered.

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, 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\
   ```

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, Control Manager 2.x, Control Manager 3.0, or Control Manager 3.5 server hosting the agents that will migrate.
5. Under **System Administrator Account**, specify the administrator **user name** and **password** that will be 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` will instruct 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` will copy 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 Manager

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

---

8. Click **Migrate**.

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

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\`

2. Double-click `AgentMigrateTool.exe`.
3. Click **Generate List** from the main menu.
4. Type the **IP address** of the Control Manager 2.5, Control Manager 3.0, or Control Manager 3.5 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 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 5-13* 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.

Chapter 6

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 6-23
- *Manage Child Servers* on page 6-27
- *Download and Deploy New Components* on page 6-32

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.

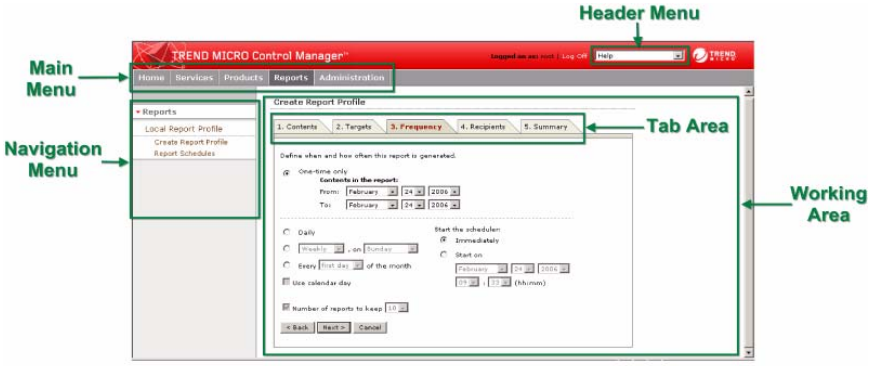


FIGURE 6-1. Control Manager Management Console

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

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

MAIN MENU	
Home	Includes shortcuts to Status Summary tab and available managed products reports
Services	Includes TrendLabs Message Board posts and available services
Products	Includes options to administer Managed Products, Communicators, and Child servers
Reports	Includes options to manage Control Manager managed products and child server reports
Administration	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	User Manager Directory Manager
Directory Manager	User Manager Directory Manager
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

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

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

  b. Provide the **user name** and **password** in the field provided.

  c. Click **Enter**.

- Remotely using any compatible browser

  To access the console remotely:

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

  `http://{hostname}/ControlManager`

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

  b. Provide the **user name** and **password** in the field provided.

  c. Click **Enter**.

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

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

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 appears:

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.

Log Off from the Management Console

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

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

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
HOME			
	●	●	●
SERVICES			
TrendLabs Message Board			●
Outbreak Prevention Services			●
Damage Cleanup Services			●
Vulnerability Assessment			●
PRODUCTS			
Add/Remove Product Agents	●	●	●

FIGURE 6-2. User Account Access

MENU ITEM	OPERATOR	POWER USER	ROOT/ADMINISTRATOR
PRODUCTS			
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			●
REPORTS			
Create Report Profile		●	●
Scheduled Reports		●	●
ADMINISTRATION			
Command Tracking	●	●	●
Event Center			●
Update Manager		●	●
Logs - Query or Purge			●
User Manager > My Account	●	●	●
User Manager > User Accounts			●
User Manager > User Groups			●
System Settings			●

FIGURE 6-2. User Account Access

MENU ITEM	OPERATOR	POWER USER	ROOT/ADMINISTRATOR
ADMINISTRATION			
Tools			●
Registration			●

FIGURE 6-2. User Account 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.

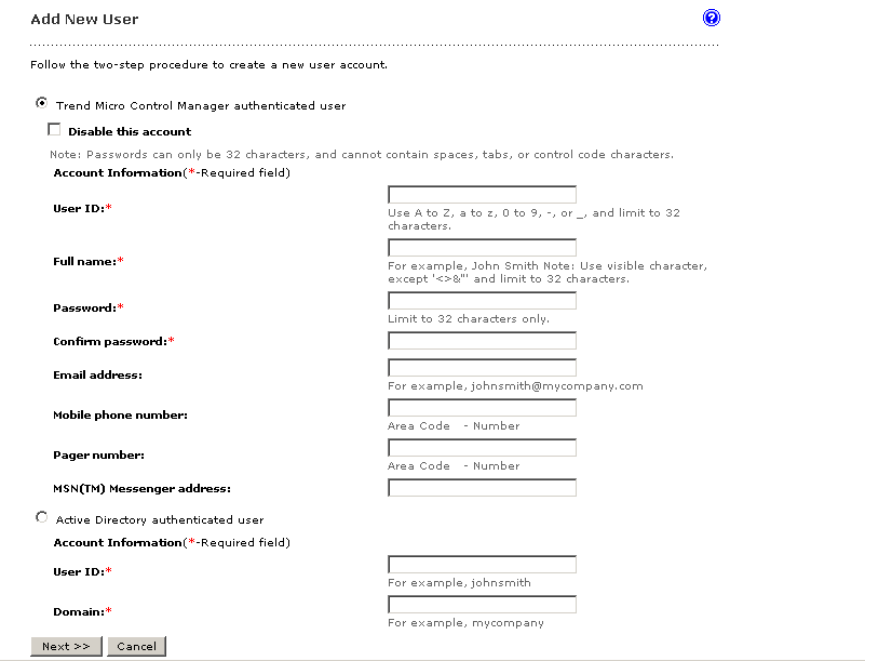
Note: Active Directory users cannot have their accounts disabled from Control Manager. To disable an Active Directory user you must disable the account from the Active Directory server.

To add a user account:

1. Click **Administration** on the main menu.

2. On the left menu, click **User Accounts**. The User Accounts screen appears.

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**.

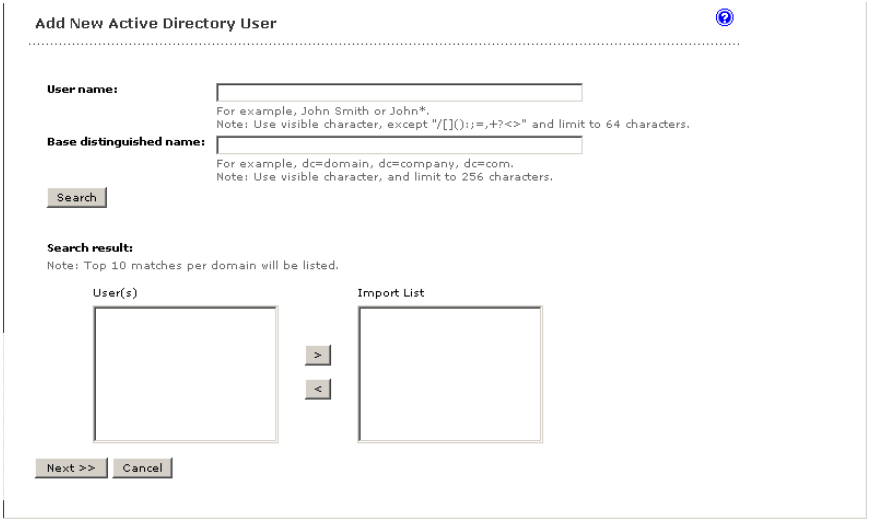
Import Active Directory Users

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.

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

To import 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. The 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.

---

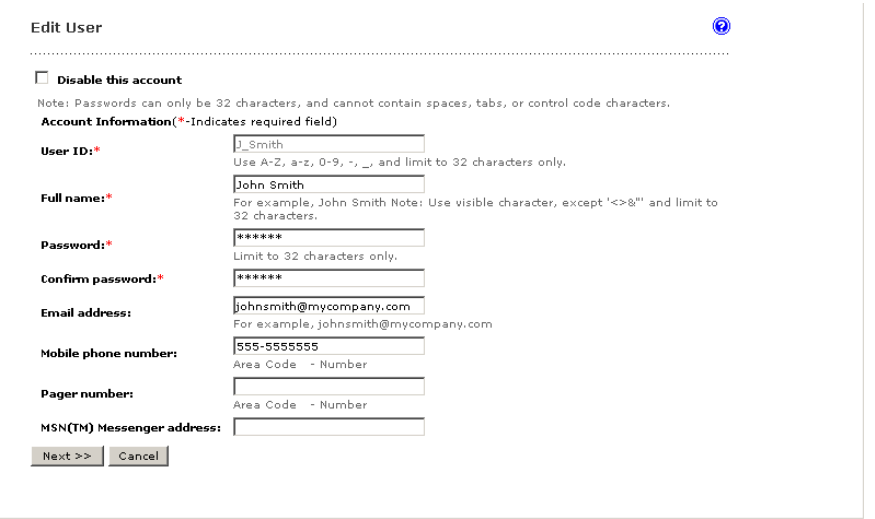
10. Click **Apply**.

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:

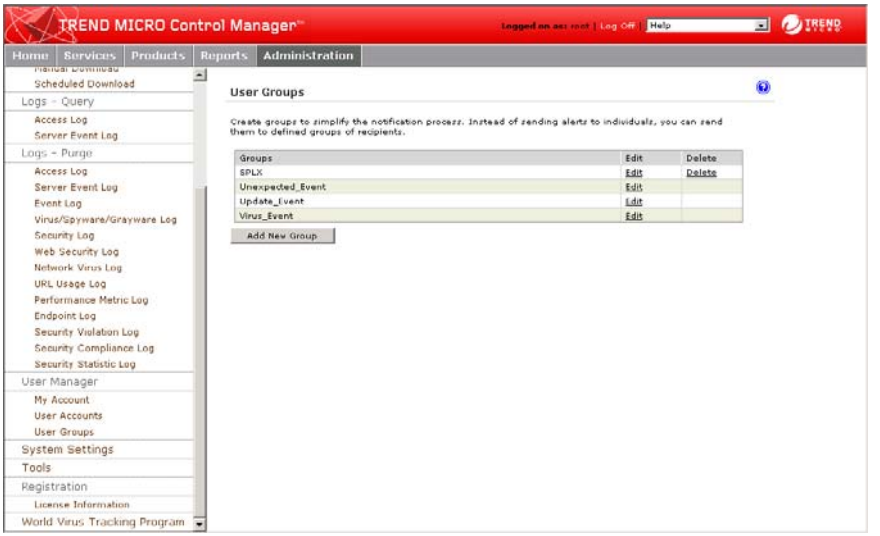
1. Click **Administration** on the main menu.
2. On the left menu, click **User Accounts**.
3. On the working area, click **Delete** beside the account.
4. Click **OK** to delete the account.

Add a User Group

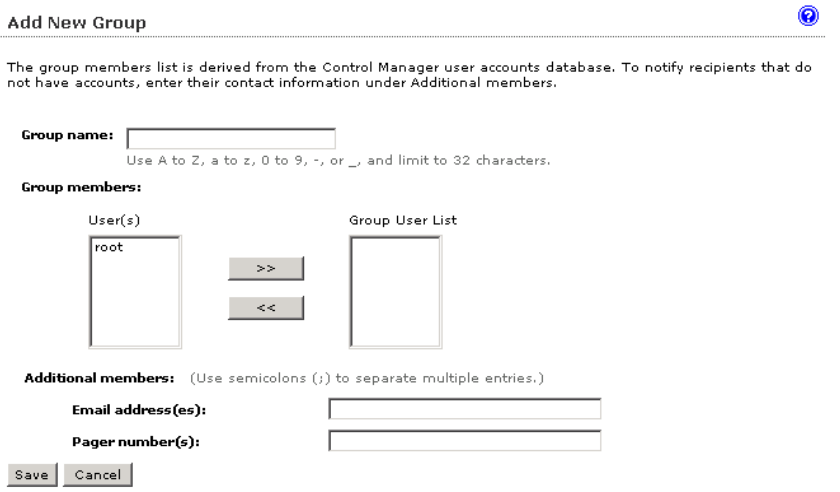
User groups simplify the management of Control Manager users by providing a convenient way to send notifications to a single group rather than to individual users. You can add users to groups according to similar properties including: user types, location, or the type of notifications they should receive. 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**.



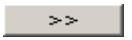
3. On the working area, click **Add New Group**.



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:

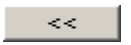
   a. Select a user from the User(s) list. Use the CTRL key to select multiple users.

   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 the number your company uses to dial out and a comma "," [each comma causes a 2 second pause])

Separate multiple entries with semicolons.

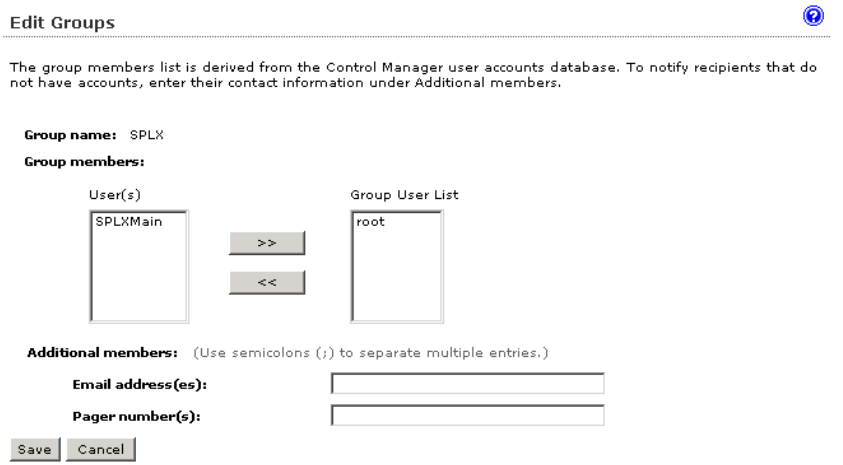
6. Click **Save**.
7. Click **OK**.

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. Control Manager now supports dynamic icons, which change with the status of the managed product. See your managed product's documentation for more information on the icons and associated status' for your managed product.

Indirectly administer the managed products either individually or by groups through the Product Directory. 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.

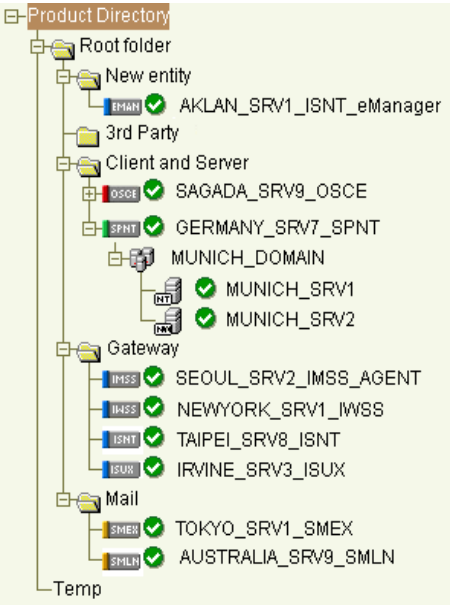
- **Deployment planning**

  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. 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
Product Status	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	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.
Tasks	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.
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 6-4. 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. 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 6-5. 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 its own managed products, a parent server indirectly manages the managed products handled directly by child servers.

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

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

TABLE 6-6. Parent and child server feature comparison

FEATURE	AVAILABLE IN PARENT	AVAILABLE IN CHILD
Create global reports	Yes	No

TABLE 6-6. 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, Content Security, and Web Security summaries
- Query Event or Security logs
- Initiate tasks
- View reports
- Access the child server management console

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

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 10-3 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. Trend Micro recommends updating the antivirus and content security components to remain protected against the latest virus and malware threats. By default, Control Manager enables virus pattern, damage cleanup template, and Vulnerability Assessment pattern download even if there is no managed product registered on the Control Manager server.

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

- **Pattern files/Cleanup templates** - 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 program** - 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.

Pattern files/Cleanup templates contain hundreds of malware signatures (for example, viruses or Trojans) and determine the managed product's ability to detect and clean malicious file infections.

PATTERN FILES/CLEANUP TEMPLATES	DESCRIPTION
Virus pattern	If a particularly damaging virus is discovered “in the wild,” or actively circulating, Trend Micro releases a new pattern file as soon as a detection routine for the threat is available (usually within a few hours) As virus authors and malicious content writers release new viruses to the public, Trend Micro collects their telltale signatures and incorporates the information into the virus pattern file. Because new and virulent viruses are discovered every day, Trend Micro frequently makes available new versions of the virus pattern, often 2-3 times a week depending on the need and threat-risk. By default, all Trend Micro antivirus applications automatically update the virus pattern less often than once a week.
Spyware/Grayware Scan pattern file	Similar to the Virus pattern, anti-spyware/grayware managed products use this file to detect spyware/grayware on clients.
Damage Cleanup Template	Damage Cleanup Services pattern
Network virus pattern file for NVW	Similar to the Virus pattern, Network VirusWall devices use this file to detect network viruses (for example, Trojans) in your network
Network Outbreak Rule	Network VirusWall component used to optimize performance of your Network Outbreak Monitor settings This enables you to detect suspicious activity on the network that may signal a virus infection or attack.
Vulnerability Assessment Pattern	Vulnerability Assessment (VA) rule used for detecting computer vulnerabilities
Vulnerability Information Database	Vulnerability Assessment (VA) database used for identifying computer vulnerabilities
Network virus pattern file for Desktop	Component used for detecting network viruses on desktop environments
Spyware/Grayware Cleanup pattern file	Component used to remove and cleanup spyware/grayware files

TABLE 6-7. Pattern files/Cleanup templates

PATTERN FILES/CLEANUP TEMPLATES	DESCRIPTION
Spyware/Grayware pattern file	Component used to detect hidden but legal program that secretly collects confidential information
Phish pattern for InterScan Web Security product line	Component used by InterScan products to detect phish

TABLE 6-7. Pattern files/Cleanup templates

Anti-spam rules are the Trend Micro-provided files used for anti-spam and content filtering.

ANTI-SPAM RULES	DESCRIPTION
Import file	Used for content filtering; the Control Manager server downloads the import file from the ActiveUpdate server
Rule file	Used for message header filtering; the Control Manager server instructs the managed product server to download the latest version from the ActiveUpdate server.

TABLE 6-8. Anti-spam rules

Engines refer to virus/malware scan engines, damage cleanup engine, VirusWall engines, and spyware/grayware engine. By default, Control Manager enables 32-bit DLL (NT/2000), damage cleanup engine, and vulnerability assessment engine

download even if there is no managed product registered on the Control Manager server. These components perform the actual scanning and cleaning functions.

ENGINES	DESCRIPTION
Virus scan engine	At the heart of all Trend Micro products lies a proprietary scan engine, known as virus scan engine application interface (VSAPI), that is capable of detecting all virus known to be “in the wild”, or actively circulating The 32-bit, multi-threaded scan engine checks files in real-time using the process called pattern matching. VSAPI also employs a number of heuristic scanning technologies that even allows it to detect new viruses, not yet seen in the wild. In addition to viruses, the scan engine protects against mass mailing worms such as Nimda and CodeRed, macro and polymorphic viruses, Trojans, and Distributed Denial of Service (DDoS) attacks. The scan engine includes an automatic clean-up routine for old virus pattern files (to help manage disk space), as well as incremental pattern updates (to help manage bandwidth).
Rule file	Used for message header filtering; the Control Manager server instructs the managed product server to download the latest version from the ActiveUpdate server.
Damage cleanup engine	Damage Cleanup Services engine
Network VirusWall 2500 1.x engine	Network VirusWall 2500 1.x engine
Network VirusWall Enforcer 2500 engine	Network VirusWall Enforcer 2500 engine
Network VirusWall 1200 1.x engine	Network VirusWall 12001.x engine
Vulnerability Assessment engine	VA engine used for detecting computer vulnerabilities
Common Firewall Driver (NTKD)	Common Firewall driver for NT-based Windows products used for endpoint protection
Common Firewall Driver (VXD)	Common Firewall driver for early Windows products used for endpoint protection
Spyware/grayware scan engine	Scan engine used for detecting spyware/grayware

TABLE 6-9. Engines

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

Tip: To minimize Control Manager network traffic, disable the download of components that have no corresponding managed products or services. When you register managed products or activate services at a later time, be sure to configure the manual or scheduled download of applicable components.

Understanding Update Manager

Update Manager provides functions that help you update the antivirus and content security components of your Control Manager network.

Updating the Control Manager network involves two steps:

- Downloading components: You can do this manually or by schedule
- Deploying components: You do this manually or by schedule

Understanding Manual Downloads

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 Download Components

This is the Trend Micro recommend method of configuring manual downloads. Manually downloading components requires multiple steps:

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

Step 1: Configure a Deployment Plan for your components

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

Step 3: Select the components to update

Step 4: Configure the download settings

Step 5: Configure the automatic deployment settings

Step 6: Complete the manual download

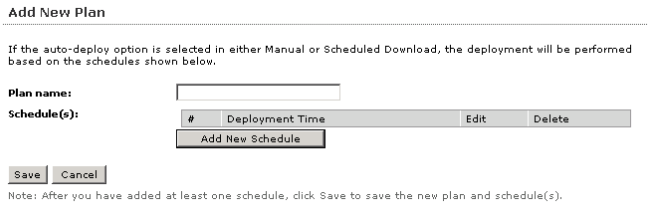
To manually download components:

Step 1: Configure a Deployment Plan for your components

1. Click **Administration** on the main menu.

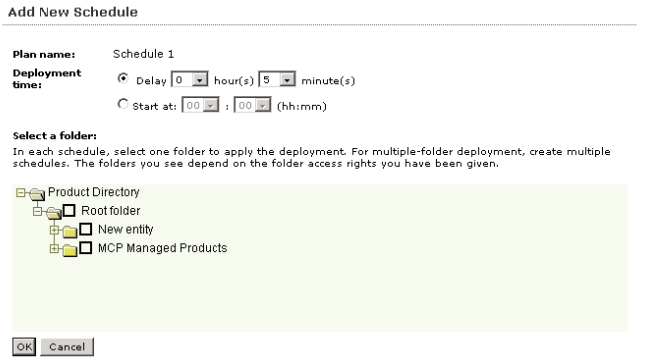
2. On the left menu under Update Manager, click **Deployment Plan**. The Deployment Plan screen appears.

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.



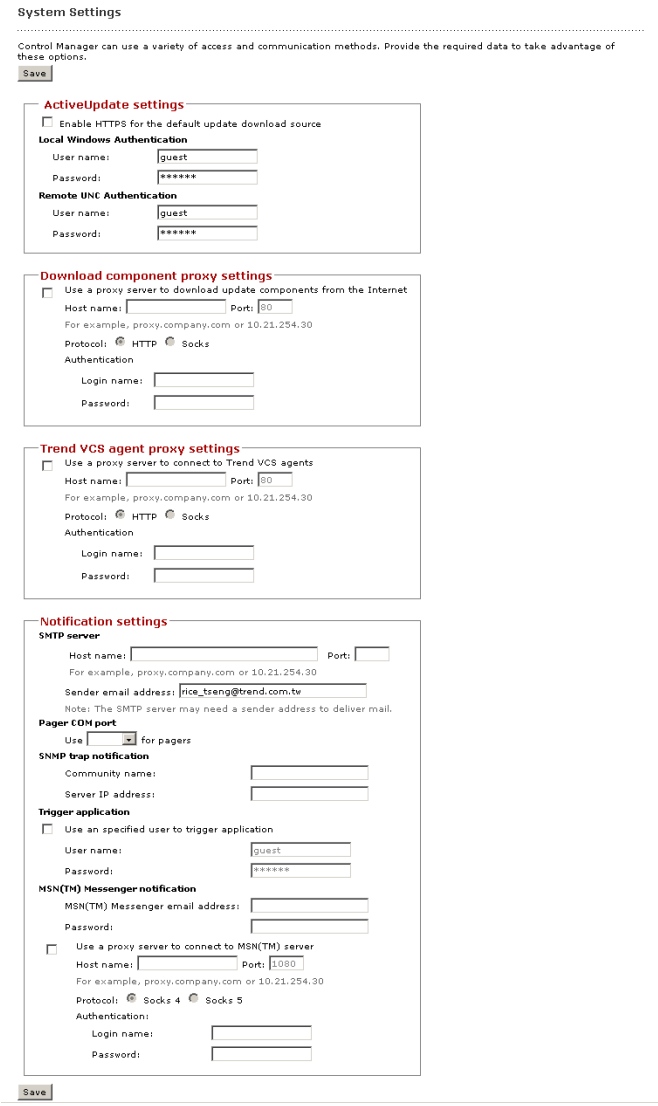
6. On the Add New Schedule screen, choose a deployment time schedule by selecting one the following options:
   - **Delay** - after Control Manager downloads the update components, Control Manager delays the deployment according to the interval you specify

     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, if you use a proxy server

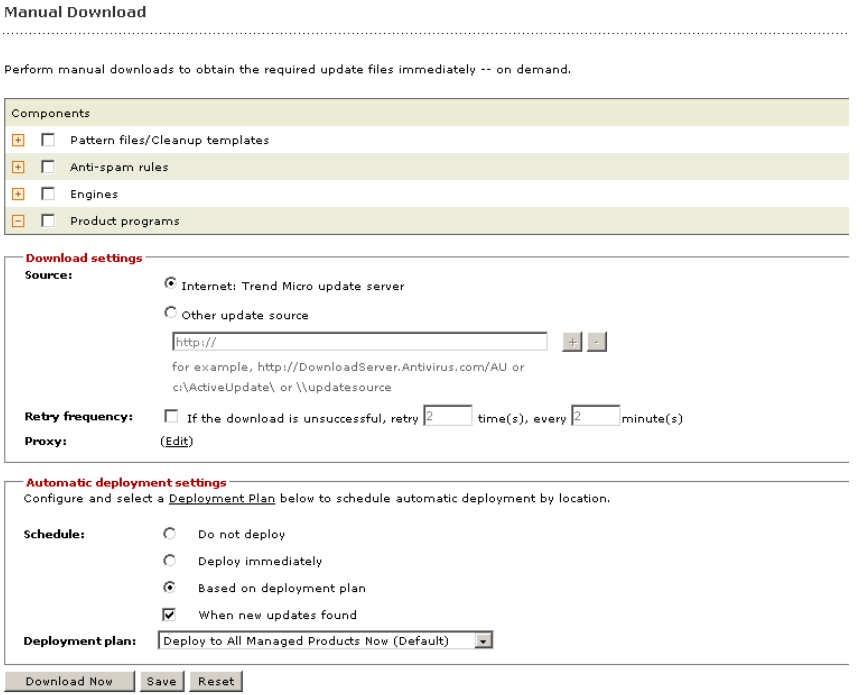
1. Click **Administration > System Settings**. The System Settings screen appears.



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.
   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 download settings

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

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

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

---

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

Step 5: Configure the automatic deployment settings

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

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

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

Step 6: Complete the manual download

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

Access Manual Download

Use the Manual Download screen to immediately obtain new components.

To access the Manual Download screen:

1. Click **Administration** on the main menu.
2. On the leftmost menu under Update Manager, click **Manual Download**.

Configure Manual Download Settings

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

To configure manual download settings:

1. Access the Manual Download screen.
2. On the working area under Download Settings:
   a. Select components that you want to download.
   b. Select the update source:
      - Internet: Trend Micro update server to download components from the official Trend Micro ActiveUpdate server.
      - **Other update source:** Type the URL of the update source in the accompanying field.

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

c. Select Retry frequency and specify the number or retries and duration between retries for downloading components.

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

---

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

3. Click **Save**.

Configure Manual Download and Automatic Deployment Settings

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

To configure manual download Automatic Deployment Settings:

1. Open the Manual Download screen.
2. 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

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

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

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

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

Configure Scheduled Download Exceptions

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

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

To configure scheduled download exceptions:

1. Click **Administration** on the main menu.
2. On the left-hand menu under Update Manager, click **Scheduled Download Exceptions**.
3. Do the following:
   - To schedule a daily exception, under Daily schedule exceptions, select the check box of the day(s) to prevent downloads, and then select the **Do not download updates on the specified day(s)** check box. Every week, all downloads for the selected day(s) are blocked.
   - To schedule an hourly exception, under Hourly schedule exceptions, select the hour(s) to prevent downloads, and then select the **Do not download**

updates on the specified hour(s) check box. Every day, all downloads for the selected hours are blocked.

4. Click **Save**.

Understanding Scheduled Downloads

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

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

- **Frequency:** Shows how often the component 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

Configuring scheduled component downloads requires multiple steps:

Step 1: Configure a Deployment Plan for your components

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

Step 3: Select the components to update

Step 4: Configure the download schedule

Step 5: Configure the download settings

Step 6: Configure the automatic deployment settings

Step 7: Enable the schedule and save settings

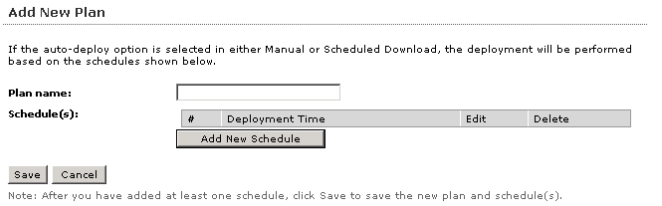
Configure Scheduled Downloads and Enable Scheduled Component Downloads

Step 1: Configure a Deployment Plan for your components

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.

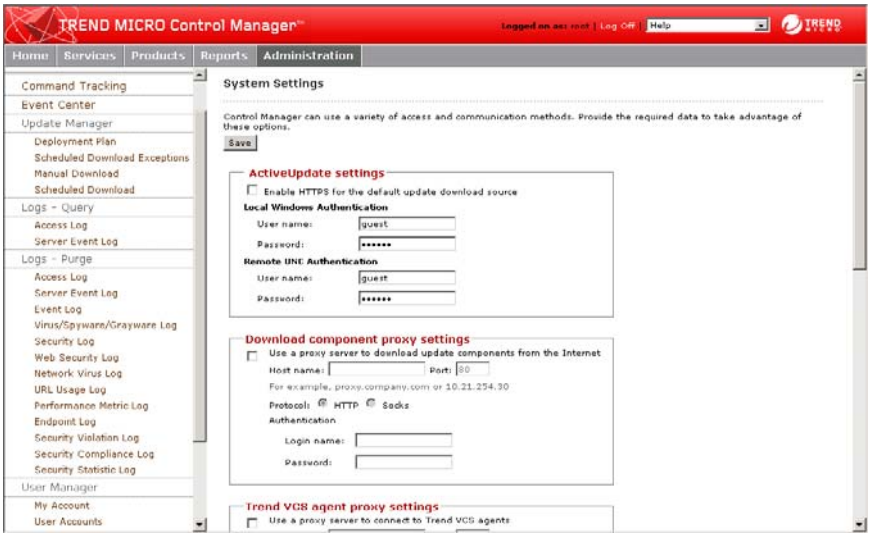
- **Start at** - Performs the deployment at a specific time

  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, if you use a proxy server

1. Click **Administration > System Settings**. The System Settings screen appears.



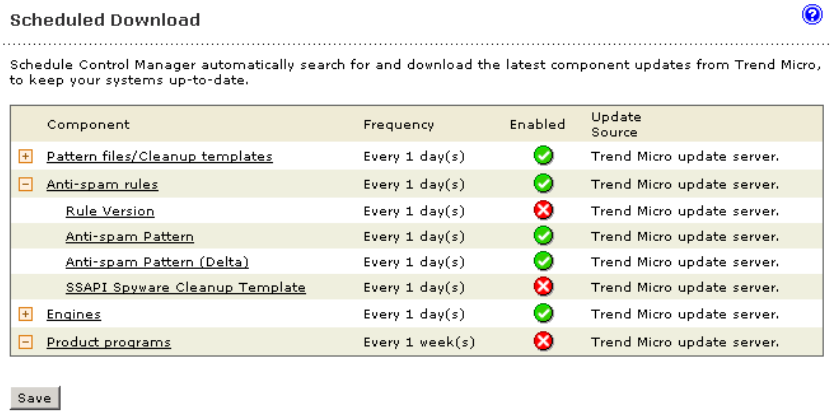
2. Select the **Use a proxy server to download update components from the Internet** checkbox in the Download component proxy settings area.
3. Type the host name or IP address of the server in the **Host name** field.
4. Type a port number in the **Port** field.
5. Select the protocol:

- HTTP
- SOCKS

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

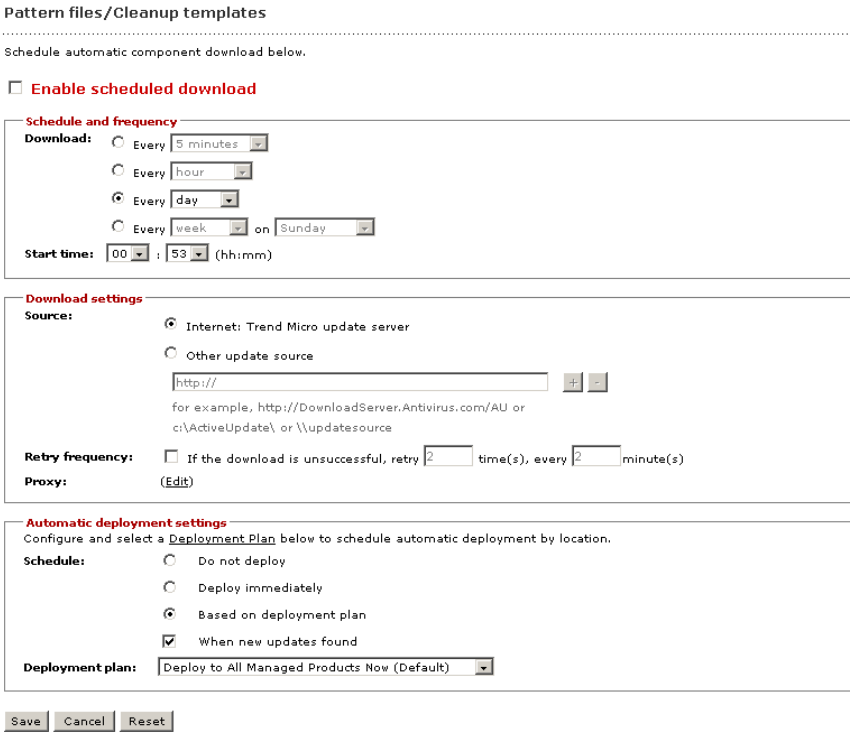
Step 3: Select the components to update

1. Click **Administration > Update Manager > 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 components to download. To select all components for a group, select:
      - **Patterns/rules**
      - **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 download schedule

1. Select the **Enable scheduled download** check box to enable scheduled download for the component.
2. Define the download schedule. Select a frequency, and use the appropriate drop down menu to specify the desired schedule. You may schedule a download 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 download settings

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

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

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

---

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

Step 6: Configure the automatic deployment settings

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

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

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

Step 7: Enable the schedule and save settings

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

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 > Update Manager > 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 components to download. To select all components for a group, select:
      - **Patterns/rules**
      - **Anti-spam rules**
      - **Engines**
      - **Product programs**

      The <Component Name> screen appears. Where <Component Name> is the name of the component you selected.
3. Under Schedule and frequency:
   a. Define the download schedule. Select a frequency, and use the appropriate drop down menu to specify the desired schedule. You may schedule a download every minute, hour, day, or week.

b. Use the **Start time** drop-down 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 > Update Manager > 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 components to download. To select all components for a group, select:

- **Patterns/rules**
- **Anti-spam rules**
- **Engines**
- **Product programs**

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

Under Download settings:

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

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

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

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

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

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

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 > Update Manager > 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 components to download. To select all components for a group, select:
      - **Patterns/rules**
      - **Anti-spam rules**
      - **Engines**
      - **Product programs**

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

Under Automatic deployment settings

3. Select when to deploy downloaded components from the Schedule area. The options are:
   - **Do not deploy:** Components download to Control Manager, but do not deploy to managed products. Use this option under the following conditions:
     - Deploying to the managed products individually
     - Testing the updated components before deployment

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

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

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

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

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

Configure System Settings

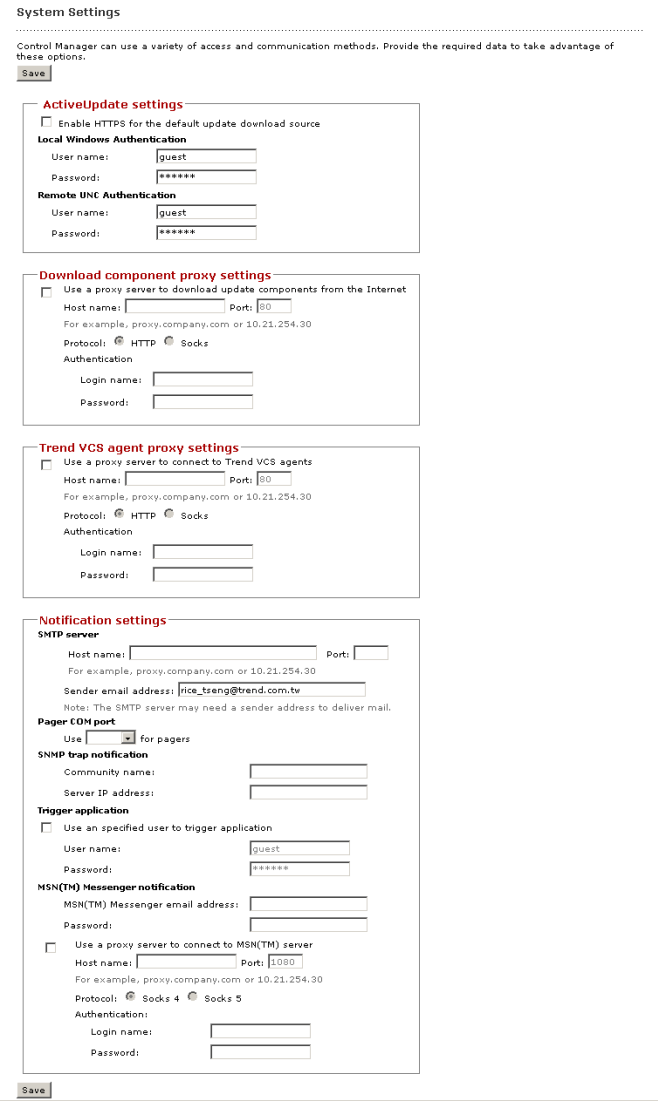
The System Settings screen to provides you with methods to configure the following settings:

- **ActiveUpdate settings:** Used for downloading components from the official Trend Micro ActiveUpdate server
- **Download component proxy settings:** Used for downloading components with a proxy server
- **Trend VCS agent proxy settings:** Used for TVCS agent component downloads
- **Notification settings:** Used for alerts sent by a variety of methods

To access System Settings:

1. Click **Administration** on the main menu.

2. On the left menu, click **System Settings**.



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**.
3. On the working area under Download component proxy settings or Trend VCS agent proxy settings, set the proxy server settings:
   a. If you are using a proxy server to connect to the Internet:
      - On the working area under Download component proxy settings, click **Use a proxy server to download update components from the Internet**

   b. On the working area under Trend VCS agent proxy settings, click **Use a proxy server to connect to Trend VCS agents**

   c. Specify the proxy server hostname and port.

   d. Select the proxy server protocol — HTTP or Socks.

   e. Type the user name and password used for proxy authentication.
4. 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**.
3. On the working area under ActiveUpdate settings, select **Enable HTTPS for the default update download source**.
4. Click **Save**.
5. Access Manual Download or Scheduled Download.

6. On the working area under **Download settings > Source** group, select **Internet: Trend Micro update server** or specify your organizations component source server in the Other Internet source field.
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 that has permission to share a folder where Control Manager will download updates.

To enable UNC download:

1. Access Click **Administration** on the main menu.
2. On the left menu, click **System Settings**.
3. On the working area under ActiveUpdate settings, provide the local Windows and Remote UNC authentication user names and passwords.
4. Click **Save**.
5. Access Manual Download or Scheduled Download.
6. On the working area under **Download settings > Source** 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:

Step 1: Add Security Configuration Analysis in the Console Root.

1. Click **Start** > **Run**, type `mmc`, and then click **OK**. A blank console window opens.
2. From the Console menu, select **All/Remove Snap-in…**.
3. On the Add/Remove Snap-in window, click **Add** and then select **Security Configuration Analysis**.
4. Click **Add** and then click **OK** to go back to the console window.

Step 2: Run Configure Computer Now and Analyze Computer Now.

1. On the left-pane, right-click the **Security Configuration and Analysis** scope item and then select **Open database…** from the pop-up menu.
2. On the Open database window, type the name for the security database file and then click **Open**.
3. On the Import Template window, select `basicsv.inf` from the security template lists and then click **Open**.
4. On the left-pane, right-click the **Security Configuration and Analysis** scope item and then select C**onfigure Computer Now…** from pop-up menu.
5. Provide the error log file name and then click **OK**.
6. On the left-pane, right-click the **Security Configuration and Analysis** scope item and then select **Analyze Computer Now…** from pop-up menu.
7. Provide the error log file name and then click **OK**.

Step 3: Set Log on as a batch job policy.

1. On the left-pane, expand the **Security Configuration and Analysis** > **Local Policies** scope item.
2. Click **User Rights Assignment**.
3. On the right-pane, double-click **Log on as a batch job**.
4. On the Analysis Security Policy Setting window, select **Define this policy in the database**.
5. 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**.

6. On the left-pane, right-click **Security Configuration and Analysis**, click **Save** and then click **Configure Computer Now** to apply the changes.

Chapter 7

Monitoring the Control Manager Network

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

This chapter covers the following topics:

- *View Summary Screens in Control Manager* on page 7-2
- *Use Event Center* on page 7-9
- *Work With Logs* on page 7-22
- *Use Reports* on page 7-30

View Summary Screens in Control Manager

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 (For more information on System information groups, see Table 7-1, "System Information Groups," on page 7-2)
- **Security level** - indicates the security setting that you specified during Control Manager installation

SYSTEM INFORMATION	DESCRIPTION
Control Manager server	The host name of the server hosting the Control Manager application
Installed version	The version and build number of the Control Manager program
Registration	The date when 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 when date you registered the product.
Running since	When the Control Manager service was last started
Virus pattern file	The version of the virus pattern used by antivirus products
Anti-spam rule	The version of the spam rule used by content security products
Damage cleanup template	The version of the cleaning template used by Damage Cleanup Services (DCS)
Damage cleanup engine	The version of the engine used by DCS

TABLE 7-1. System Information Groups

SYSTEM INFORMATION	DESCRIPTION
Network outbreak rule	The version of the collaborative antivirus rule file used by packet scanning and antivirus products like Trend Micro Network VirusWall 1200
Network virus pattern file for NVW	The version of the network pattern used by packet scanning products
Network VirusWall 1200 1.x engine	The version of the engine used by packet scanning antivirus products
Network VirusWall 2500 1.x engine	The version of the engine used by packet scanning antivirus products
Network VirusWall Enforcer 2500 engine	The version of the engine used by packet scanning antivirus products
Vulnerability Assessment pattern file	The version of the vulnerability pattern used by Vulnerability Assessment Services (VAS)
Vulnerability Assessment engine	The version of the vulnerability engine used by VAS
Spyware/Grayware scan pattern file	The version of the component used to detect hidden but legal programs that secretly collect confidential information
Spyware/Grayware cleanup pattern file	The version of the component used to remove hidden but legal programs that secretly collect confidential information
Network virus pattern file for desktop	The version of the Network virus pattern file for desktop products
Common Firewall Driver	The version of the Common Firewall Driver used by OfficeScan clients
Rapid anti-spam pattern file	The version of the rapid anti-spam pattern file used by content security products
TMASE pattern file	The Anti-spam pattern file version
SPS PASE Library Windows	The Anti-spam library for Windows
SPS PASE Library Solaris	The Anti-spam library for Solaris
SPS PASE Library Linux	The Anti-spam library for Linux

TABLE 7-1. System Information Groups

SYSTEM INFORMATION	DESCRIPTION
Spyware/Grayware scan engine	The version of the engine used by Anti-Spyware Enterprise Edition 1.0
Spyware/Grayware cleanup template	**The version of the cleaning template used by Anti-Spyware Enterprise Edition 1.0**
Phish pattern for InterScan Web Security product line (IWSS/IWSA)	The version of phish pattern used by the InterScan Web Security product line
Virus scan engine	The platform, version, and update time of the scan engine used by different antivirus managed product services registered to the Control Manager server

TABLE 7-1. System Information Groups

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 Command Tracking later for results.

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

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

TABLE 7-2. Command Tracking Details

INFORMATION	DESCRIPTION
In Progress	The number of managed products or child servers that currently perform the command
All	The total number of managed products and child servers to which Control Manager issued the command

TABLE 7-2. Command Tracking Details

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

Understanding Command Details

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

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

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

- **In Progress:** Indicates the number of managed products or child servers that currently perform the command

Details for the Individual Products or Services

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

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

  These are the Status values:

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

TABLE 7-3. Command Details status

- **Description:** Explains the Status

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

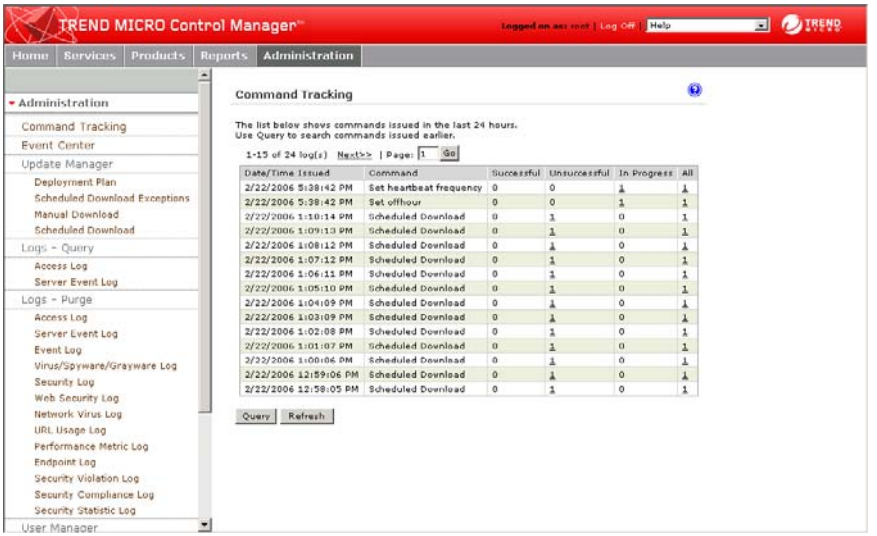
Query and View Commands Issued in the Past 24 Hours

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

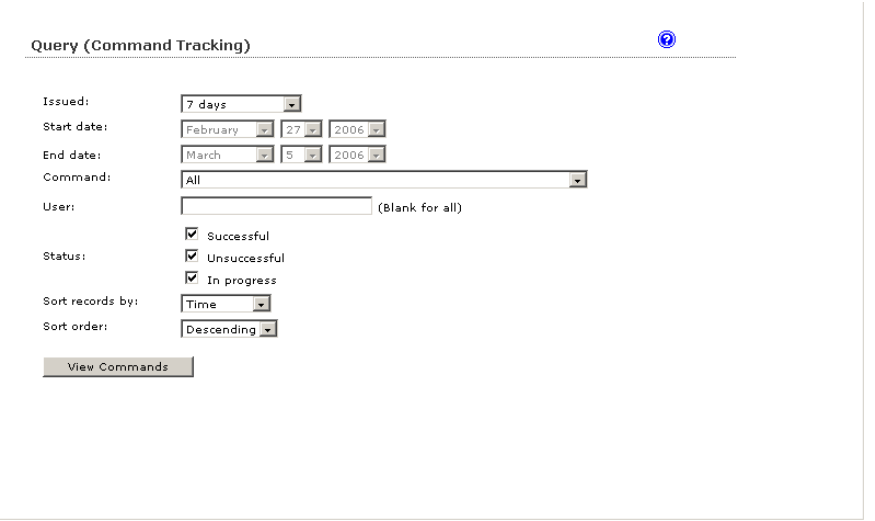
To query and view commands issued in the past 24 hours:

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 the 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 detected by antivirus managed products. For more information, Table 7-4, “Alert Events,” on page 7-10.
- **Outbreak Prevention Services:** Provides information about policy application and update information about Outbreak Prevention Services (OPS)

  Outbreak Prevention Services notification types group the following service events:

  - Active Outbreak Prevention Policy received
  - Outbreak Prevention Mode started
  - Outbreak Prevention Mode stopped
  - Outbreak Prevention Policy update unsuccessful
  - Outbreak Prevention Policy update successful
- **Damage Cleanup Services:** Provides information about policy application and update information about damage cleanup services-related events

  Damage Cleanup Services notification type groups the following service events:

  - Damage Cleanup Services task started
  - Damage Cleanup Services task completed
- **Vulnerability Assessment:** Provides "Vulnerability Assessment task completed" event notification
- **Update:** Provides antivirus and content security components update results (successful or unsuccessful). For more information, Table 7-5, “Update Alert Events,” on page 7-10.

- **Unusual:** Provides information about product options or service activation and deactivation. For more information, Table 7-6, "Unusual Alert Events," on page 7-11.

ALERT	DESCRIPTION
Virus outbreak alert	Applicable to antivirus managed products
Special virus alert	Applicable to antivirus managed products
Virus found	• First and second actions unsuccessful - applicable to antivirus managed products • First action successful - applicable to antivirus managed products • Second action successful - applicable to antivirus managed products
Special spyware/grayware alert	Applicable to anti-spyware/grayware managed products
Spyware/Grayware found	• Spyware/Grayware found - first or second actions successful - applicable to anti-spyware/grayware managed products • Spyware/Grayware found - first and second actions unsuccessful/unavailable - applicable to anti-spyware/grayware managed products
Network virus alert	Applicable to packet scanning products (for example, Network VirusWall 1200)
Potential vulnerability attack detected	Applicable to packet scanning products (for example, Network VirusWall 1200)

TABLE 7-4. Alert Events

ALERT	DESCRIPTION
Scan engine update unsuccessful	Applicable to antivirus managed products
Scan engine update successful	Applicable to antivirus managed products
Pattern files/Cleanup templates update unsuccessful	Applicable to antivirus managed products
Pattern files/Cleanup templates update successful	Applicable to antivirus managed products

TABLE 7-5. Update Alert Events

ALERT	DESCRIPTION
Anti-spam rule update unsuccessful	Applicable to content security managed products
Anti-spam rule update successful	Applicable to content security managed products

TABLE 7-5. Update Alert Events

ALERT	DESCRIPTION
Real-time scan enabled	Applicable to antivirus managed products
Real-time scan disabled	Applicable to antivirus managed products
Product service started	Applicable to antivirus and content security managed products
Product service stopped	Applicable to antivirus and content security managed products

TABLE 7-6. Unusual Alert Events

Customizing Notification Messages

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

These variables are:

TAGS	DESCRIPTION
Common variables used by all event notifications	
%cmserver%	Control Manager server hostname
%computer%	Network name of the client machine where an event was detected
%entity%	Product Directory path of the managed product where an event occurred
%event%	Event that triggered the notification
%pname%	Managed product name

TABLE 7-7. Notification Message Variables

TAGS	DESCRIPTION
%pver%	Managed product version
%time%	Time (hh:mm) when an event occurred
Virus variables: Used by alert or Outbreak Prevention Service event notifications	
%egnver%	• Scan engine version. • Used by the alert event category as well as the Active Outbreak Prevention Policy received and Outbreak Prevention Services started notification types. For the notification types of the alert event category, this variable refers to the scan engine version currently installed on the managed product server. • For the Active outbreak prevention policy received and Outbreak Prevention Services started notification types, this variable refers to the Outbreak Prevention Policy required.
%ptnver%	• Virus pattern version. • Used by the alert event category as well as the Active Outbreak Prevention Policy received and Outbreak Prevention Services started notification types. For the notification types of the alert event category, this variable refers to the virus pattern version currently installed on the managed product server. • For the Active outbreak prevention policy received and Outbreak Prevention Services started notification types, this variable refers to the Outbreak Prevention Policy required.
%threat_info%	• Virus threat information provided by outbreak prevention policies. • Used by Active Outbreak Prevention Policy received and Outbreak Prevention Services started.
%vcnt%	• Trigger value for outbreak alerts. • If the number of detected viruses exceeds this value, Control Manager sends alert notification.
%vdest%	• Virus destination. • For example, the intended recipient takes the value of %vdest% if an antivirus managed product detected a virus in an email. • Used by alert event category.
%vfile%	Infected file name. Used by alert event category.
%vfilepath%	Infected file directory. Used by alert event category.
%vname%	Virus or malware name. Used by alert event category.

TABLE 7-7. Notification Message Variables

TAGS	DESCRIPTION
%vsrc%	• Virus origin or infection source. • For example, the message sender takes the value of %vsrc% if an antivirus managed product detected a virus in an email. • Used by the alert event category as well as the network virus alert notification type.
Special variables: Used by Damage Cleanup Services, Network VirusWall 1200, and Vulnerability Assessment task completed-related events	
%action%	Network VirusWall 1200 action (pass, drop, or quarantine) on network virus.
%description%	Error description used by the Potential vulnerability attack detected, Damage Cleanup Services task completed, and Vulnerability Assessment task completed events.

TABLE 7-7. Notification Message Variables

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 the **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. 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

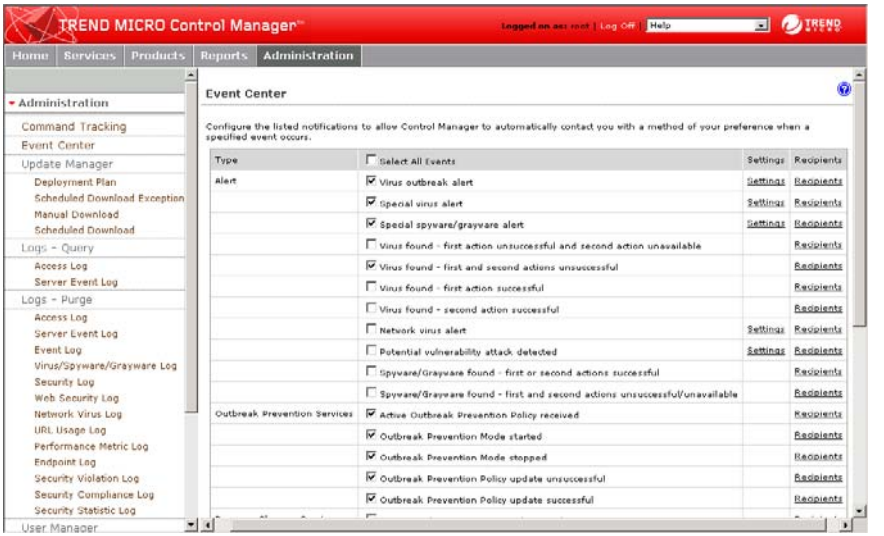
For example, your organization is using a batch file that calls the net send command. Use the **Parameter** field to define commands applied by the trigger application.

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**.



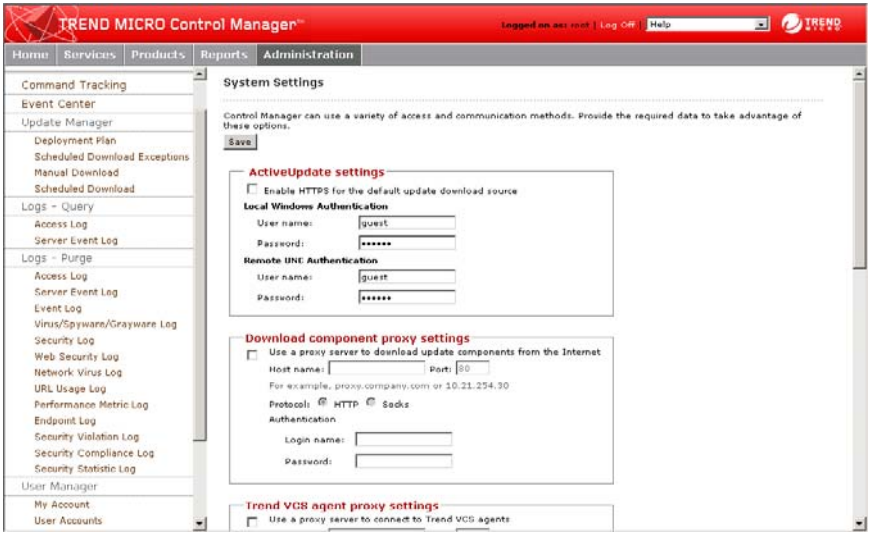
3. Do one of the following:
   - Select/clear the event check boxes.
   - Select/clear Enable all notifications to activate/deactivate Control Manager notifications.
4. Click **Apply**.

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 **System Settings**. The System Settings screen appears.



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**.

   i. Specify the proxy server **hostname** and **port**.

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

   iii. 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**.

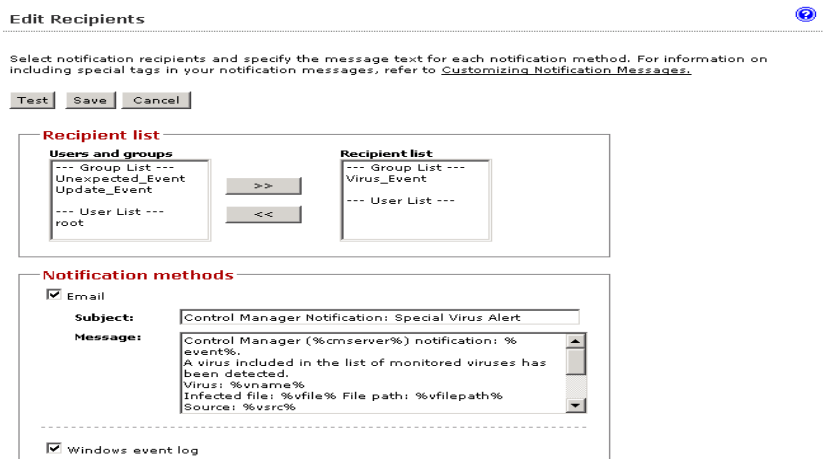
Configure Notification Recipients and Test Notification Delivery

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 to 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* on page 7-15.

6. Provide the **notification message** in the corresponding message fields.

7. Click **Test** to experiment if your system is able to deliver the notifications.

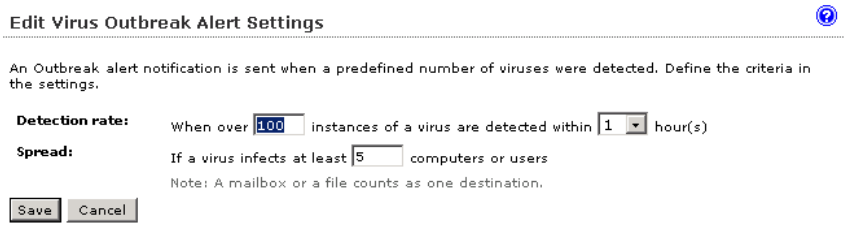
8. Click **Save**.

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**.

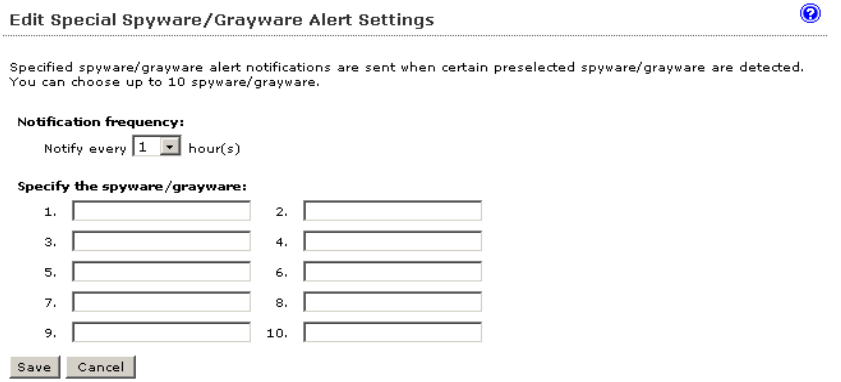
Configure Special Spyware/Grayware Alert Settings

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

To configure special 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 spyware/grayware alert event.



4. On the Edit Special spyware/grayware Alert Settings, specify the **Notification frequency** (in hours) using the list.
5. Type the spyware/grayware names that you want to monitor. You can list up to 10 items of spyware/grayware.
6. Click **Save**.

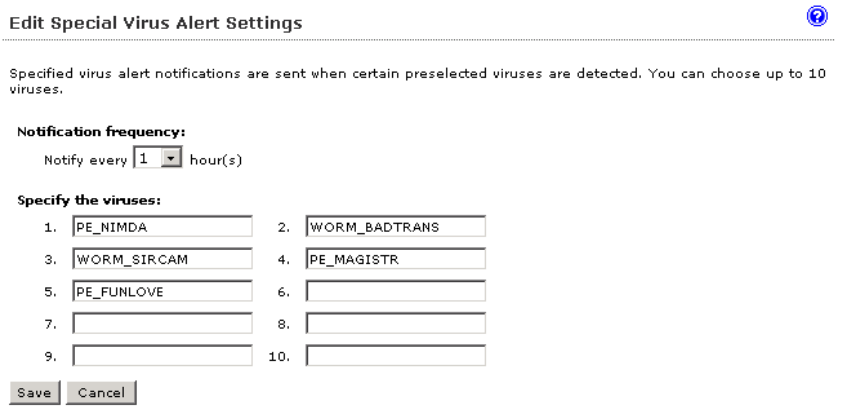
Configure Special Virus Alert Settings

Configure Control Manager to send notifications whenever it detects a virus on your system. Special virus alert notifications provide an early warning 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**.

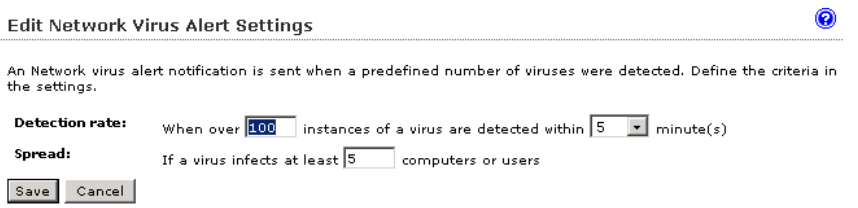
Configure Network Virus Alert Settings

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

To configure network virus alert settings:

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

3. On the working area, click **Settings** adjacent to the Network virus alert event.



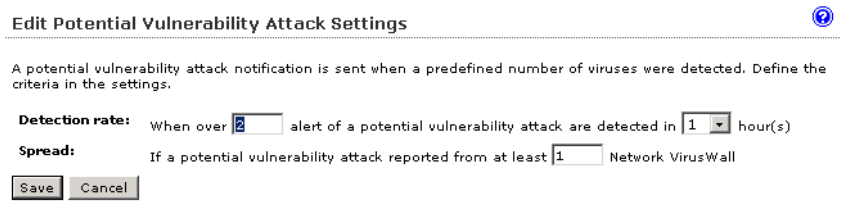
4. On the Edit Network Virus Alert Settings page, provide the following:
   - **Detection rate** - the number of viruses that triggers an outbreak alert
   - **Time period** - the period of consideration for detection rate parameter, in minute(s)
   - **Spread** - the number of computers infected
5. Click **Save**.

Configure Potential Vulnerability Attack Detected Settings

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

To configure potential vulnerability attack detected settings:

1. Click **Administration** on the main menu.
2. On the left menu, click **Event Center**.
3. On the working area, click **Settings** adjacent to the Potential vulnerability attack detected event.



4. On the Edit Potential Vulnerability Attack Settings page, provide the following:
   - **Detection rate** - the number of viruses that triggers an outbreak alert
   - **Time period** - the period of consideration for detection rate parameter, in hour(s)
   - **Spread** - the number of Network VirusWall that reported the potential vulnerability attack
5. Click **Save**.

Work With Logs

Control Manager organizes logs into two categories:

- **Server logs:** Logs generated by parent and child Control Manager servers
- **Client logs:** Logs generated by Control Manager clients and managed products

Server Logs

The Control Manager server generates two kinds of server logs: Access and System Event.

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

TABLE 7-8. Control Manager Server Logs

Client Logs

Client logs provide you with information about the performance of your managed products. You can obtain information for specific or groups of products administered

by the parent or child server. Aside from the Windows Event log, managed products generate different kinds of logs depending on their function.

SERVER LOGS	DESCRIPTION
Event logs	Refer to actions initiated by either a user or the computer. Query all or any of the following events: • Virus outbreak • Module update • Enabling a service • Disabling a service • Security violation • Unusual network virus behavior
Security logs- Virus / Web security	Indicate the source of the infection or intrusion, also referred to as the channel. You can view logs according to the type of channels infected: • Content security violation • Virus found in download traffic • Virus found in email • Virus found in files • Web security violations • Network security violations
Status logs	Contain information about the environment of a managed product or child server. The Status tab uses this information.

TABLE 7-9. Control Manager Client Logs

Control Manager is a client-server system, so managed product logs are also referred to as 'client logs'. Control Manager logs are called 'server logs'.

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

Managed Product	Event Log	Virus/ Spyware/ Grayware Log	Security Log	Web Security Log	Network Virus Log	Status Log	URL usage	Performance Metric Log	Endpoint Log	Security Violation Log	Security Compliance Log	Security Statistic Log
InterScan eManager	●		●			●						●
InterScan Messaging Security Suite	●	●	●			●						●
InterScan WebProtect for ICAP	●	●		●		●	●					●
InterScan for Cisco CSC SSM	●	●	●	●	●	●	●					
OfficeScan Corporate Edition	●	●				●			●			●
ServerProtect	●	●				●						●
ServerProtect for Linux												
ScanMail eManager	●		●			●						●
ScanMail for Domino/Lotus Notes	●	●				●						●
ScanMail for Microsoft Exchange	●	●				●						●

TABLE 7-10. Control Manager Managed Products Logs

Managed Product	Event Log	Virus/ Spyware/ Grayware Log	Security Log	Web Security Log	Network Virus Log	Status Log	URL usage	Performance Metric Log	Endpoint Log	Security Violation Log	Security Compliance Log	Security Statistic Log
Network VirusWall 2500	●				●	●				●	●	●
Network VirusWall 2500	●				●	●				●	●	●
Network VirusWall 1200	●				●	●						

Table 7-10. Control Manager Managed Products Logs

More logs mean abundant available information about the Control Manager system performance.

These many logs occupy more disk space as well. You must balance the need for information with your available system resources.

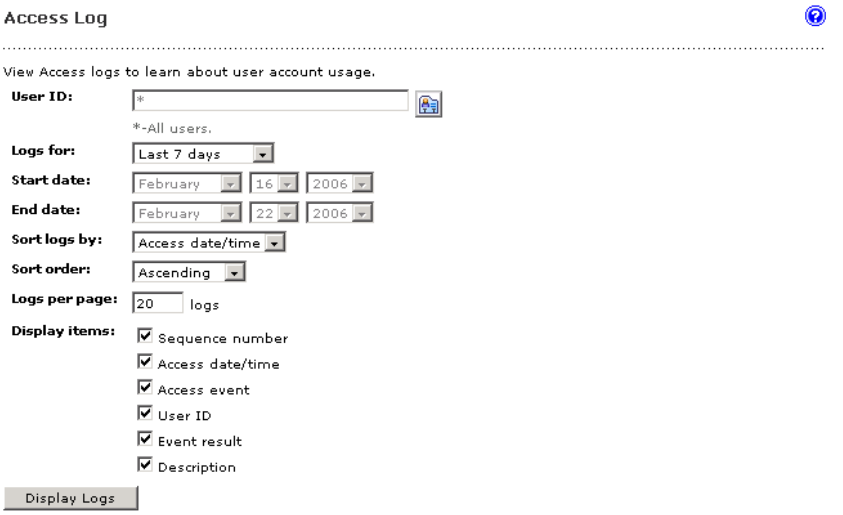
Open Access Log and Server Event Logs

Use the Access Log screen to query and audit user access to the Control Manager management console.

To open the Access Log:

1. Click **Administration** on the main menu.

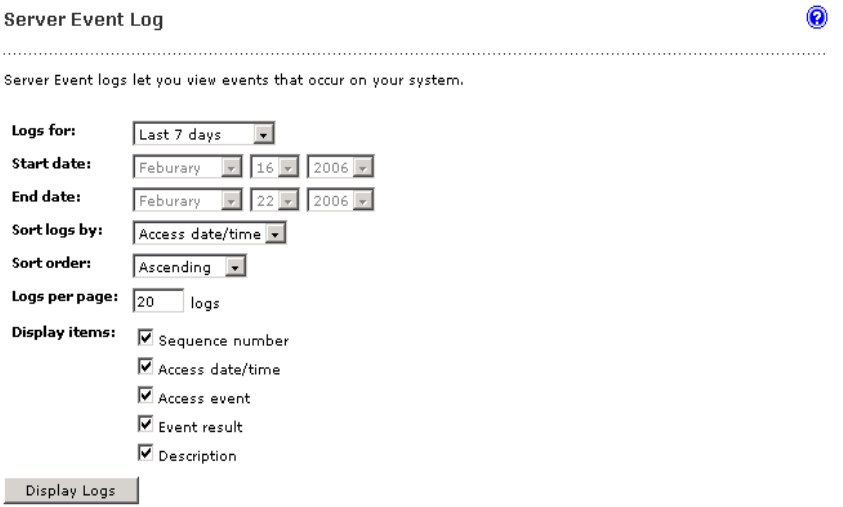
2. On the leftmost menu under Logs - Query, click **Access Log**.



Use the Server Event Log screen to query server event logs.

To open the Server Event Log:

1. Click **Administration** on the main menu.
2. On the leftmost menu under Logs - Query, click **Server Event Log**.



Query Access or Server Event Logs

Use the Access Log or Server Event Log screen to query Access or Server event logs.

To query Access or Server event logs:

1. Open the Access or Server Event Log screen.
2. On the working area, provide the following search parameters:
   - **User ID:** Applies to Access logs; allows you to search for specific users

     Type an asterisk ("*") to view information on all users. To specify a specific user, click , and then enable the check box of required user.
   - **Logs for:** Indicates the scope of your query
   - **Start date:** Indicates the start date (month, day, and year) for the Specified range

- **End date:** Indicates the end date (month, day, and year) for the Specified range
- **Sort logs by:** Sorts logs according to Access date/time, Access event, or User ID (for Access logs only).
- **Sort order:** Displays logs in ascending or descending order
- **Logs per screen:** Indicates the number of logs displayed per screen
- **Items to display:** Indicates the log details displayed

3. Click **View Logs** to start the query.

Save Logs to a *.CSV file

Use the Save Logs as CSV screen to export logs to a CSV file.

To save logs to a *.CSV file:

1. Query Access or Server event logs.
2. On the working area under the Access Logs or System Event Logs results, click **Export Logs into CSV**.

   Control Manager saves the query result in a CSV file with system-defined file name. Depending on the size of the log, it may take a few minutes to generate a CSV file.
3. On Export Logs into CSV, right-click **Retrieve the File** and then select **Save Target As**.
4. On the Save As screen, specify the location where you want to keep the file.
5. Click **Save**.

Note: Use an electronic spreadsheet application (for example, Microsoft Excel) to open *.CSV files.

Open <log type> (Purge Settings)

Use the <log type> (Purge Settings) screen to set purge settings or immediately delete logs for the following types:

- Access Log

- Server Event Log
- Event Log
- Virus Log
- Security Log
- Web Security Log
- Network Virus Log
- URL Usage Log
- Performance Metric Log

To open the <log type> (Purge Settings):

1. Click **Administration** on the main menu.
2. On the leftmost menu under Logs - Purge, click the link corresponding to the <log type>.

Use the <log type> (Purge Settings) screen to purge logs immediately.

To purge logs immediately:

1. Open the <log type> (Purge Settings) screen.
2. On the working area, click **Delete All**.

Configure Purge Log Settings

Use the <log type> (Purge Settings) screen to configure purge settings.

To configure purge log settings:

1. Open the <log type> (Purge Settings) screen.
2. On the working area, select **Enable automatic purge of <log type>**.
3. Specify the maximum number of logs that will be retained (in terms of the number of log entries).
4. In Purge setting, specify the age of logs that will purge.
5. In Purge offset, specify the number of logs to be removed when the maximum number of logs, is reached.
6. 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*
- *Global reports*

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

Local Reports

Local reports are 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.

Use Local Reports screen to view available one-time-only and scheduled local report profiles.

To access Local Reports:

1. Click **Reports** on the main menu.
2. On the leftmost menu under Reports, click **Local Report Profile**.

Note: When you have multiple reports available, sort reports according to Report Profile name or Date Created.

Global Reports

Global reports are reports about managed products administered by child servers as well as the parent server.

Use Global Reports screen to view available one-time-only and scheduled global report profiles.

To access Global Reports:

1. Click **Reports** on the main menu.
2. On the leftmost menu under Reports, click **Global Report Profile**.
3. When multiple reports are available, sort reports according to Report Profile or Last Created date.

Note: Only the parent server can display the global report profiles.

When you have multiple reports available, sort reports according to Report Profile name or Date Created.

Understanding Report Templates

A report template outlines the look and feel of Control Manager reports. In particular, a template defines which sections appear in a report:

- Headers
- Report body
- Footers

Trend Micro Control Manager 3.5 adds 3 new report templates to the 77 previously available since Service Pack 3. The reports added in Service Pack 3 fall into five categories: Desktop, Fileserver, Gateway, MailServer and Executive Summary. The new reports in Control Manager 3.5 fall into a new 6th category: Network Products. This category offers reports related to Network VirusWall.

Note: In Control Manager 3.5 spyware/grayware are no longer considered viruses. This change effects the virus count in all original virus related reports.

To generate these reports, click **Reports** on the main menu, then click **Create Report Profile** under Local Report Profile on the navigation menu. In the Contents tab that appears in the working area, you can enter a report name, an optional report title and an optional report description. Use the **Report Category** list to peruse the six

categories of reports listed below. Clicking a mark into a checkbox includes the associated report in the final exported report file.

DESKTOP PRODUCT REPORTS	REPORT TYPES
Spyware/Grayware Detection Reports	• Spyware/Grayware Detected • Most Commonly Detected Spyware/Grayware (10, 25, 50, 100)
Virus Detection Reports	• Viruses Detected • Most Commonly Detected Viruses (10, 25, 50, 100)
OfficeScan Client Information Reports	• Detailed Summary • Basic Summary
OfficeScan Product Registration Report	Registration Status
Comparative Reports	• Spyware/Grayware, Grouped by (Day, Week, Month) • Viruses, Grouped by (Day, Week, Month)
OfficeScan Server Deployment Reports	• Detailed Summary • Basic Summary • Detailed Failure Rate Summary
OfficeScan Damage Cleanup Services Reports	• Detailed Summary • Most Commonly Cleaned Infections (10, 25, 50, 100)

TABLE 7-11. Desktop Product Reports and Report Types

EXECUTIVE SUMMARY REPORTS	REPORT TYPES
Spyware/Grayware Detection Reports	• Spyware/Grayware Detected • Most Commonly Detected Spyware/Grayware (10, 25, 50, 100) • Detected Spyware/Grayware List for All Entities
Virus Detection Reports	• Viruses Detected • Most Commonly Detected Viruses (10, 25, 50, 100) • Virus Infection List for All Entities

TABLE 7-12. Executive Summary Reports and Report Types

EXECUTIVE SUMMARY REPORTS	REPORT TYPES
Comparative Reports	• Spyware/Grayware, Grouped by (Day, Week, Month) • Viruses, Grouped by (Day, Week, Month) • Damage Cleanups, Grouped by (Day, Week, Month) • Spam, Grouped by (Day, Week, Month)
OfficeScan Server Deployment Reports	• Detailed Summary • Basic Summary • Detailed Failure Rate Summary
Vulnerability Reports	• Machine Risk Level Assessment • Vulnerability Assessment • Most Commonly Cleaned Infections (10, 25, 50, 100) • Worst Damage Potential Vulnerabilities (10, 25, 50, 100) • Vulnerabilities Ranked by Risk Level

TABLE 7-12. Executive Summary Reports and Report Types

GATEWAY PRODUCT REPORTS	REPORT TYPES
Spyware/Grayware Detection Reports	• Spyware/Grayware Detected • Most Commonly Detected Spyware/Grayware (10, 25, 50, 100)
Virus Detection Reports	• Viruses Detected • Most Commonly Detected Viruses (10, 25, 50, 100)
Comparative Reports	• Spyware/Grayware, Grouped by (Day, Week, Month) • Viruses, Grouped by (Day, Week, Month) • Spam, Grouped by (Day, Week, Month)
Deployment Rate Reports	• Detailed Summary • Basic Summary • Detailed Failure Rate Summary

TABLE 7-13. Gateway Product Reports and Report Types

MAIL SERVER PRODUCT REPORTS	REPORT TYPES
Spyware/Grayware Detection Reports	• Spyware/Grayware Detected • Most Commonly Detected Spyware/Grayware (10, 25, 50, 100)
Virus Detection Reports	• Viruses Detected • Most Commonly Detected Viruses (10, 25, 50, 100) • Top Senders of Infected Email (10, 25, 50, 100)
Comparative Reports	• Spyware/Grayware, Grouped by (Day, Week, Month) • Viruses, Grouped by (Day, Week, Month)
Deployment Rate Reports	• Detailed Summary • Basic Summary • Detailed Failure Rate Summary

TABLE 7-14. Mail Server Product Reports and Report Types

SERVER BASED PRODUCT REPORTS	REPORT TYPES
Spyware/Grayware Detection Reports	• Spyware/Grayware Detected • Most Commonly Detected Spyware/Grayware (10, 25, 50, 100)
Virus Detection Reports	• Viruses Detected • Most Commonly Detected Viruses (10, 25, 50, 100) • Top Senders of Infected Email (10, 25, 50, 100)
Comparative Reports	• Spyware/Grayware, Grouped by (Day, Week, Month) • Viruses, Grouped by (Day, Week, Month)
Deployment Rate Reports	• Detailed Summary • Basic Summary • Detailed Failure Rate Summary • OPS Deployment Rate for IMSS

TABLE 7-15. Server Based Product Reports and Report Types

NETWORK PRODUCT REPORTS	REPORT TYPES
Network VirusWall Reports	Policy Violation report: Policy violations, Grouped by (Day, Week, Month)
	Service Violation report: Service violations, Grouped by (Day, Week, Month)
	Most common clients in violation: Clients with the most violations, (10, 25, 50, 100)

TABLE 7-16. Server Based Product Reports and Report Types

Control Manager 3.5 also provides 18 templates stored in `<root>\Program Files\Trend Micro\Control Manager\Reports` as Crystal Report version 9 files (*.rpt). These templates also apply to Local and Global reports.

CONTROL MANAGER 3.0 REPORTS	DESCRIPTION
Top 10 Virus Detection Points Report	Includes the top 10 managed products and number of detected viruses.
All Entities Virus Infection List	Includes all managed products and number of detected viruses.
Top 10 Infected Email Sender Report	Includes the top 10 senders of infected messages and number of infected messages.
Top 10 Infected Files Report	Includes the top 10 infected files.
Daily Virus Count	Includes the number of viruses detected and counted per day.
Top 10 Virus Report	Includes the top 10 viruses detected during the date range specified.
Top 10 Security Violation Report	Includes the top 10 content security policies violated and number of infections.
Deployment Rate	Includes the deployment status, managed product deployed to, last reported time, and percentage completed.
Virus Infection Channel vs. Product	Includes the source of the virus infection and number of infections.

TABLE 7-17. Control Manager 3.0 Reports

CONTROL MANAGER 3.0 REPORTS	DESCRIPTION
Web Security Violations Report	Includes blocking type and rule, as well as the number of web security rule violations.
Desktop Antivirus Protection Summary	Includes virus detection of desktop antivirus managed products (for example, OfficeScan).
Filter Events by Frequency Report	Includes InterScan Messaging Security Suite virus and spam detection.
Filter Events by Policy Report	Includes messages filtered according to InterScan Messaging Security Suite policies.
Spam Summary for Recipients Report	Includes the top 10 spam recipients and spam information.
Spam Summary for Domains Report	Includes the top 10 domains affected by spam.
OfficeScan Deployment Status	Includes an OfficeScan server deployment status. This template is only available when creating local reports.
Outdated OfficeScan Client	Includes OfficeScan clients that do not have the current components (virus pattern, scan engine, product program) as the OfficeScan server. This template is only available when creating local reports.
Consolidated Report	Includes information available in the other 17 Control Manager 3.0 original templates. A Global Consolidated Report profile generates information provided by all templates, except those provided by the Deployment Rate template.

TABLE 7-17. Control Manager 3.0 Reports

Understanding Report Profiles

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

Note: 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

Creating a report profile is a five-step process. Creating local or global reports, the process stays very similar. The process to create a report profile is as follows:

Step 1: Select whether to create a local or global report

Step 2: Configure the Contents tab settings

Step 3: Configure the Targets tab settings

Step 4: Configure the Frequency tab settings

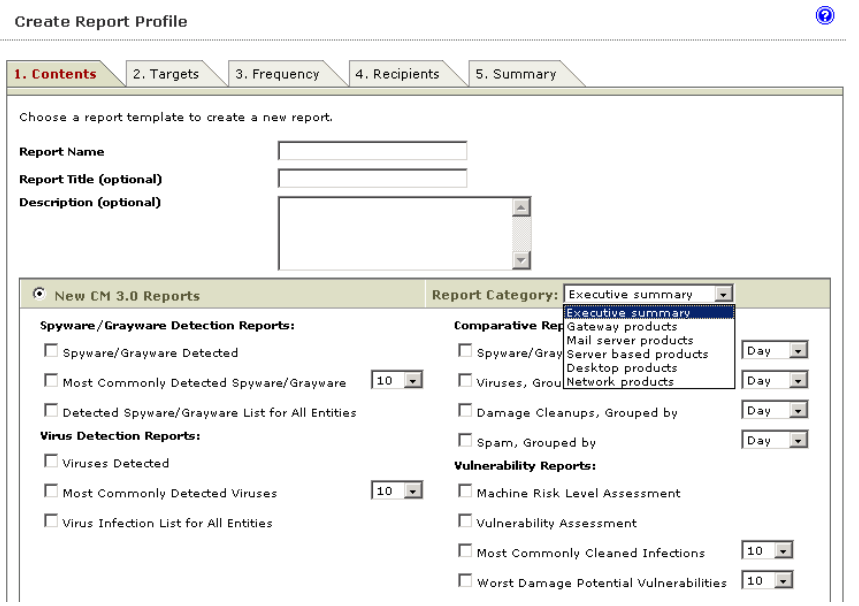
Step 5: Configure the Recipient tab settings

To create local or global report profile:

Step 1: Select whether to create a local or global report

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.

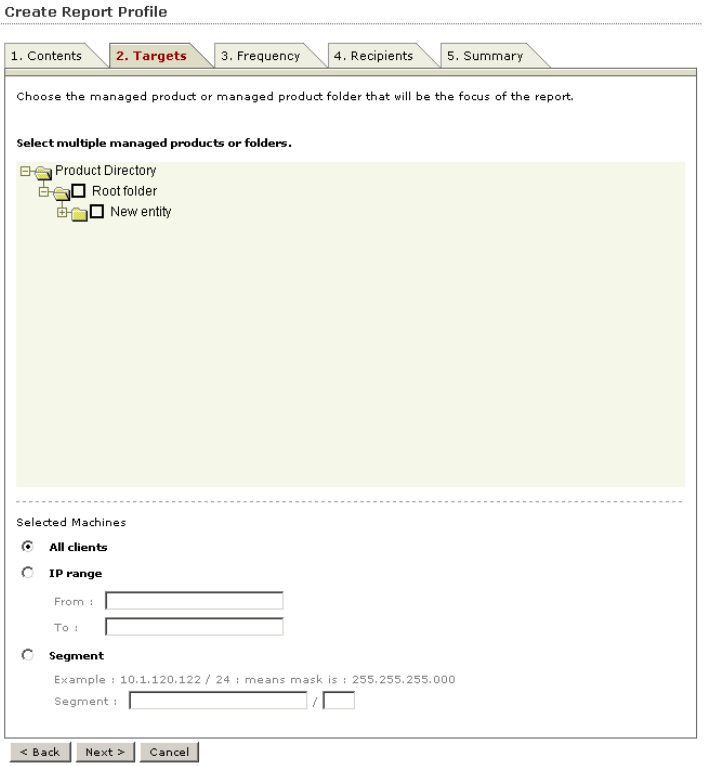
3. On the left menu under Local Report Profile or Global Report Profile, click **Create Report Profile**.



Step 2: Configure the Contents tab settings

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. Select the report template from the **Select report template** list.
5. Select the report format.

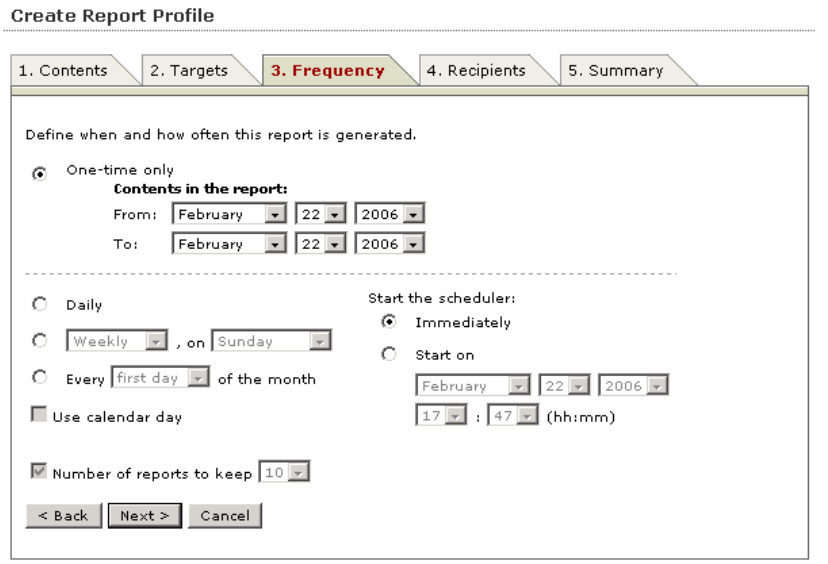
6. Click **Next >** to proceed to the Targets tab.



Step 2: Configure the Contents tab settings

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 only contains 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 will 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 Frequency tab settings

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

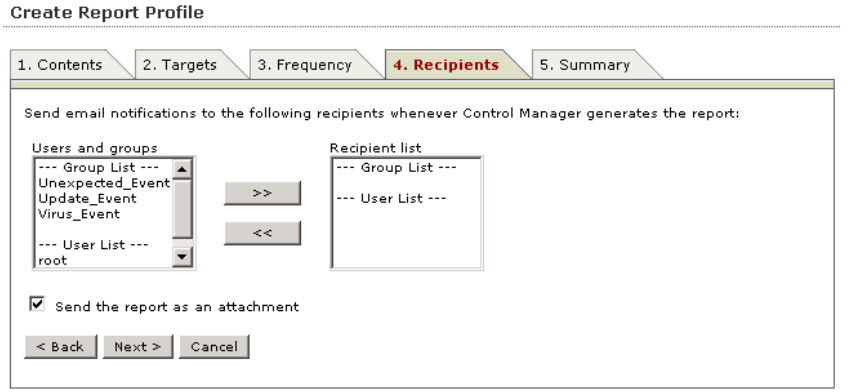
  If it is not checked, the start time is the same generation hour of the first day and end time is the generation hour of the day when generation occurs

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, navigate to the Local or Global Scheduled Reports screen, and then clear the check box adjacent to the scheduled report profile.

---

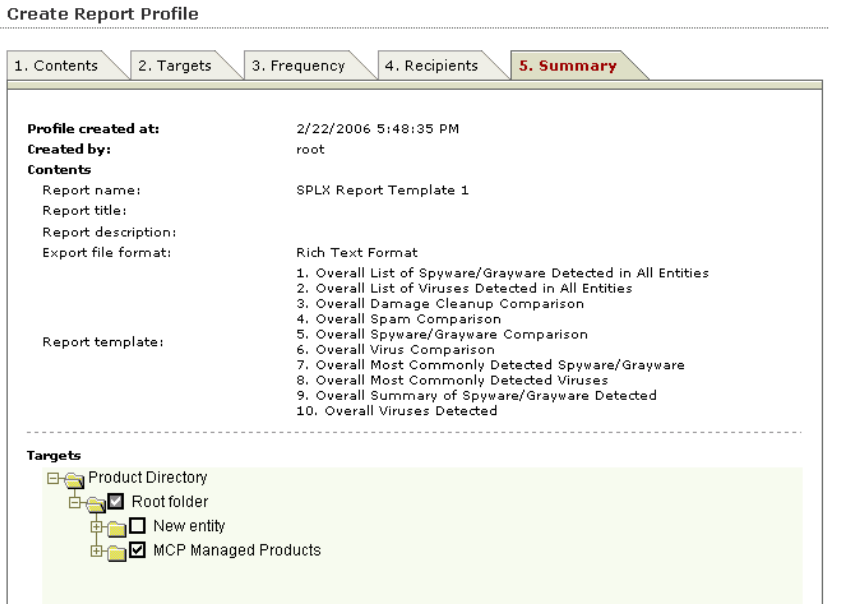
4. Click **Next >** to proceed to the Recipient tab.



Step 5: Configure the Recipient tab settings

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.

Review Report Profile Settings

Use the Profile Summary screen to review profile settings.

To access Profile Summary and review report profiles:

- Access Local or Global Reports

  On the working area under the Profile Summary column, click **View Profile**.
- Access Local or Global Scheduled Reports

  On the working area under the Profile Summary column, click **View Profile**.

Enable Scheduled Report Profiles

By default, Control Manager enables scheduled profiles upon creation. In an event that you disable a profile (for example, during database or agent migration), you can re-enable it via the Scheduled Local Reports or Scheduled Global Reports screen.

To enable scheduled report profiles:

1. Access Local or Global Scheduled Reports.
2. On the working area under Report Profiles column, click the profile checkbox.

   Click the checkbox adjacent to Report Profiles to select or deselect all profiles.
3. Click **Enable**.

Note: The options to enable, disable, and edit one-time-only profiles are not available because Control Manager generates these reports only once.

Disable Scheduled Report Profiles

To disable scheduled report profiles:

1. Access Local or Global Scheduled Reports.
2. On the working area under Report Profiles column, click the profile checkbox.

   Click the checkbox adjacent to Report Profiles to select or deselect all profiles.
3. Click **Disable**.

Note: You do not have the options to enable or disable one-time-only reports available, because Control Manager generates them only once.

Modify Scheduled Report Profiles

Use Local Report Profile or Global Report Profile to edit scheduled profiles.

To edit scheduled report profiles:

1. Access Local or Global Reports.
2. On the working area under the Profile Summary column, click **Edit Profile**.
3. On the Edit Profile, modify settings.
4. Click **Save**.

Delete Report Profiles

Control Manager lets you delete local profiles when you no longer need them.

To delete report profiles:

1. Access Local or Global Reports.
2. On the working area under the Report Profiles column, select the profile.
3. Click the checkbox adjacent to Report Profiles to select or deselect all profiles.
4. Click **Delete**.
5. Click **OK** to confirm the profile deletion.

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 **Run Now** to create scheduled reports on demand.

To generate on-demand scheduled 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.
4. On the Available Reports for {profile name} under **Generate a {Frequency} report starting from**, specify the starting month, day, and year.
5. Click **Run Now**.

It may take a few seconds to generate a report, depending on its contents. As soon as Control Manager finishes generating a report, the screen refreshes and the **View** link adjacent to the report becomes available.

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.

Delete Reports

Use Available Reports for {profile name} to delete actual reports.

To delete reports:

1. Access Local or Global Reports.
2. On the working area under the Available Reports column, click the corresponding **View** link.
3. On the Available Reports for {profile name} under the Submission Time column, select the submission time.
4. Click the check box adjacent to Submission Time to select or deselect all reports.
5. Click **Delete**.
6. Click **OK** to confirm the report deletion.

Chapter 8

Administering Managed Products

This chapter presents material administrators will need to manage the Control Manager network. Topics introduced in this chapter are as follows:

- *Understanding Communicators* on page 8-2
- *Understanding Managed Products* on page 8-22
- *Understanding Temp* on page 8-36
- *Managing Third Party Products* on page 8-39
- *Managing Child Servers* on page 8-42

Understanding Communicators

The Communicator, or the Message Routing Framework, serves as the communications backbone for the Control Manager system. This component of the Trend Micro Infrastructure (TMI) or MCP handles all communication between the Control Manager server and managed products. Communicators interact with Control Manager to communicate with managed products.

By installing the Control Manager agent on a managed product server, you can use this application to manage the product with Control Manager. Agents interact with the managed product and Communicator. An agent serves as the bridge between managed product and communicator. Hence, you must install agents on the same machine as managed products. There are currently only two instances where an agent must operate remotely:

- Trend Micro OfficeScan Corporate Edition, installed on a NetWare server
- NetScreen firewall management

The Control Manager installation checks if the Communicator is already available on the managed product server. If so, it does not install another instance of the Communicator. Multiple agents in a product server share a single Communicator. The Communicator takes care of:

- Securing messages by encryption and anti-replay functions provided by the OpenSSL open source library, and Trend Micro-developed end-to-end authentication
- Receiving and relaying commands from the Control Manager server to the managed product
- Receiving and relaying status information from managed products to the Control Manager server

The above descriptions highlight the following points:

- TMI can exist by itself; managed products, on the other hand, cannot operate in the absence of communicator
- Though there can be as many agents on a server as there are managed products, only one Communicator is required for each server
- Multiple managed products can share communicator functions

Understanding Agents

Control Manager 3.5 uses MCP, Control Manager 2.x, and TVCS agents to manage products on the Control Manager network:

- **Trend VCS Agent (version 1.84 or later)** - Older versions of certain Trend Micro products require this agent, an upgraded version of the original Trend VCS agent specifically designed for compatibility with Control Manager 2.5 or 3.0 servers.
- **Control Manager Agent (version 2.51 or higher)** - Certain versions Trend Micro products require this agent, built according to the Control Manager 2.5 (and above) architecture.
- **Trend Micro Management Communication Protocol (MCP) Agent** - Trend Micro's next generation agent supporting enhanced security, SSO, one-way and two-way communication, and cluster nodes.

The following table enumerates the features supported by Trend VCS, Control Manager 2.x, and MCP agents.

FEATURE	MCP AGENTS	CONTROL MANAGER 2.X AGENTS	TREND VCS AGENTS
Outbreak Prevention Services (OPS)	Yes	Yes	No
Single Sign-on (SSO)	Yes	No	No
One-way/two-way communication	Yes	No	No
NAT support	Yes	No	No
Cluster node support	Yes	No	No
Agent polls TMCM for updates and commands	Yes	No	No
Re-registration with the Control Manager server if the Agent database is corrupted or deleted	Constant polling	Automatic after 8 hours	Only when the communicator service is restarted

TABLE 8-1. Agent Comparison

FEATURE	MCP AGENTS	CONTROL MANAGER 2.X AGENTS	TREND VCS AGENTS
Communication security	HTTPS/HTTP	Encryption with optional authentication	No encryption, server-to-agent authentication only
Communicators	No	Yes	No
Work and Idle state support	Yes	Yes	No
Communicator heartbeat	Yes	Yes	No
Notification: Virus pattern expired	Yes	Yes	No
Notification: Agent unable to update components	Yes	Yes	No
Notification: Agent unable to deploy components	Yes	Yes	No
Notification: Product service stopped	Yes	Yes	Not supported. In InterScan VirusWall for Windows, this results in a "real-time scan stopped" notification instead

TABLE 8-1. Agent Comparison

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

MCP AGENTS	2.X AGENTS
Poll commands for the managed product from Control Manager server	Receiving commands from the Control Manager server, via the Communicator
Collecting managed product status and logs, and sending them to the Control Manager server, through HTTPS	Collecting managed product status and logs, and sending them to the Control Manager server, through the Communicator

TABLE 8-2. MCP / 2.x Agent Comparison

Understanding Managed Products, Communicators, and Child Servers Connection Status Icons

The Control Manager managed products, Communicators, and child server use the following connection status icons:

CONNECTION STATUS DESCRIPTION	MANAGED PRODUCT	
Product service is running		
Product service is not running		
TMI service is not running		Within heartbeat's maximum delay setting
		Beyond the heartbeat's maximum delay setting
The socket or network connection between the Communicator and managed product is broken		
Unable to resolve the DNS name between the Communicator and Control Manager server		Within heartbeat's maximum delay setting
		Beyond the heartbeat's maximum delay setting

TABLE 8-3. Status Icons for Managed Products

CONNECTION STATUS DESCRIPTION	COMMUNICATORS	
TMI service is running		
TMI service is not running		Within heartbeat's maximum delay setting
		Beyond the heartbeat's maximum delay setting
Idle mode following the Communicator Scheduler		

TABLE 8-4. Status Icons for Communicators

CONNECTION STATUS DESCRIPTION	COMMUNICATORS
The socket or network connection between the Communicator and managed product is broken	
Unable to resolve the DNS name between the Communicator and Control Manager server	

TABLE 8-4. Status Icons for Communicators

CONNECTION STATUS DESCRIPTION	CHILD	
TMI service is not running	Status is not changed	Within heartbeat's maximum delay setting
		Beyond the heartbeat's maximum delay setting
The child server service (Casprocessor.exe) is running		
Casprocessor.exe or the child server's Communicator is not running. Either the child server is shutdown or the Communicator service is disabled		
The child server is disabled from the parent server management console		

TABLE 8-5. Status Icons for Child Servers

Understanding the Control Manager Security Levels

Control Manager has three security levels used for communication between the server and managed products and child servers for both older agents and MCP agents. For MCP agents, Security Level applies to the virtual folders of IIS, 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 8-6. Security Level Behavior for MCP

Depending on the security level of older agents, Control Manager provides the following encryption and authentication:

- **SSL packet-level encryption:** Control Manager applies Secure Socket Layer (SSL) packet-level encryption to all security levels. SSL packet-level encryption is a protocol developed by Netscape for secure transactions across the Web. SSL uses a form of public key encryption, where the information can be encoded by the browser using a publicly available public key, but can only be decoded by a party who knows the corresponding private key.

  The Control Manager agents can encrypt their communication using the public key. In return, the Control Manager server uses a private key to decrypt the agent message.

- **Trend Micro authentication:** Control Manager applies Trend Micro authentication 5 (High) security level.

  When using High level, Control Manager first applies the SSL packet-level encryption and then further strengthens the encryption through Trend Micro authentication

Note: You can modify the Control Manager security level through TMI.cfg. However, doing so requires the modification of all TMI.cfg present in the Control Manager network TMI.cfg of the Control Manager server including all managed products and child servers. Otherwise, the server and agent communication will not work.

SECURITY LEVEL (FOUND IN TMI.CFG)	SECURITY LEVEL SELECTION (DURING INSTALLATION)	END-TO-END AUTHENTICATION	MESSAGE-LEVEL ENCRYPTION
1	Low	N/a	40-bit (RC4)
2	Medium	N/a	128-bit (RC4)
5	High	Trend Micro authentication	128-bit (RC4 + 3DES)

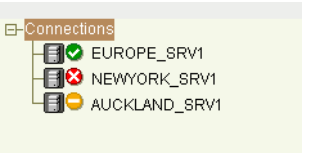
TABLE 8-7. Security Level Behavior for Older Agents

Understanding the Connections Tree

The Connections tree provides you with the following information:

- The status of the connection between Communicators and managed product.
- The name of the computing environment containing the Communicator installation

In the example below, the Connections tree identifies the Communicators available in the Control Manager network, and displays the Communicator's connection status.



ICON	DESCRIPTION
	Server where the Communicator resides
	Communicator connection status

TABLE 8-8. Communicator Connection Status

Using Communicator Scheduler

The Communicator Scheduler determines the periods when the agent sends information to Control Manager server, allowing you to manage the flow of information.

The Control Manager agent installation assigns a default Communicator Schedule. You can modify the schedule to suit your Control Manager network needs. The Communicator Schedule follows a daily setting, that is, it applies the schedule to an agent on a daily basis. There is no weekly or monthly work hour configuration available.

When you set a schedule, that schedule applies to all managed products sharing a Communicator.

Note: In an event when a Communicator is Idle during an Outbreak Prevention Mode, corresponding managed products will still perform the Outbreak Prevention Services commands without reporting the result to the agent. As a result, the Communicator does not know the status or result. Command Tracking lists the result of Outbreak Prevention Policy-related commands under the Fail category.

The Communicator Scheduler Idle and Working schedules apply only to the managed product Communicator. You cannot set the Idle schedule for child servers, and there is 00~24 Working hours.

Note: The Communicator Scheduler still lists the Child server Communicators. However, you do not have the check boxes available.

Using Communicator Heartbeat

Communicator heartbeat refers to the Control Manager agent message that notifies the Control Manager server with "I am alive" information. The Communicator provides this mechanism to determine whether the managed products remain active.

The heartbeat defines when a Communicator sends information to the Control Manager server. Use the Communicator Scheduler to define the heartbeat Working and Idle hours.

The Communicator polls the Control Manager server at regular intervals for the following purposes:

- Ensure that the Control Manager console displays the latest information
- Check whether the connection between the managed product and the server remains functional

There are three heartbeat statuses:

- **Active** - within the Working hour
- **Inactive** - idle hour or not within the Working hour
- **Abnormal** - disconnected

The Communicator for older agents sends the heartbeat using the User Datagram Protocol (UDP) instead of using a connection-oriented protocol, where available.

Note: In addition to providing periodic heartbeat to the Control Manager server, the Communicator also sends real-time managed product status information to the server.

MCP Heartbeat

To monitor the status of managed products, MCP agents poll Control Manager based on a schedule. Polling occurs to indicate the status of the managed product and to check for commands to the managed product from Control Manager. The Control Manager Web console then presents the product status. This means that the managed product's status is not a real-time, moment-by-moment reflection of the network's status. Control Manager checks the status of each managed product in a sequential manner in the background. Control Manager changes the status of managed products to offline, when a fixed period of time elapses without a heartbeat from the managed product.

Active heartbeats are not the only means Control Manager has for determining the status of managed products. The following also provide Control Manager with the managed product's status:

- Control Manager receives logs from the managed product. Once Control Manager receives any type of log from the managed product successfully, this implies that the managed product is working fine.

- In two-way communication mode, Control Manager actively sends out a notification message to trigger the managed product to retrieve the pending command. If server connects to the managed product successfully, it also indicates that the product is working fine and this event will be counted as a heartbeat.
- In one-way communication mode, the MCP agent periodically sends out query commands to Control Manager. This periodical query behavior works like a heartbeat and is treated as such by Control Manager.

The MCP heartbeats implement with the following ways:

- **UDP:** If the product can reach the server using UDP, this is the most lightweight, fastest solution available. However, this does not work in NAT or firewall environments. Also the transmitting client cannot make sure that the server does indeed receive the request.
- **HTTP/HTTPS:** To work under a NAT or firewall environment, a heavyweight HTTP connection can be used to transport the heartbeat

Control Manager supports both UDP and HTTP/HTTPS mechanisms to report heartbeats. Control Manager server finds out which mode the managed product applies during the registration process. A separate protocol handshake occurs between both parties to determine the mode.

Aside from simply sending the heartbeat to indicate the product status, additional data can upload to Control Manager along with the heartbeat. The data usually contains managed product activity information to display on the console.

Using the Schedule Bar

Use the schedule bar in the Communicator Scheduler screen to display and set Communicator schedules. The bar has 24 slots, each representing the hours in a day.

Blue slots denote Working status or the hours that the Communicator sends information to the Control Manager server. White slots indicate Idle time. Define Working or Idle hours by toggling specific slots.

You can specify at most three consecutive periods of inactivity. The sample schedule bar below shows only two inactive hours:

The active periods specified by the bar are from 0:00 A.M. to 7:00 A.M, 8:00 A.M to 3:00 PM, and from 6:00 P.M. to 12:00 P.M.

Determining the Right Heartbeat Setting

When choosing a heartbeat setting, balance between the need to display the latest Communicator status information and the need to manage system resources. Trend Micro's default settings is satisfactory for most situations, however consider the following points when you customize the heartbeat setting:

HEARTBEAT FREQUENCY	RECOMMENDATION
Long-interval Heartbeats (above 60 minutes)	The longer the interval between heartbeats, the greater the number of events that may occur before Control Manager reflects the communicator status on the Control Manager management console. For example, if a connection problem with a Communicator is resolved between heartbeats, it then becomes possible to communicate with a Communicator even if the status appears as (inactive) or (abnormal).
Short-interval Heartbeats (below 60 minutes)	Short intervals between heartbeats present a more up-to-date picture of your network status at the Control Manager server. However, this is a bandwidth-intensive option.

TABLE 8-9. Heartbeat Recommendations

Access Communicators

Use the Computer screen to view the numbers of active, inactive, or abnormal communicators as well as the total count in the Control Manager network.

To access Communicators:

1. Click **Products** on the main menu.
2. On the leftmost menu, select **Computers** from the list and then click **Go**.
3. Click the available links in the Active, Inactive, Abnormal, or Total column to view the connection status details for available Communicators.

View Communicators Connection Status Details

Use the Connection Status (Details) screen to view the Communicators available in the Control Manager network and their status.

To view Communicators connection status details:

1. Click **Products** on the main menu.

2. On the leftmost menu, select **Computers** from the list and then click **Go**.
3. On working area, click the available links in the Active, Inactive, Abnormal, or Total column.
4. Sort Communicators in ascending or descending order according to **Status**, **Computer name**, **IP Address**, or **Communicator Version**.
5. Click **Back** to go return to the Computers screen.

View Communicators and Communicators Status

Control Manager displays Communicators in the Connections tree based on the Product Directory folders and managed products that you can access. If you do not have access to a specific folder or managed product, the Communicator used by that managed product will not be available in the Connections tree.

To view Communicators and Communicators status in your Control Manager network:

1. Click **Products** on the main menu.
2. On the leftmost menu, select **Computers** from the list and then click **Go**.
3. On the left-hand menu, select a **Communicator** in the Connections tree. The Communicator Status screen provides the following information:
   - **System Information** - supplies the following information about the machine where the Communicator is installed:
     - **Operating system**
     - **IP address**

Note: The IP address field for the Communicators screen can display up to 6 IP addresses.

   - **Communicator Status** - provides the following Communicator details:
     - **Uptime** - indicates when the Communicator was last turned on
     - **Last heartbeat time** - indicates when the Communicator last established connection to the Control Manager server
     - **Version** - indicates the version of the Communicator application

- **Registration** - indicates when the Communicator registered to the Control Manager server

- **Managed products** - lists the managed products sharing the Communicator
- **Schedule** - displays the Communicator Schedule

Access Communicator Scheduler

Use the Communicator Scheduler screen to configure schedule when agents send information to the Control Manager server.

To access the Communicator Scheduler screen:

1. Access **Communicators**
2. On the leftmost menu, click **Communicator Scheduler**.

Set Communicator Schedules

You can define up to three sets of schedules that specify when the agent interacts with the communicator.

Note: A child server Communicator should always have constant communication with the Control Manager server; the Communicator Scheduler screen does not allow changes in a child server Communicator schedule.

To set a schedule for a managed product Communicator:

1. Access **Communicators**
2. On the leftmost menu, click **Communicator Scheduler**.
3. On the working area, select the Communicator and then click the schedule (1st Schedule, 2nd Schedule, or 3rd Schedule).
4. Define the schedule. Specify a new time or use the default setting.
   - To specify a new setting, toggle the appropriate time slots in the schedule bar and then click **Save**
   - To use the default setting, click **Apply Default** and **Save**

Modify the Default Communicator Schedule

Use the Default Communicator schedule to automatically set the communicator schedule.

To modify a managed product Communicator schedule:

1. Access **Communicators**
2. On the leftmost menu, click **Communicator Scheduler**.
3. On the working area, click **Edit Default**.
4. On the Edit Default Schedule, toggle the appropriate time slots.
5. Click **Save**.

Access Communicator Heartbeat

Use Communicator Heartbeat to define the Frequency and Maximum delay times (in minutes) for Control Manager server and agent communication.

To access the Communicator Heartbeat screen:

1. Access **Communicators**.
2. On the leftmost menu, click **Communicator Heartbeat**.

Set Communicator Heartbeat

Use the Communicator heartbeat screen to set the heartbeat settings.

Note: The Communicator heartbeat setting only applies to Communicators for managed products directly controlled by the Control Manager server. Child Control Manager server Communicators use predefined values:
Frequency: 3 minutes
Maximum delay: 5 minutes

To set the heartbeat Frequency and Maximum delay times:

1. Access **Communicators**.
2. On the leftmost menu, click **Communicator Heartbeat**.
3. On the working area, leave the default values or specify new settings for the following:

- **Frequency** - defines how often the Communicator responds to Control Manager server messages. The permitted values are between 5 to 480 minutes
- **Maximum delay** - specifies how long Control Manager waits for a response from the Communicator before changing its management console status to (inactive). The allowable values are between 15 to 1440 minutes.

Note: The Maximum delay must be at least triple the Frequency value.

4. Click **Save**.

Restart Control Manager Services

Use the Windows Services screen to restart any of the following Control Manager services:

- Trend Micro Management Infrastructure
- Trend Micro CCGI
- Trend Micro Control Manager

Note: These are the services that run in the background on the Windows operating system, not the Trend Micro services that require Activation Codes (for example, Outbreak Prevention Services, Damage Cleanup Services).

To restart Control Manager services:

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

Modify the Control Manager External Communication Port

The Communicator is responsible for agent and server communication.

By default, the Communicator uses port 10198 for communication between Control Manager processes (internal communication) and port 10319 for communication between the Control Manager agent and server (external communication).

Changing the external communication port is a two-step process.

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

1. Open <root>\Program Files\Trend Micro\COMMON\ccgi\commoncgi\config\CCGI_Config.xml using a text editor (for example, Notepad).

WARNING! *Use care when modifying Control Manager *.xml or *.cfg files. To ensure that you can rollback to the original settings, backup CCGI_Config.xml.*

---

2. Specify a new value for the OuterPort parameter. This value represents the external communication port.

   For example, set OuterPort="2222" to use port 2222.

3. Save and close CCGI_Config.xml.
4. Open <root>\Program Files\Trend Micro\COMMON\TMI\TMI.cfg using a text editor.

WARNING! *Making incorrect changes to the configuration file can cause serious system problem. Backup TMI.cfg to restore your original settings.*

---

5. Replace the OuterPort parameter value to match the value of CCGI_Config.xml.
6. Save and close TMI.cfg.
7. Stop and restart all Control Manager services.

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

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

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

Modify the Security Level

Control Manager implements the security level you specified during the Control Manager installation. TMI.cfg allows you to change the security level without reinstalling the product.

To change the Control Manager security level:

1. Open <root>:\Program files\Trend Micro\COMMON\TMI\TMI.cfg using any text editor (for example, Notepad).

WARNING! *Making incorrect changes to the configuration file can cause serious system problem.*

2. Backup TMI.cfg to restore your original settings.
3. Change the value of MaxSecurity parameter. Use 1, 2, or 5, which corresponds to the security level you want.
4. Save and close TMI.cfg.
5. Open the Windows Services screen to stop and then restart the Control Manager services.
6. Repeat steps 1 to 3 to modify TMI.cfg for all agents present in your Control Manager network.

WARNING! *Set all TMI.cfg in your Control Manager network (server and agents) to the same security level value (MaxSecurity). Otherwise, the server and agent communication will not work.*

Modify the Communicator Heartbeat Protocol

By default, the connectionless User Datagram Protocol (UDP) is used to send Communicator Heartbeat from managed product to the Control Manager server.

To change the Communicator Heartbeat protocol to TCP:

1. Open <root>:\program files\Trend Micro\COMMON\TMI\TMI.cfg using any text editor (for example, Notepad).

WARNING! *Making incorrect changes to the configuration file can cause serious system problem. Backup TMI.cfg to restore your original settings.*

2. Change the value of AllowUDP parameter to 0.
3. Save and close TMI.cfg.
4. Open the Windows Services screen to stop and then restart the Control Manager services.
5. Repeat steps 1 to 3 to modify TMI.cfg for all agents present in your Control Manager network.

WARNING! *Set all TMI.cfg in your Control Manager network (server and agents) to the same security level value (AllowUDP). Otherwise, the server and agent communication will not work.*

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 1-5.

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 `cgiCmdNotfiy.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 `cgiCmdNotfiy.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

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 TMCM 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.

Understanding Managed Products

A managed product refers to an antivirus, content security or third party product represented in the Product Directory. The Control Manager management console represents managed products as icons (for example, or). 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.

Understanding Product Directory

Take care when planning the structure of the Product Directory, a logical grouping of managed products, 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. On the other hand, granting access to a specific managed product only grants access to that specific product.
- **Deployment planning:** Control Manager deploys virus pattern, scan engine, spam rule, and program updates to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory will therefore simplify the designation of recipients.
- **Outbreak Prevention Policy and Damage Control Template deployments:** OPP and DCS deployments depend on Deployment Plans for efficient distribution of Outbreak Prevention Policy and cleanup tasks.

As shown in this sample Product Directory, managed products identify the registered antivirus or content security product, as well as provide the connection status.

Product Directory icons:

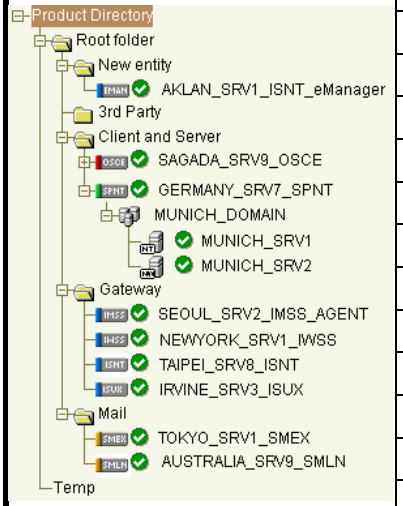
PRODUCT DIRECTORY TREE	ICON	DESCRIPTION
	or	New entity or user-defined folder name
	EMAN	InterScan eManager
	OSCE	OfficeScan Corporate Edition
	SPNT	ServerProtect Information Server
		ServerProtect Domain
	NT	ServerProtect for Windows (Normal Server)
	NW	ServerProtect for NetWare (Normal Server)
	IMSS	InterScan Messaging Security Suite
	IWSS	InterScan Web Security Suite
	ISNT	InterScan VirusWall for Windows
	ISUX	InterScan VirusWall for UNIX
	SMEX	ScanMail for Microsoft Exchange
	SMLN	ScanMail for Lotus Notes
	NVW	Network VirusWall
	FW	NetScreen Global PRO Firewall
		Managed Product connection status icon

TABLE 8-10. Managed Product Icons

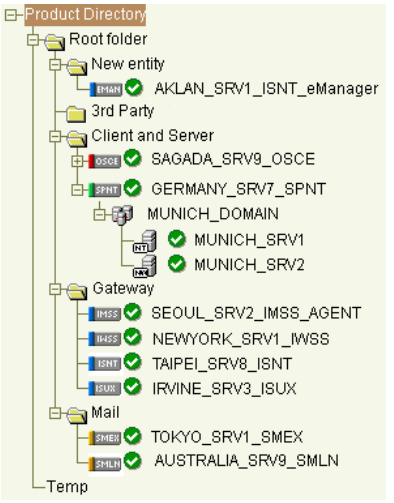
Arrange the Product Directory using the Directory Manager. Use descriptive folders to group your managed products according to their protection type and the Control Manager network administration model. For example, grant access rights to mail administrators to configure the Mail folder.

Accessing a Managed Product's Default Folder

Newly registered managed products 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.

The following presents different scenarios for the accessible folders given to the account and the resulting default managed product location:



Accessible Folder Given to the Account	Default Managed Product Location
Root folder	New entity
Mail	Mail
SAGADA_SRV9_OSCE	New entity

User accounts set to access a specific managed product cannot access any newly registered managed products.

TABLE 8-11. Managed Products vs. User Access

Access Product Directory

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

Note: Viewing and accessing the folders in the Product Directory depends on the Account Type and folder access rights used to log on to the management console.

To access the Product Directory:

1. Click **Products** on the main menu.

2. On the leftmost menu, select **Managed Products** from the list and then click **Go**.

Manually Deploy New Components Using the Product Directory

Manual deployments allow you to update the virus patterns, spam rules, and scan engines of your managed products on demand. This is useful especially during virus outbreaks.

Download new components before deploying updates to specific or groups of managed products.

To manually deploy new components using the Product Directory:

1. Click **Products** on the main menu.
2. On the leftmost menu, select **Managed Products** from the list and then click **Go**.
3. On the left-hand menu, select the desired managed product or folder.
4. On the working area, click the **Tasks** tab.
5. Select **Deploy <component>** from the Select task list.
6. Click **Next>>**.
7. Click **Deploy Now** to start the manual deployment of new components.
8. Monitor the progress via Command Tracking.
9. Click the **Command Details** link to view details for the Deploy Now task.

View Managed Products Status Summaries

The Product Status screen displays the Antivirus, Content Security, and Web Security summaries for all managed products present in the Product Directory tree.

There are two ways to view the managed products status summary:

- Through Home page
- Through Product Directory

To access through the Home page

- Upon opening the Control Manager management console, the Status Summary tab of the Home page shows the summary of the entire Control Manager system. This summary is identical to the summary provided by the Product Status tab in the Product Directory Root folder.

To access through Product Directory:

1. Click **Products** on the main menu.
2. On the left-hand menu, select the desired folder or managed product.
   - If you click a managed product, the Product Status tab displays the managed product's summary
   - If you click the Root folder, New entity, or other user-defined folder, the Product Status tab displays Antivirus, Content Security, and Web Security summaries

---

Note: By default, the Status Summary displays a week's worth of information ending with the day of your query. You can change the scope to Today, Last Week, Last Two Weeks, or Last month available in the Display summary for list.

Configure Managed Products

Depending on the product and agent version:

- You can configure products either individually or in groups according to folder division

  Perform group configuration using the folder Configuration tab.

Note: When performing a group configuration, verify that you want all managed product in a group to have the same configuration. Otherwise, add managed products that should have the same configuration to Temp to prevent the settings of other managed products from being overwritten.

- The Configuration tab shows either the product's Web console or a Control Manager-generated console

To configure a product:

1. Click **Products** on the main menu.
2. On the leftmost menu, select **Managed Products** from the list and then click **Go**.
3. On the left-hand menu, select the desired managed product or folder.
4. On the working area, click the **Configuration** tab.

5. Select the product to configure from the Select product list.

Note: Step 4 is necessary when you use the folder Configuration tab.

6. At the Select configuration list, select the product feature to access or configure.
7. Click **Next**. The managed product Web-based console or Control Manager-generated console appears.

Tip: For additional information about configuring managed products, refer to the product's documentation.

Issue Tasks to Managed Products

Use the Tasks tab to invoke available actions to a group or specific managed product. Depending on the managed product, all or some of the following tasks are available:

- Deploy engines
- Deploy pattern files/cleanup templates
- Deploy program files
- Enable/Disable Real-time Scan
- Start Scan Now

Deploy the latest spam rule, pattern, or scan engine to managed products with outdated components. To successfully do so, the Control Manager server must have the latest components from the Trend Micro ActiveUpdate server. Perform a manual download to ensure that current components are already present in the Control Manager server.

To issue tasks to managed products:

1. Access the Product Directory.
2. On the left-hand menu, select the desired managed product or folder.
3. On the working area, click the **Tasks** tab.
4. Select the task from the Select task list.
5. Click **Next**.

6. Monitor the progress through Command Tracking. Click the **Command Details** link at the response screen to view command information.

Query and View Managed Product Logs

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

To query and view managed product logs:

1. Access the Product Directory.
2. On the left-hand menu, select the desired managed product or folder.
3. On the working area, click the **Logs** tab.
4. Select the client log type:

   Event Logs:

   a. Provide the following search parameters:

PARAMETER	DESCRIPTION
Severity	Refers to the degree of information available. The options are: Critical, Warning, Information, Error, Unknown. Select the check box of your chosen parameter
Incident	Refers to events. The options are: All events, Virus outbreak, Module update, Service On, Service Off, Security violation, Unusual network virus behavior
Product	If you select a folder, this list shows the managed products belonging to the folder. To view information on all products, select All. Otherwise, query logs of a specific managed product
Logs for	View all logs, or only those that the managed product generated within a specific interval. For the latter option, you can specify logs for the last 24 hours, day, week, month, or custom range If you chose Specified range, select the appropriate month, day, and year for the Start date and End date
Sort logs by	Sort results according to the date/time, computer name, product, event, or severity
Sort order	Sort results in ascending and descending order

TABLE 8-12. Search Parameters for Event Logs

b. Click **Display Logs** to begin the query and display the query results.

Security Logs:

a. Select All virus log incidents or a specific security logs type and then click **Query**.

b. Provide the following search parameters:

PARAMETER	DESCRIPTION
Logs for	View all logs, or only those that the managed product generated within a specific interval. For the latter option, you can specify logs for the last 24 hours, day, week, month, or custom range If you chose Specified range, select the appropriate month, day, and year for the Start date and End date
Sort logs by	Sort results according to the date/time, computer name, product, event, or severity
Sort order	Sort results in ascending and descending order

TABLE 8-13. Search Parameters for Security Logs

c. Click **Display Logs** to begin the query.

Note: eManager managed products records content security violations in the Security Logs, not in the Virus Logs.

5. The Query Result screen displays the results in a table format.
6. The Generated at entity column of the result table indicates the Control Manager server time.

Recover Managed Products Removed From the Product Directory

The following scenarios can cause Control Manager to delete managed products from the Product Directory:

- Reinstalling the Control Manager server and selecting Delete existing records and create a new database option

  This option creates a new database using the name of the existing one.

- Replacing the corrupted Control Manager database with another database of the same name
- Accidentally deleting the managed product using the Directory Manager

If a Control Manager server's managed products records are lost, the agents on the products still "know" where they are registered to. The product agent will automatically re-register itself after 8 hours or when the service is restarts.

To recover managed products removed from the Product Directory:

- Restart Trend Micro Control Manager service on the managed product server. For more information, see *Restart Control Manager Services* on page 8-16
- **Wait for the Agent to re-register itself:** By default, the Control Manager agent verifies its connection to the server every eight (8) hours. If the agent detects that its record has been deleted, it will re-register itself automatically.

  Refer to Change agent connection re-verification frequency to modify the agent verification time.

Change Agent Connection Re-Verification Frequency

By default, Control Manager 2.x agents re-verify their connection with the Control Manager server every eight hours. Edit a configuration file on the agent machine to modify the frequency.

To change agent connection re-verification frequency:

1. From the managed product's server, navigate to the Control Manager agent home directory (for example, c:\Program Files\Trend\IMSS\Agent).
2. Back up Entity.cfg.
3. Open Entity.cfg using a text editor (for example, Notepad).
4. Search for the parameter ENTITY_retry_hour and specify an integer value to modify the default verification time.
5. The ENTITY_retry_hour value is in terms of number of hours. Acceptable values are from 1 to 24 hours.
6. Save and close Entity.cfg to apply the new verification time.

Search for Managed Products, Product Directory Folders or Computers

Use the Search button to quickly:

- Add a specific or a group of managed products to Temp
- Find and locate a specific managed product in the Product Directory

To search for a folder or managed product:

1. Access Product Directory.
2. On the left menu, click **Search**.
3. On the working area, provide the following search parameters:

PARAMETER	DESCRIPTION
Search for	Select the object of the search from the drop down list Search for managed products or Communicators based on their name, folder name, or computer name.
Keyword	This allows you to search for the object by name Select **Case sensitive** to narrow down the search results.
Managed product status / Communicator status	Select the appropriate connection status, for the Communicator or managed product The options are: All, Active, Inactive, Abnormal, Product Active, and Product Inactive. Choose All to search for objects regardless of the connection status.
Product	Select the appropriate product from the list. Choose **All** to search for all products.

TABLE 8-14. Search Parameters

4. Click **Begin Search** to start searching.
5. Control Manager presents the search results in a table format. You may opt to directly create the temp sub-folder where the search results will be grouped.

Refresh the Product Directory

To refresh the Product Directory:

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

Understanding Directory Manager

After the Control Manager agent installation, the managed product first appears in the Product Directory under the default folder.

Use the Directory Manager to customize the Product Directory organization to suit your administration model needs. For example, you can group products by location or product-type messaging security, web security, file storage protection, and so on.

The Directory allows you to create, modify, or delete folders, and move managed products between folders. You cannot, however, delete nor rename the New entity folder.

Carefully organize the managed products belonging to each folder. Consider the following factors when planning and implementing your folder and managed product structure:

- Product Directory
- User Accounts
- Deployment Plans

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	Pro's	Con's
Geographical or Administrative	Clear structure	No group configuration for identical products
Product type	Group configuration and status is available	Access rights may not match

TABLE 8-15. Product Grouping Comparison

Grouping Type	Pro's	Con's
Combination of both	Group configuration and access right management	Complex structure, may not be easy to manage

TABLE 8-15. Product Grouping Comparison

Using the Directory Manager Options

Directory Manager provides seven options: New Folder, Delete, Rename, Undo, Redo, Cut, and Paste.

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

To use and apply changes in the Directory Manager:

- Right-click a folder or managed product to open a pop-up menu that presents a list of actions you can perform
- Click + or the folder to display the managed products belonging to a folder
- Press **Enter** or click anywhere when you rename a folder
- Click **Save** to apply your changes and update the Directory Manager organization
- Click **Reset** to discard changes that are not yet saved

Access Directory Manager

Use Directory Manager to group managed products together.

To access the Directory Manager:

1. Access Product Directory.
2. On the left-hand menu, click **Directory Manager**.

Create Folders

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

To create a folder:

1. Access the Directory Manager.
2. On the working area, right-click where you want to create a new folder. If you are building the tree for the first time, right-click the Root folder.
3. Select **New folder** from the pop-up menu. Control Manager creates a new sub-folder under the main folder.
4. Type a name for the new folder or use the default name and then press **Enter**.
5. Click **Save**.

Except for the New entity folder, Control Manager lists all other folders in ascending order, starting from special characters (!, #, $, %, (,), *, +, -, comma, period, +, ?, @, [,], ^, _, {, |, }, and ~), numbers (0 to 9), or alphabet characters (a/A to z/Z).

Renaming Folders or Managed Products

To rename a folder or managed product:

1. Access Directory Manager.
2. On the working area, right-click the folder or managed product you want to rename and then select **Rename** from the pop-up menu. The folder/managed product name becomes an editable field.
3. Type a name for the new folder or use the default name and then press **Enter**.
4. Click **Save**.

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

Move Folders or Managed Products

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

1. Access Directory Manager.
2. On the working area, select the folder or managed product you want to move.

3. Do one of the following:
   - Drag-and-drop the folder or managed product to the target new location
   - Cut and paste the folder or managed product to the target new location
4. Click **Save**.

Delete User-Defined Folders

Take caution when deleting user-defined folders in the Directory Manager, you may accidentally delete a managed product which causes it to unregister from the Control Manager server.

To delete a user-defined folder:

1. Access the Directory Manager.
2. On the working area, right-click the folder you want to delete and then select **Delete** from the pop-up menu.
3. Click **Save**.

Note: You cannot delete the New entity folder

Take caution when deleting user-defined folders, you may accidentally delete a managed product

---

Understanding Temp

Temp, a collection of managed product shortcuts, allows you to focus your attention on specific products without changing the Product Directory organization. Use Temp for deploying updates to groups of products with outdated components.

Consider the following issues when using Temp:

- Control Manager deletes all managed product shortcuts when you log off the management console.
- You can only add the managed products to Temp if you can see them in the Product Directory, you cannot make shortcuts to products that you cannot access.

Using Temp

You can manipulate managed products in Temp the same way you would with managed products in the Product Directory. The folders and managed products belonging to Temp have the same folder and managed product-level controls. However, Control Manager determines what actions you can perform on the managed products according to your user account's access rights.

You can use Temp for the following purposes:

- Issue commands to groups of managed products using folder-level access rights.
- Select a specific managed product, and then use the available Product Directory tabs to perform an action.

Access Temp

Use Temp to collect managed product shortcuts.

To access Temp:

1. Access Product Directory.
2. On the leftmost menu, click **Temp**.

Adding Managed Products to Temp

There are three methods to add managed products to Temp:

- From the Search results
- From the Product Directory

- Add managed products with outdated components based on the Status Summary page

Trend Micro recommends that you add several managed products at once to Temp using the last method. The Status Summary screen provides information as to which managed products use outdated components. It simplifies virus pattern and scan engine updates on groups of managed products belonging to different folder groups.

Note: Adding managed products to Temp only allows you to collect managed products with outdated components doing so does not trigger automatic deployment.

To add from the Search results

1. Click **Products** on the main menu.
2. On the left-hand menu, click **Search**.
3. On the working area, search for managed products or folders.
4. Specify a sub-folder name in the **Temp sub-folder for managed products** field for the Temp sub-folder that will contain the managed product shortcuts.

Note: Step 4 is optional. If you want to create multiple folder levels belonging to Temp, specify \{folder name level1}\{sub-folder name level2} in the Temp sub-folder for entities field. For example, if you specify \pattern\mail, the following Temp structure appears:

---

5. Click **Add**. Control Manager adds managed products from the search results to Temp.

To add from the Product Directory

1. Access the Product Directory.
2. On the left-hand menu, select the managed product you want to add to Temp.
3. Press "+" on the numeric keypad.

To add managed products with outdated components based on the Status Summary page:

1. Access Product Directory.
2. On the left-hand menu, select the desired Product Directory folder.
3. On the working area, click the **Product Status** tab.
4. At the Component Status table, click one of the numeric links indicating the number of managed products that are outdated. Depending on the link you clicked, the Virus Pattern Status (Outdated), Scan Engine Status (Outdated), Spam Rule Status (Outdated) screen opens displaying the computer name, product name, product version, and outdated component version.
5. Click **Add to Temp** in the status page. Control Manager organizes the managed products to Temp using folders named after the page from which they were added. For example, Control Manager places managed products added from the Scan Engine Status (Outdated) page under the Scan Engine Status (Outdated) folder.

Note: Clicking **Add to Temp** only adds the managed products shown on the status page. If the list of managed products spans more than one screen, click **Add to Temp** on all screens to add all products with outdated component.

---

6. Click **Back** to return to the Status Summary page, and then proceed to the next outdated component. Repeat the instructions until Control Manager adds all the outdated managed products to Temp.

Removing Managed Products from Temp

To remove a managed product from Temp:

1. Access Product Directory.
2. On the left-hand menu, click **Temp**.

3. From the available managed product on the Temp list, select the folder or managed product shortcut that you want to remove.
4. Press "-" in the numeric keypad.

Note: Control Manager removes managed product shortcuts in Temp when you log off from the management console.

Removing managed products from Temp will neither disconnect the antivirus or content security product nor uninstall the Control Manager agent from the Control Manager server.

Managing Third Party Products

Control Manager is able to manage more than just Trend Micro products. Control Manager can also support 3rd-party products.

Understanding the Control Manager Agent for NetScreen™ Firewall

Control Manager administers NetScreen firewalls through the NetScreen-Global PRO security management system. You can indirectly manage all firewalls that are compatible with Global PRO through Control Manager.

Control Manager applies outbreak prevention policies to NetScreen-Global PRO managed product — using Outbreak Prevention Services (OPS). Control Manager adds the port blocking instructions in outbreak prevention policies as policies in Global PRO's Policy Builder.

Note: For a list of Global PRO-compatible firewalls, refer to the NetScreen Web site at www.netscreen.com.

Therefore, the agent for NetScreen Firewall operates "remotely." You must install the Control Manager agent for NetScreen on the Control Manager server that manages the NetScreen Global-PRO firewall management software.

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 that will be 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
- Location of the Control Manager server public encryption key (E2EPublic.dat)

The following procedure assumes that you will be using an existing Arbitrator when logging on to Global PRO.

To determine the Certificate Name of a Global PRO Arbitrator:

1. On the NetScreen Policy Manager logon screen, select an Arbitrator used for Global PRO communication. Choose an Arbitrator that uses SSL.
2. Click **Edit**.
3. Copy the 16-digit certificate number at the **Cert. Name** field.

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

Tip: Specify a permanent User ID on the Control Manager server. If the account you provided is deleted, you will encounter difficulties when managing the product.

Trend Micro recommends the use of the Control Manager superuser account.

---

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

Updating NetScreen-Global PRO Settings

Use the Configuration tab to update the setting you use to connect to NetScreen-Global PRO. The Control Manager agent sets these configurations during agent installation.

To update settings:

1. Access the Product Directory.
2. On the left-hand menu, click the **NetScreen-Global PRO** managed product.
3. On the working area, click the **Configuration** tab.
4. Select **Firewall Management-NetScreen** on the Select a product drop down menu.
5. Click **Next**.
6. Update NetScreen settings. You can configure the following settings:
   - **IP address** - The IP address of the NetScreen-Global PRO machine
   - **Port** - The port used for communicating with Global PRO

- **User name** - An administrator-level user name for the Global PRO Arbitrator
- **Password** - An administrator-level password used by the user name you specified
- **Certificate name** - A 16-digit number assigned to an Arbitrator

Managing Child Servers

The Control Manager Enterprise version 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.

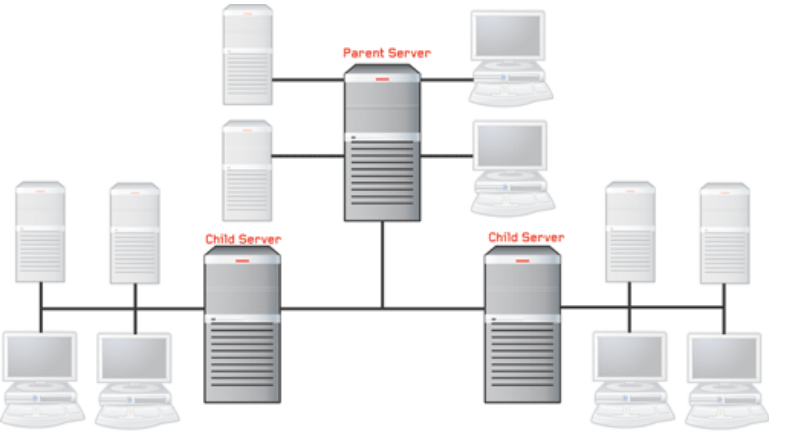


FIGURE 8-1. The cascading management structure uses two-tier Parent-Child architecture

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

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

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 8-16. 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).

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

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

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

Tip: Trend Micro recommends the management of not more than 200 child servers and 9,600 managed products for one Control Manager parent server.

Understanding the Parent Server and Child Server Communication

The cascading tree enumerates the parent server and all child servers in a Control Manager network.

Note: The parent server and child server communication uses port 10319 via TCP/UDP.

The following table describes the connection status in a Control Manager cascading tree:

ACTION	Parent / Child	Parent / Child	Parent / Child	Parent / Child	Stand Alone Server
Direct unregistration	●				
Force unregistration	●	●	●	●	
Registration					●
Uninstall Control Manager (save Database)	●	●	●	●	●
Uninstall Control Manager (delete Database)	●	●	●	●	●

TABLE 8-17. Parent and child server relationship

Based on the table:

- Direct unregistration of a disabled child server is not allowed
- Direct or force unregistration of an active child server retains the child server record in the parent server database and removes the child server record in the child server database
- If you uninstall the Control Manager application on a disabled child server, save the Control database, re-install Control Manager, and then re-register it to the same parent server, the child server status will remain the same—disabled

- If you uninstall the Control Manager application on a disabled child server, delete the Control database, re-install Control Manager, and then re-register it to the same parent server, the child server status will become active

In addition, the table highlights the following parent and child server relationship when the cascading relationship is set to enable:

- The parent server:
  - Polls each child servers to update the Status Summary screen in real-time
  - Updates a child server connection status every three minutes
- The child server:
  - Sends logs to the parent server
  - Sends new or updated report profiles

Disabling a child server does not permanently cut the connection between the two Control Manager servers. The parent and child server connection is still present. The parent server issues a single command to the child server — Enable Cascading Control Manager. Once the child server receives and accepts this command, the parent server resumes managing the child server.

Registering or Unregistering Child Servers

Use CasTool.exe 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.

The action to register or unregister child servers does not generate the same result as to enable or disable child servers. The former permanently cuts the parent and child server connection, while the latter temporarily suspends the connection by maintaining the heartbeat connection between two servers.

For example, if you registered child server xyz to parent server a, 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 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

Using CasTool.exe Commands

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

COMMAND	DESCRIPTION
castool /p:{parent server name:port}	To specify the parent server that the child server will register to. For example: castool /p:MUNICH_SRV1:2061 Use /p in conjunction with other CasTool child server registration commands. Do not use it separately.
castool /n:{parent server user account}	To specify the user account to register a child server to a parent server. {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. For example: castool /n:root Trend Micro suggests the use of the parent server superuser account created during the Control Manager installation. Use /n in conjunction with other CasTool child server registration commands. Do not use it separately.
castool /c:"{child server display name}"	To specify the name of the Control Manager child server displayed on the parent server's management console cascading structure tree. {child server display name} should not exceed 64 characters and should contain letters, numbers, and the following characters: "_", "-". For example: castool /c:"TOKYO_CHILD1" Use /c in conjunction with other CasTool child server registration commands. Do not use it separately.

TABLE 8-18. CasTool.exe Commands

COMMAND	DESCRIPTION
castool /f:"{local directory}"	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. For example: castool /f:"c:\e2epublic.dat" Use /f in conjunction with other CasTool child server registration commands. Do not use it separately.
castool /u	To unregister a child server from the parent server (normal unregistration). Use /u in conjunction with the CasTool debug command.
castool /e	To unregister a child server from the parent server (forced unregistration). Use /e to unregister a child server from a parent server whose status is disabled or abnormal.
castool /s	To specify that an HTTPS connection exists between parent and child server. The command gets the E2EPublic.dat key from the parent server. For example: castool /n:root /p:cm.test.com:8080 /c:”child_01” /s 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. Use /s in conjunction with CasTool registration commands. Do not use it separately.
castool /d	To enable CasTool.exe debugging. CasTool.exe saves debug logs in <root>:\Program Files\Trend Micro\Control Manager\debuglog folder. Use /d in conjunction with CasTool registration and unregistration commands. Do not use it separately.

TABLE 8-18. CasTool.exe Commands

Use CasTool.exe

CasTool.exe is a command-line program that allows you to 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 use 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 a list of commands you can execute.

Register a Child Server

Use CasTool.exe to register a child server to a parent server.

To register a child server:

1. Start CasTool.exe.
2. Execute one of the following:

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

Example 1:

```
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
```

Example 2:

```
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 will then register 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}"
```

Example 3:

```
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.

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

Unregister a Child Server

Use CasTool.exe or the cascading structure Directory Manager to unregister a child server to a parent server.

To Unregister a Child Server Using CasTool.exe:

1. Start CasTool.exe.
2. Execute one of the following:
   - Normal Unregister Command: `castool /u`
   - Force Unregister Command: `castool /e`

Tip: You can use the /d command to debug the process while CasTool unregisters a child server.

When you uninstall Control Manager from a child server, the child server executes the "castool /u /d" so that it automatically unregisters itself from a parent server.

To Unregister a Child Server Using the Cascading Manager:

1. Access the cascading structure tree.
2. On the leftmost menu, click **Cascading Manager**.
3. On the working area, select the child server you want to unregister and then click **Delete**.

Tip: Trend Micro recommends using the Cascading Manager Delete option only when the child server status is abnormal. Be careful when using the Cascading Manager, you may accidentally unregister child servers that are not supposed to be unregistered.

Debug CasTool.exe

Use the CasTool.exe /d command to debug the tool. The feature proves especially helpful when registering or unregistering from a parent server results in program errors or unsuccessful attempts.

To debug CasTool.exe:

1. Start CasTool.exe.
2. Execute the debug command in conjunction with the register or unregister command. For example:

   To register a child server:

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

   To unregister a child server:

   ```
   castool /d /u
   ```

Access the Cascading Structure Tree

Use the cascading structure tree to view and access functions for child servers.

Note: You can only access the cascading structure tree via the parent server management console.

To access the cascading structure tree:

1. Click **Products** on the main menu.
2. On the left-hand menu, select Control Managers from the list and then click **Go**.

View the Cascading Structure Status Summaries

The Global Status screen displays the Antivirus, Content Security, and Web Security summaries for all managed products handled by the child servers. By default, the Global Status and Status tabs display a week's worth of summaries. You can change the scope to Today, Last Week, Last Two Weeks, or Last Month available in the Display summary for list.

To view the cascading structure status summaries:

1. Access the cascading structure tree.
2. On the left-hand menu, select the parent or a child server.
   - If you click the parent server, the Global Status tab displays the group summaries of the managed products handled by all child servers
   - If you click a child server, the Product Status tab displays the group summaries of the selected child server

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

   The default time interval is 1440 minutes (1 day) and start time is "12:00 am". Configure these values to suit your management needs.

Note: A child server will upload status summary to the parent server when either 2,500 records is reached or 3 minutes elapsed time has passed. During the time when the child server has not yet uploaded new logs to the parent server, the Outdated,

Current, and Total managed product information in the Component Status table of the child server Product Status screen may not be current.

Configure Log Upload Settings

Use the child server Configuration tab to set the schedule as to when the child server sends logs to the parent server.

To configure log upload setting:

1. Access the cascading structure tree.
2. On the left-hand menu, select a child server.
3. On the working area, click the **Configuration** tab.
4. Click the **Schedule child Control Manager server log uploads** link.
5. On the Log Upload, select **Upload child Control Manager server logs to the parent server**.
6. Set the upload scheduled.
   - Select **Upload logs as soon as they are available** to instruct the child server to immediately send logs to the parent server

Note: Selecting **Upload logs immediately** will prompt the child server to constantly send logs to the parent server - causing network traffic.

   - Select **Schedule log upload to upload logs at a specific schedule**

   a. Set the Frequency—Daily or Weekly.

   b. Set the Start time by selecting the hour and minutes from the list. By default, the Start time is 20:00.

7. Select **Set the maximum upload time: hours** and set the maximum upload time that determines the length of time that the child server will upload logs to the parent server. The default maximum upload time is 8 hours.
8. Click **Save**.

Tip: Trend Micro recommends that you schedule the log upload with "Frequency = Daily" and "Start Time = after office hours or during off-peak hours" to prevent

network traffic during business hours. However, when the child server has not yet uploaded new logs to the parent server, the Component Status table of the child server's Product Status screen may not show current Outdated, Current, and Total managed product information.

Enable or Disable Child Server Connection

Use the child server Configuration tab to enable or disable child server connection to the parent server.

To enable or disable child server connection:

1. Access the cascading structure tree.
2. On the left-hand menu, select a child server.
3. On the working area, click the **Configuration** tab.
4. Click the **Enable or Disable a child server connection link**.
5. On the working area, do one of the following:
   - Select **Enable a connection to this child Control Manager server** to enable a disabled child server
   - Select **Disable the connection to this child Control Manager server** to disable an enabled child server

WARNING! *Use care when disabling a child server connection. Managed products information registered to a disabled child server will not be automatically uploaded to the parent server after you re-enable the child server connection. Restart the Trend Micro Control Manager service after enabling a child server to upload new managed product information to the parent server.*

6. Click **Apply**.

Note: A disabled child server does not send logs to the parent server or queue logs on its local server (that is, on the disabled child server itself)

Issue a Task to Child Servers

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

- Deploy Pattern Files/Cleanup Templates and Anti-spam Rules
- Deploy engines
- Deploy program files
- Open Child Console

To issue a task:

1. Access the cascading structure tree.
2. On the left-hand menu, select a child server.
3. On the working area, click the **Tasks** tab.
4. Click any of the available tasks.
5. On the task page, click **Deploy Now**.
6. Monitor the progress through Command Tracking. Click the **Command Details** link at the response screen to view command information.

Query and View Child Server Logs

Use the Logs tab to query and view logs for the parent or specific child server.

To query and view parent and child server logs:

1. Access the cascading structure tree.
2. On the left-hand menu, click the parent server or a specific child server.
3. On the working area, click the **Logs** tab.

4. Select the client log type:

Event Logs

On the Event Logs Query page, provide information for the following search parameters:

PARAMETER	DESCRIPTION
Severity	Refers to the degree of information available. The options are: Critical, Warning, Information, Error, Unknown. Select the check box of your chosen parameter
Incident	Refers to events. The options are: All events, Virus outbreak, Module update, Service On, Service Off, Security violation, Unusual network virus behavior
Product	If you select a folder, this list shows the managed products belonging to the folder. To view information on all products, select All. Otherwise, query logs of a specific managed product
Logs for	View all logs, or only those that the managed product generated within a specific interval. For the latter option, you can specify logs for the last 24 hours, day, week, month, or custom range If you chose Specified range, select the appropriate month, day, and year for the Start date and End date
Sort logs by	Sort results according to the date/time, computer name, product, event, or severity
Sort order	Sort results in ascending and descending order

TABLE 8-19. Search Parameters for Event Logs

Security Logs

a. On the Security Logs Query screen, select All virus log incidents or a specific security logs type and then click **Query**.

b. Provide information for the following search parameters:

PARAMETER	DESCRIPTION
Logs for	View all logs, or only those that the managed product generated within a specific interval. For the latter option, you can specify logs for the last 24 hours, day, week, month, or custom range If you chose Specified range, select the appropriate month, day, and year for the Start date and End date
Sort logs by	Sort results according to the date/time, computer name, product, event, or severity
Sort order	Sort results in ascending and descending order

TABLE 8-20. Search Parameters for Security Logs

5. Click **Display Logs** to begin the query. The Query Result screen displays the results in a table format.

WARNING! *The Generated at entity column of the result table indicates the Control Manager parent server time.*

View Child Server Reports

Use the Reports tab to view a child server's existing report profiles.

To view child server reports:

1. Access the cascading structure tree.
2. On the left-hand menu, select a child server.
3. On the working area, click the **Reports** tab.

Note: When multiple reports are available in the Reports screen, sort reports according to Report Profile or Last Created date.

4. Under Available Reports, click the **View** link of the report profile that you want to open.

5. On the Available Reports for {profile name}, sort reports according to **Submission Time** or **Stage Completion Time**.
6. Under the Status column, click **View Report**. A new browser window opens that displays the reports content.

Refresh the Cascading Tree

To refresh the cascading tree:

While at the cascading tree, click the icon on the upper right corner of the left-hand menu.

Renaming a Child Server Alias

Use the rename option to change a child server alias.

To change a child server alias:

1. Access the cascading structure tree.
2. On the left-hand menu, click **Cascading Manager**.
3. On the working area, right-click the child server whose alias you want to rename and then select **Rename** from the pop-up menu. The child server alias becomes an editable field.
4. Type the new alias.
5. Click **Save**.

Recover Child Servers Accidentally Removed from the Cascading Manager

In an event when you have accidentally unregistered a child server using the Cascading Manager Delete option, you need to unregister and then re-register the child server to the parent server.

To recover child servers accidentally removed from the Directory Manager:

1. From the child server's Windows 2000 command interpreter, execute the force unregistration command:

   ```
   castool /e
   ```

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

Understanding the Control Manager Database

Control Manager uses the Microsoft SQL Server database (db_ControlManager.mdf) to store data included in logs, Communicator schedule, managed product and child server information, user account, network environment, and notification settings.

The Control Manager server establishes the database connection using a System DSN ODBC connection. The Control Manager installation generates this connection as well as the ID and password used to access db_ControlManager.mdf. The default ID is sa. Control Manager encrypts the password.

To maximize the SQL server security, configure any SQL account used to manage db_ControlManager with the following minimum permissions:

- dbcreator for the server role
- db_owner for the db_controlmanager role

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

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

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

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

Because the Control Manager database runs on a scalable database — SQL Server, the theoretical limit is whatever the hardware can handle. Trend Micro has tested up to 2,000,000 entries. If the database server performance is overworked or pushed to its limit, the management console may experience connection time-outs.

Understanding the db_ControlManager Tables

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

Note: Do not use any of the SQL tools to add, delete, or modify records without instructions from Trend Micro Technical Support.

The following tables make up the Control Manager database:

Directory Manager Tables	Description
CDSM_Entity	Stores the managed product information
CDSM_Agent	Stores Communicator information
CDSM_Registry	Stores registry information
CDSM_UserLog	Stores information as to who, which options, and what time a user accesses the management console; this is useful for auditing management console accesses
CDSM_SystemEventlog	Stores system logs generated by internal processes

TABLE 8-21. Directory Manager Tables

Server Command Controller Tables	Description
tb_TVCSCommandList	Stores managed product commands
tb_TVCSCommandTaskQueue	Stores commands issued to managed products
tb_CommandTracking	Stores command status

TABLE 8-22. Server Command Controller Tables

Server Command Controller Tables	Description
tb_CommandItemTracking	Stores detailed command status
tb_ProcessInfo	Stores MsgReceiver.exe, CmdProcessor.exe, LogReceiver.exe, LogRetriever.exe, and UIProcessor.exe information
tb_LoginUserSessionData	Stores user logon session control
tb_ManualDownload	Stores manual download information
tb_ScheduleDownload	Stores scheduled download information

TABLE 8-22. Server Command Controller Tables

Managed Product Tables	Description
tb_EntityInfo	Stores the managed product information
tb_VirtualEntity	Stores TVCS1.x agent registration information

TABLE 8-23. Managed Product Tables

Log Tables	Description
tb_TempLog	Stores the raw data of product logs
tb_AV*Log	Stores product log * corresponds to Virus, Event, Status, PEInfo, WebSecurity. These tables stores the product status log as well as the pattern and engine version, update and deploy time, and the unhandled virus count.
tb_InValidLog	Stores unidentified log information
• tb_TotalWebSecurityCount • tb_TotalVirusCount • tb_TotalSecurityCount • tb_TopTenSource • tb_TopTenDestination • tb_TopTenVirus	Stores virus summary information for Status Summary and reports
tb_LogPurgePolicy	Stores purge log settings

TABLE 8-24. Log Tables

Log Tables	Description
tb_LogPurgeCounter	Stores purge log counter
• tb_InstanceForVirusOutbreak • tb_InstanceForSpecialVirus • tb_InstanceForVirusOutbreak	Stores log instanced used in alert notifications

TABLE 8-24. Log Tables

Notification Tables	Description
• tb_Alert_NTF_JobList • tb_Event_NTF_JobList	Stores notification queue list
tb_EventNotificationFilter	Stores Event Center configuration
• tb_SendEMailNotification • tb_SendPagerNotification • tb_SendSNMPTrapNotification • tb_SendWindowsNTEventLogNotification	Stores notification method settings
tb_VirusOutBreakPolicy	Stores rules used during virus outbreak
tb_SpecialVirusPolicy	Stores the user specified virus name
• tb_VirusOutbreakAccumulate • tb_SpecialVirusAccumulate	Stores virus counter information
• tb_UGNtfRelation • tb_NtfUserGROUP • tb_GroupAndUserRelation	Stores user and group notification settings

TABLE 8-25. Notification Tables

Report Tables	Description
• tb_ReportScheduleTask • tb_ReportTaskQueue	Stores and handles report generation tasks
tb_ReportItemTracking	Stores report template file catalog

TABLE 8-26. Report Tables

Pattern and Engine Deployment Tables	Description
• tb_DeploymentPlans • tb_DeploymentPlansTF	Stores deployment plan information
tb_DeploymentPlanTasks	Stores deployment task queue
tb_DeployNowJobList	Stores ongoing deployment plan status
tb_DeployCommandTracking	Stores deployment command tracking information
tb_DeploymentPlanTargets	Stores the managed product information that applied the deploy command

TABLE 8-27. Pattern and Engine Deployment Tables

Backing Up db_ControlManager Using osql

In an event when the Control Manager database is corrupted or destroyed, use a backup copy to restore your settings. When using MSDE, use the MSDE command line interface — osql, to generate a database backup.

To generate a database backup using osql:

1. From the Control Manager server, click **Start** > **Run**.
2. Type `cmd` and then click **OK**.
3. On the Windows 2000 command interpreter, execute the following commands:

```
osql -U {ID} -P {password} -n -Q "BACKUP DATABASE
{Control Manager database} TO DISK = '{path and
backup name}'"
```

Where:

{ID} — administrator user name account used to access the Control Manager database. This is defined during the Control Manager setup.

{password} — password used to access the Control Manager database. This is defined during the Control Manager setup.

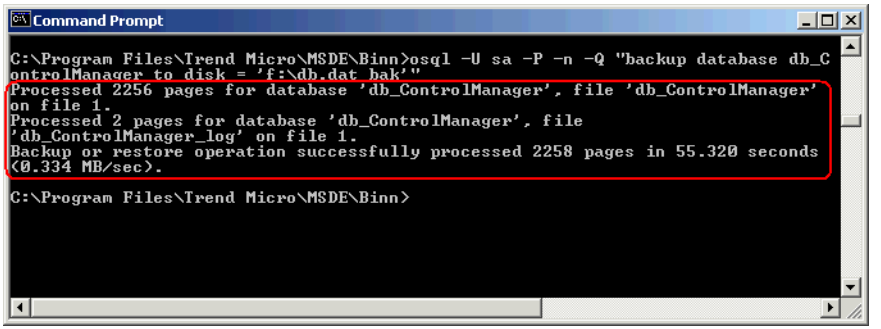
{Control Manager database} — name of the Control Manager database

{path and backup name} — target location and the backup filename

For example:

```
osql -U sa -P -n -Q "BACKUP DATABASE
db_ControlManager TO DISK = 'f:\db.dat_bak'"
```

A successful database backup produces a similar result as the following:



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

Tip: Trend Micro recommends backing up the Control Manager database regularly. Always back up when you are about to modify the Control Manager database (for example, installing a managed product).

Restore Backup db_ControlManager Using osql

Use the MSDE command line interface that comes with your version of MSDE, <root>:\Program Files\Trend Micro\MSDE\osql, to restore backup database.

To restore the backup database:

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

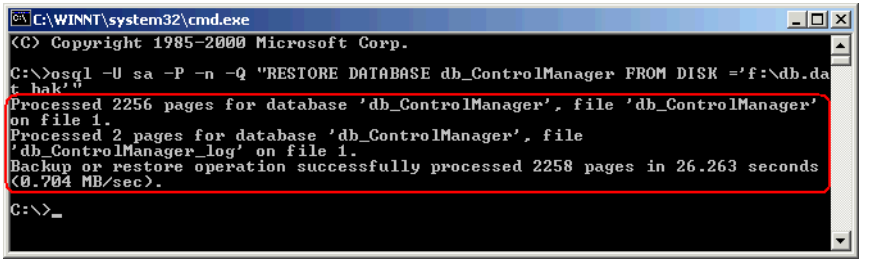
5. Type cmd and then click **OK**.
6. On the Windows 2000 command interpreter, execute the following commands:

```
osql -U {ID} -P {password} -n -Q "RESTORE
DATABASE {Control Manager database} FROM DISK =
'{path and backup name}'"
```

For example:

```
osql -U sa -P -n -Q "RESTORE DATABASE
db_ControlManager FROM DISK = 'f:\db.dat_bak'"
```

A successful database restoration produces a similar result as the following:



7. Click **Start** > **Programs** > **Administrative Tools** > **Services** to open the Services screen.
8. Right-click **<Control Manager service>**, and then click **Restart**.
9. Start Control Manager.

For more information on how to use osql, refer to the MSDN library.

Backing Up db_ControlManager Using the SQL Server Enterprise Manager

In an event when the Control Manager database is corrupted or destroyed, use a backup copy to restore your settings. When using SQL Server, use the SQL Server Enterprise Manager to back up the Control Manager database.

To back up db_ControlManager using the SQL Server Enterprise Manager:

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

Tip: Trend Micro recommends regular back ups of the Control Manager database. Always back up when you are about to modify the Control Manager database (for example, adding installing a managed product).

Restore backup db_ControlManager Using SQL Server Enterprise Manager

Use the SQL Server Enterprise Manager to restore the backup Control Manager database.

To restore backup db_ControlManager:

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

4. Click **Start > Programs > Microsoft SQL server > Enterprise manager** to access the SQL Server Enterprise Manager.
5. On the console, click **Microsoft SQL servers > SQL server group > {SQL server} (Windows NT) > Databases**. {SQL server} is the SQL Server hostname.
6. Right-click **db_controlmanager** and then click **All tasks > Restore Database…**.
7. On the Restore database, select the database to restore.
8. Click **OK** to start the restoration process.
9. Click **OK** when the message "Restore of database '{Control Manager database"}' completed successfully."
10. Click **Start > Programs > Administrative Tools > Services** to open the Services screen.
11. Right-click **<Control Manager service>**, and then click **Restart**.
12. Start Control Manager.

Shrink db_controlmanager_log.ldf Using SQL Server Enterprise Manager

The transaction log file for the Control Manager database is …\data\db_ControlManager_log.LDF. SQL Server generates the transaction log as part of its normal operation.

db_ControlManager_log.LDF contains all managed product transactions using db_ControlManager.mdf.

By default, the transaction log file has no file size limit on the SQL Server configuration. This leads to filling up the available disk space.

To shrink the db_controlmanager_log.ldf file size:

1. Back up the Control Manager database using the SQL Server Enterprise Manager.
2. Purge the transaction log.
3. On the SQL Server, click **Start > Programs > MS SQL Server** to open the Query Analyzer.
4. Select the SQL server and specify the Windows authentication if prompted.

5. On the list, select the **db_ControlManager** database.
6. Copy and paste the following SQL script:

```
DBCC SHRINKFILE(db_controlmanager_Log, 10)
BACKUP LOG db_controlmanager WITH TRUNCATE_ONLY
DBCC SHRINKFILE(db_controlmanager_Log, 10)
```

Note: On the SHRINKFILE(db_controlmanager_Log, 10) function, the parameter 10 will be the resulting file size of db_controlmanager_Log.ldf in megabytes (MB).

7. Click **Execute** to run the SQL script.
8. Check the `db_controlmanager_log.ldf` file size. It should be 10MB.

Shrink db_ControlManager.mdf and db_ControlManager.ldf Using SQL Commands

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

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

```
Alter Database db_controlManager set recovery
FULL
Backup log db_controlManager with truncate_only
DBCC shrinkDatabase(db_controlManager)
```

Note: The 3rd command might take longer depending on the size of the database.

```
EXEC sp_dboption 'db_ControlManager', 'trunc. log
on chkpt.', 'TRUE'
Alter Database db_controlManager set recovery
simple
Alter Database db_controlManager set auto_shrink
on
```

Chapter 9

Using Trend Micro Services

This chapter provides details about the various services available when using Control Manager. Topics include the following:

- *Understanding Trend Micro Services* on page 9-2
- *Understanding Enterprise Protection Strategy (EPS)* on page 9-3
- *Introducing TrendLabs Message Board* on page 9-5
- *Participating in the World Virus Tracking Program* on page 9-5
- *Introducing Outbreak Prevention Services* on page 9-6
- *Preventing Virus Outbreaks and Understanding the Outbreak Prevention Mode* on page 9-9
- *Outbreak Prevention Mode Tutorial* on page 9-18
- *Using Vulnerability Assessment* on page 9-22

Understanding Trend Micro Services

Trend Micro recognized that a new approach to antivirus management was needed to significantly reduce the threat and costs of virus attacks. After considerable research and testing, Trend Micro has redefined virus protection—moving beyond reactive, point products to a proactive, centralized protection system that enables a rapid, methodical response to any attack on any system—from Internet gateways to PCs, file servers, and email servers.

The new approach combines the following services:

- **TrendLabs Message Board -** A real-time message board that quickly provides latest update component information and characterizes new viruses so they can be identified and quickly eliminated
- **Outbreak Prevention Services** - Industry-unique services that provide Outbreak Prevention Policies to help deflect, isolate, and stem outbreak attacks
- **Damage Cleanup Services** - Comprehensive services that help clean and repair systems infected by Trojan viruses or worms
- **Vulnerability Assessment** - provides system administrators or other network security personnel with the ability to assess security risks to their networks

Trend Micro's integrated approach to virus protection begins when an administrator sends a virus sample to TrendLabs where a targeted prevention policy (a pre-pattern file recommendation) is created to contain the outbreak and prevent spreading. When Control Manager retrieves this information, system administrators can use Outbreak Prevention Services to quickly understand the scope of the attack and take effective interim steps against it without jeopardizing business productivity by having to shut down a port. They can also quickly disseminate Outbreak Prevention Policy recommendations to other system administrators within the enterprise who may be hit with the same problem.

This proactive response—the ability to incorporate antivirus knowledge throughout the network and have real-time visibility into all virus-related events as they happen—can only be accomplished with central management. The rapid identification services and delivery systems shorten the time to containment, thereby limiting the spread of the virus. This process minimizes the effect of the virus on the productivity of the enterprise, as well as dramatically reducing the costs of cleanup.

Understanding Enterprise Protection Strategy (EPS)

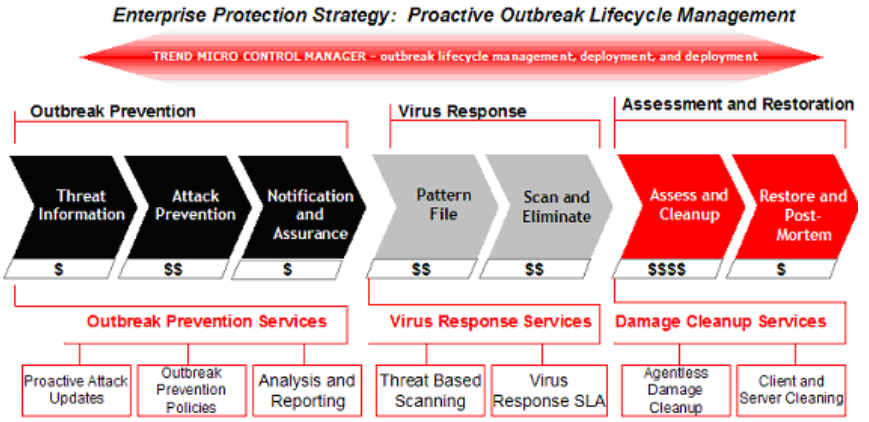


FIGURE 9-1. Enterprise Protection Strategy

EPS arms businesses with industry-specific services and support to wage war against mixed-threat attacks with confidence.

- Proactive services combat viruses by containing infiltration and cleaning potential attackers hiding in systems
- Industry's only Virus Response Service Level Agreement guarantees virus detection
- EPS architecture exports Trend Micro's 'think-tank' of antivirus knowledge and support to vulnerable points on the network

EPS establishes a 'command center' to help identify and defend all vulnerabilities within the enterprise.

- Enterprise-wide policy coordination and reporting
- Partner integration with third-party devices
- Heterogeneous platform support

EPS provides a battle plan during an attack while minimizing casualties and damage.

- Virus Outbreak Lifecycle approach– industry unique and based on real customer experience
- Enterprise-wide coordination identifies network vulnerabilities and helps enable customers to proactively attack outbreaks
- Focus on the critical stages before and after pattern file deployment manages explosive costs and system damage

Highlighting the Value of EPS

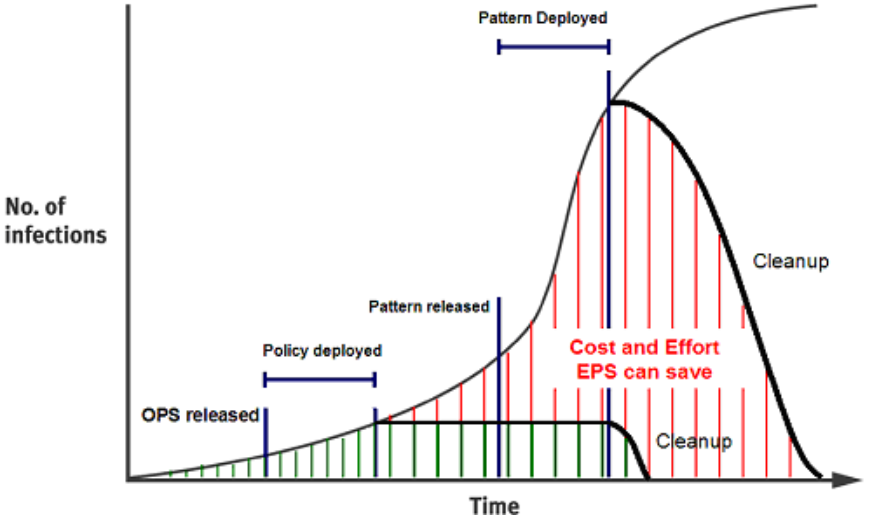


FIGURE 9-2. Cost vs. Effort

The graph demonstrates that putting protection in place as quickly as possible and ridding the network of post-attack vulnerabilities can minimize the devastating effects of outbreaks over time.

By using EPS and Outbreak Prevention Services, enterprises can minimize their risk and dramatically lower costs. By deploying policies early in the lifecycle and before pattern file generation, an organization can dramatically reduce the cost and effort (area under the curve), in addition to increasing the overall level of protection.

Trend Micro's expertise, architecture, and services provide a strong return on investment, improve overall protection, and increase the productivity of enterprise networks.

Introducing TrendLabs Message Board

As a Control Manager user and Trend Micro customer, you can receive alerts from TrendLabs(SM) about emerging virus outbreaks before they affect your system.

The Trend Micro TrendLabs Message Board provides version numbers and the times when TrendLabs releases update components (such as virus pattern files, scan engines, damage cleanup templates and Outbreak Prevention Policies) to identify the threats against which you should protect yourself with Control Manager.

Participating in the World Virus Tracking Program

The Trend Micro Virus Map displays information about actual virus infections detected by HouseCall, our online virus scanner for PCs, and managed products registered to Trend Micro Control Manager. You can view this dynamic map to analyze worldwide virus trends in real time and help predict virus outbreaks, and prevent them proactively.

You can add your data to the Trend Micro Virus Map by choosing to participate in the World Virus Tracking Program. When you choose to participate, Trend Micro Control Manager will only send anonymous information (via the HTTPS protocol and port 443), and you can stop participating any time by choosing No and updating your status on the Control Manager management console.

To participate in the World Virus Tracking Program:

1. Click **Administration** on the main menu.
2. On the left-hand menu, click **World Virus Tracking Program**.
3. On the working area, click **Yes, I want to participate...**.
4. Click **Save**.

Introducing Outbreak Prevention Services

FIGURE 9-3. Outbreak Prevention Services

Understanding Outbreak Prevention Services

The Outbreak Prevention phase refers to the critical period when managed products have identified a virus outbreak, but before a pattern file has become available. During this crucial time, system administrators must endure a chaotic, time-consuming process of communication—often to global and decentralized groups within their organizations.

Outbreak Prevention Services delivers notification of new threats and continuous and comprehensive updates on system status as an attack progresses. The timely delivery of detailed virus data coupled with predefined, threat-specific action and scanning policies delivered immediately after a new threat identification allows enterprises to quickly contain viruses and prevent them from spreading.

Additionally, by centrally deploying and managing policy recommendations, Outbreak Prevention Services helps eliminate the potential for miscommunication, applies policies, and deploys critical attack information as it is happening.

By providing automatic or manual download and deployment of policies via Trend Micro Control Manager, Outbreak Prevention Services import knowledge to critical access points on the network directly from experts at TrendLabs, Trend Micro's global security research and support network.

This subscription-based service requires minimal up-front investment and provides enterprise-wide coordination and outbreak management via Trend Micro products which reside across critical points on the network including the Internet gateway, mail server, file server, caching server, client, remote and broadband user, and third-party enterprise firewalls.

Benefits of Outbreak Prevention Services

Besides quickening the enterprise's response time, Outbreak Prevention Services can deliver significant operational protection and cost benefits.

BENEFIT	REASONS
Proactive Protection Against Mixed Threat Attacks	• Contains outbreaks without stopping business productivity (that is, shut down ports) • Reduces the chaos associated with defining the threat and behavior • Automatic policy creates a 24x7, no-touch defense system
Expertise and Knowledge	• Recommendations from the experts– policy formulation • Knowledge base of policies for prior viruses
Consistency, Reduced Coordination, Cost Reduction	• Consistent application of policy • Removes logistical challenges of notifying critical parties
Policy and Attack Correlation	• Assurance and reporting = Enterprise-wide visibility and coordination

TABLE 9-1. Benefits of OPS

Activate Outbreak Prevention Services

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

To activate Outbreak Prevention Services:

1. Click **Administration** on the main menu.
2. On the left-hand menu under Registration, click **License Information**.
3. On the working area under Outbreak Prevention Services License Information, click the **Activate the product** link.

4. Do the following:
   - **If you don't have an Activation Code:** click the **Register online** link and follow the instructions on the Online Registration Web site to obtain an Activation Code
   - **If you have an Activation Code:** in the New box, type your Activation Code
5. Click **Activate**.

View Outbreak Prevention Services Status

View the Outbreak Prevention Services Status page to instantly know the state of the following service status items:

ITEM	DESCRIPTION	STATE
Scheduled policy download	Provides information about whether Control Manager automatically downloads Outbreak Prevention Policies according to a specified schedule.	On/Off
Automatic Outbreak Prevention Mode for red alert	Provides information about whether Control Manager will automatically trigger Outbreak Prevention Mode for red alert viruses.	On/Off
Automatic Outbreak Prevention Mode for yellow alert	Provides information about whether Control Manager will automatically trigger Outbreak Prevention Mode for yellow alert viruses.	On/Off

TABLE 9-2. OPS Status

In addition, this page also provides an easy way to view the Control Manager components and the version that are currently in use.

To view the Outbreak Prevention Services status:

1. Click **Services** on the main menu.
2. On the left-hand menu under Services, click **Outbreak Prevention**. This page automatically refreshes to make sure the top threat and status information is current.

Preventing Virus Outbreaks and Understanding the Outbreak Prevention Mode

Even before receiving the appropriate pattern file from Trend Micro, an enterprise can deflect, isolate and stem attacks with the help of attack-specific information and Outbreak Prevention Policies from Trend Micro Outbreak Prevention Services. With Outbreak Prevention Services, you can centrally deploy policy recommendations to minimize coordination efforts and help ensure a consistent application of policies throughout the network. Policy recommendations delivered via Outbreak Prevention Services help system administrators respond quickly against new viruses to contain outbreaks, minimize system damage and prevent undue downtime.

Using deployment plans you can restrict the application of Outbreak settings to specific segments of the network if you have divided your network segment into different deployment plans. This approach can prove very useful for large networks composed of several sites. Administrators can apply the settings to only those areas actually affected by the outbreak.

Outbreak Prevention Mode includes the following elements:

- Downloads Outbreak Prevention Policies — a collection of recommended software settings for handling the virus outbreak
- Displays the product settings that will be set, thereby allowing you to modify the settings according to the demands of your network

  Outbreak Prevention Services provide recommendations for managed products that must be set.
- Blocks/deflects malicious code from entering or spreading throughout the network
- Customizes Control Manager's notification functions for the outbreak
- Real-time reporting on policy deployment and status
- Ability to approve and deploy policy manually or automatically
- Allows you to set a special, abbreviated, update-download schedule that is only active for the duration of the policy

  This enables you to automatically update new virus patterns as soon as they become available.
- Detailed information on threats as soon as they are characterized

Understanding Outbreak Prevention Policies

Apply Outbreak Prevention Policies, collections of product settings, to your managed products using Outbreak Prevention Services. Trend Micro creates these settings in response to virus outbreaks, and provides them to Control Manager users as part of the Outbreak Prevention Services.

These policies serve as the key to protecting a network during a virus outbreak. They protect critical points on the network, including the Internet gateway, mail server, file server, caching server, client, remote and broadband user, and third-party enterprise firewalls. For example, viruses that only propagate through email will only have policies with settings for messaging systems.

The following diagram illustrates how Control Manager can deploy policies at all layers to protect critical points during a virus outbreak.

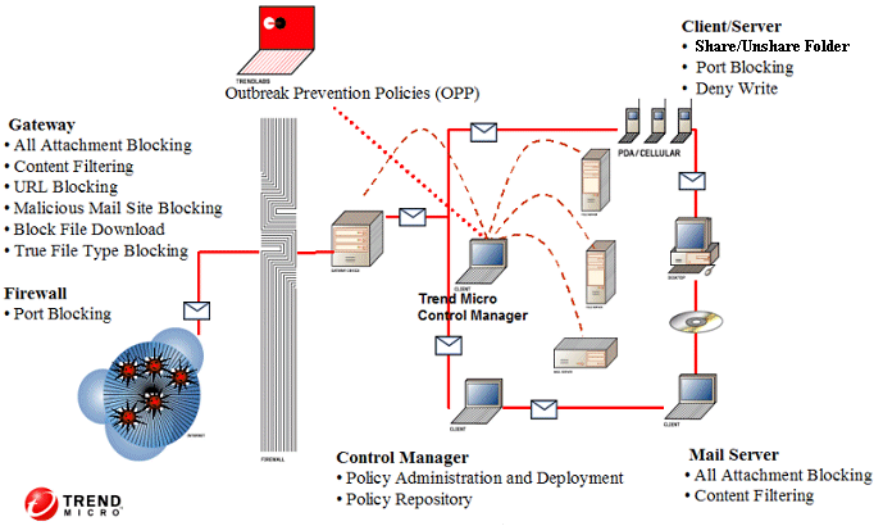


FIGURE 9-4. Deploying OPP

Access the Outbreak Prevention Services Settings Screen

To access the Outbreak Prevention Services Settings screen:

1. Click **Services** on the main menu.

2. On the left-hand menu under Services, click **Outbreak Prevention > Settings**.

Update Outbreak Prevention Policies

It is important to use the latest Outbreak Prevention Policies to protect your network during virus outbreaks. Update Outbreak Prevention Policies both manually or set a scheduled update.

To Update Outbreak Prevention Policies Manually:

1. Click **Services** on the main menu.
2. On the left-hand menu under Services, click **Outbreak Prevention**. This page automatically refreshes to make sure the top threat and status information is current.
3. On the working area under Service Status, click **Update Now** to download the latest Outbreak Prevention Policies.
4. Click **OK** twice after downloading the Outbreak Prevention Policies.

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

Tip: After installing Control Manager for the first time, Trend Micro strongly recommends you perform an Update Now to update your policies immediately. For subsequent updates, use the Scheduled Update function.

To Schedule Updates to Outbreak Prevention Policies:

1. Click **Services** on the main menu.
2. On the left-hand menu under Services, click **Outbreak Prevention > Settings**.
3. On the working area, click the **Download** tab.
4. Under Scheduled policy download settings, select the **Enable scheduled policy update** check box.
5. From the Download frequency list, choose the number of minutes for Control Manager to check for updated Outbreak Prevention Policies.
6. Under Download source, click the source that contains the latest Outbreak Prevention Policies. By default, this is the Trend Micro ActiveUpdate server. If you choose another Internet source, type the location in **Other update source**.

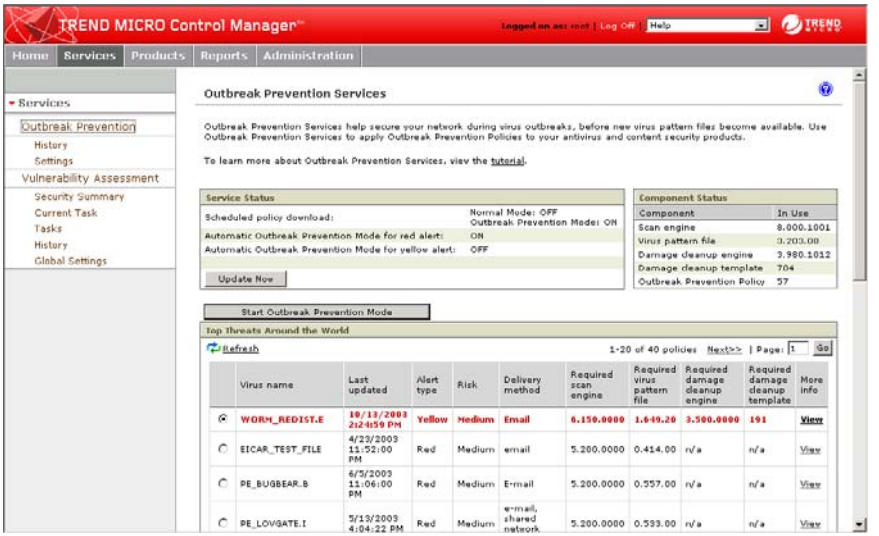
7. Click **Save**.
8. Click **OK**.

Start Outbreak Prevention Mode

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

To start Outbreak Prevention Mode:

1. Click **Services** on the main menu.
2. On the left-hand menu under Services, click **Outbreak Prevention**. This page automatically refreshes to make sure the top threat and status information is current.



3. On the working area under Service Status, click **Update Now** to download the latest Outbreak Prevention Policies (this is optional if you have already enabled Scheduled Update and are using the latest Outbreak Prevention Policies).
4. Click **OK** twice after downloading the Outbreak Prevention Policies.

5. Under Top Threats Around the World, click the name of the virus that currently presents a threat to your network. By default, Control Manager lists newest threat first, and the remaining threats in alphabetic order. Each Outbreak Prevention Policy is designed to counter a specific threat.
6. Click **Start Outbreak Prevention Mode**.
7. Under Outbreak Prevention Policy, in the Policy in effect for list, choose the number of days that Control Manager continues in Outbreak Prevention Mode.
8. From the Deployment plan list, choose a plan to deploy the Outbreak Prevention Policies to the managed products.
9. Under Outbreak Prevention Policy Details, select the **Do not block permitted port numbers specified in the Outbreak Prevention settings** check box to ensure ports defined as exceptions are not blocked.
10. Configure managed product settings.
11. Click **Recommended Settings**.
12. Click **Activate**.
13. Click **OK**. Outbreak Prevention Mode has started and the icon appears on the management console header.

Edit an Outbreak Prevention Policy

After you have started Outbreak Prevention Mode, modify Outbreak Prevention Policies to suit your network needs. For example, you could:

- Change the duration of the length of Outbreak Prevention Mode
- Choose a different deployment plan
- Permit specified port numbers
- Configure registered managed product settings

To edit an Outbreak Prevention Policy:

1. Click **Services** on the main menu.
2. On the left-hand menu under Services, click **Outbreak Prevention**. This page automatically refreshes to make sure the top threat and status information is current.
3. On the working area, click **Edit Policy**.

4. Under Outbreak Prevention Policy, in the Policy in effect for list, choose the number of days that Control Manager continues in Outbreak Prevention Mode.
5. From the Deployment Plan list, choose a plan to deploy the Outbreak Prevention Policies to the managed products (to view/edit or add deployment plans, click Administration, and then under Update Manager, clic**k Deployment Plan).**
6. **Under Outbreak Prevention Policy Details, select the Do not block permitted port numbers specified in the Outbreak Prevention settings** check box to ensure ports defined as exceptions are not blocked.
7. Configure managed product settings.
8. Click **Recommended Settings**.

Tip: When you click Recommended Settings, the TrendLabs recommended settings are applied and any user-defined settings are removed. If necessary, based on the latest information, these recommendations are updated with each Outbreak Prevention Policy release. Trend Micro recommends you apply the recommended settings.

9. Click **Activate**.

Set Automatic Outbreak Prevention Mode

Outbreaks can occur anytime. Automatic Outbreak Prevention can automatically deploy Outbreak Prevention Policies for red or yellow alert viruses to managed products and send notifications.

VIRUS ALERT	DESCRIPTION
Criteria for Red Alert Viruses	Several infection reports from each business unit reporting rapidly spreading malware, where gateways and email servers may need to be patched. The industry's first 45-minute Red Alert solution process is started: An official pattern release (OPR) is deployed with notification of its availability, any other relevant notifications are sent out, and fix tools and information regarding vulnerabilities are posted on the download pages.

TABLE 9-3. Virus Alert Criteria

VIRUS ALERT	DESCRIPTION
Criteria for Yellow Alert Viruses	Infection reports are received from several business units as well as support calls confirming scattered instances. An official pattern release (OPR) is automatically pushed to deployment servers and made available for download. In case of an email-spreading malware, content filtering rules, called Outbreak Prevention Policies (OPP), are sent out to automatically block related attachments on servers equipped with the product functionality.

TABLE 9-3. Virus Alert Criteria

To set Automatic Outbreak Prevention Mode:

1. Click **Services** on the main menu.
2. On the left-hand menu under Services, click **Outbreak Prevention**. This page automatically refreshes to make sure the top threat and status information is current.
3. Click the **Automatic Outbreak Prevention Mode** tab.
4. Do the following:
   - To set Automatic Outbreak Prevention Mode for red alert viruses, under Red Alert Viruses, select the **Enable automatic outbreak prevention** check box.
   - To set Automatic Outbreak Prevention Mode for yellow alert viruses, under Yellow Alert Viruses, select the **Enable automatic outbreak prevention** check box.
5. From the Prevention duration list, choose the number of days that Outbreak Prevention Mode is active.
6. From the Deployment plan list, choose a plan to deploy the Outbreak Prevention Policies to the managed products.
7. Do the following:
   - Under Excluded products, select managed products that will not receive Outbreak Prevention Policies. Important: These products will not benefit from Outbreak Prevention Services and will have a greater chance of becoming infected during outbreaks.
   - Under Permitted ports, specify ports that Control Manager will keep open during an outbreak.

- To automatically trigger Damage Cleanup Services, under Damage Cleanup, select the **Enable Damage Cleanup Services** check box. Click **Damage Cleanup** to configure Damage Cleanup Services settings.
- To automatically trigger Vulnerability Assessment, under Vulnerability Assessment, select the **Enable Vulnerability Assessment** check box.

8. Click **Save**.

Configure Outbreak Prevention Mode Download Settings

Configure how often Control Manager checks for updated Outbreak Prevention Policies during Outbreak Prevention Mode. In addition, you can also choose which deployment plan to use to deploy the updated Outbreak Prevention Policies.

To configure Outbreak Prevention Mode download settings:

1. Click **Services** on the main menu.
2. On the left-hand menu under Services, click **Outbreak Prevention**. This page automatically refreshes to make sure the top threat and status information is current.
3. Click the **Download link**.
4. Under Outbreak Prevention Mode download settings do the following:
   - In the Download frequency list, choose how often Control Manager checks for updated Outbreak Prevention Policies.
   - In the Components to deploy list, choose a deployment plan to use to deploy downloaded components. For more information about deployment plans, see Understanding deploying updates.
   - To deploy the virus pattern file only, select the **Exclude Scan Engine Deployment** check box.
5. Click **Save**.

Stop Outbreak Prevention Mode

Manually stop Outbreak Prevention Mode before the policy duration has been exceeded.

When Control Manager is in Outbreak Prevention Mode, the icon appears on the management console.

To stop Outbreak Prevention Mode:

1. Click **Services** on the main menu.
2. On the left-hand menu under Services, click **Outbreak Prevention**.
3. Click **Stop Outbreak Prevention Mode**.
4. Click **OK**.

View Outbreak Prevention Mode History

This Outbreak Prevention Services feature allows you to view applied Outbreak Prevention Policies. The History screen shows the following information:

HEADING	DESCRIPTION
#	Indicates the order in which the tasks were performed; a lower the number indicates a newer task
Virus	The virus or malware that caused the outbreak
Started by	The User ID of the Control Manager user that applied the policy
Outbreak Prevention Mode Duration	Indicates how long Outbreak Prevention Mode was active. The starting time appears on the left, the completion (or abort) time is on the right.
Status	Indicates the results of the task. To view the result or status of a task, click View beside the task.

TABLE 9-4. History Screen Information

To view Outbreak Prevention Mode history:

1. Click **Services** on the main menu.
2. On the left-hand menu under Services, click **Outbreak Prevention > History**. To view the status of a specific Outbreak Prevention Policy, click **View** in the same row. The status window displays the number of viruses detected by your antivirus products.

Outbreak Prevention Mode Tutorial

Outbreak Prevention Mode Introduction

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

- What is the threat?– Identify the source of the virus outbreak
- What can my system do now?– Evaluate existing policies
- How do I protect my system?– Start Outbreak Prevention Mode
- What follow up procedures should I follow?

What is the Threat? - Identifying the Source of the Outbreak

Trend Micro provides registered customers with services that help identify the threats that threaten their systems. The following warn you of potential or emerging virus or malware outbreaks:

ALERT METHODS	DESCRIPTION
Scheduled Outbreak Prevention Policy downloads	Control Manager can inform you if it downloads Outbreak Prevention Policies that correspond to an ongoing virus outbreak. To receive notification about this event, enable Active Outbreak Prevention Policy received at the Event Center. Upon receiving the notification, start Outbreak Prevention Mode immediately.
TrendLabs Message Board	The Trend Micro TrendLabs Message Board provides the version numbers and the time TrendLabs releases the antivirus and content security components. This helps identify malware threats and provides update information about your Control Manager system.
Your Technical Account Manager (TAM)	Depending on the support arrangement you have with Trend Micro, your Technical Account Manager will inform you of any outbreak alerts. Upon receipt of the warning, update your outbreak prevention policies.
Trend Micro virus bulletins	You can subscribe to this service at the Trend Micro Web site.

TABLE 9-5. Identifying the Source of the Outbreak

ALERT METHODS	DESCRIPTION
Special Virus alert	This Control Manager feature, configured at the Event Center, warns you when a Trend Micro product detects an outbreak-causing virus on your network. This allows you to immediately take precautionary measures, such as warning your company's employees about certain kinds of email messages.

TABLE 9-5. Identifying the Source of the Outbreak

What Can My System Do Now? - Evaluating Existing Policies

Upon receiving a virus outbreak warning, you must assess if your system is equipped to deal with the threat. The Outbreak Prevention Services status screen displays the Outbreak Prevention Policies currently on your Control Manager server.

View the Outbreak Prevention status, and verify if existing Outbreak Prevention Policies cover the virus causing the outbreak.

Tip: Simplify this evaluation process by enabling Control Manager features that inform you about the availability of outbreak prevention policies that correspond to ongoing virus outbreaks.

For Outbreak Prevention Services alerts, see *Use Event Center* on page 7-9

For creating scheduled policy downloads, see*Update Outbreak Prevention Policies* on page 9-11

What best describes your Control Manager server's capabilities?

- The virus is covered by the Outbreak Prevention Policies currently on Control Manager
- The virus is not covered by the Outbreak Prevention Policies currently on Control Manager

Virus Covered by Existing Policies

Control Manager can handle the outbreak. Start Outbreak Prevention Mode and apply the Outbreak Prevention Policy that corresponds to the virus outbreak.

Virus Not Covered by Existing Policies

If existing Outbreak Prevention Policies do not cover the virus outbreak, you must obtain a new policy from Trend Micro.

Trend Micro recommends manually updating outdated Outbreak Prevention Policies.

How Do I Protect My System?

Start Outbreak Prevention Mode to apply the policy that corresponds to the virus outbreak. After Control Manager has entered Outbreak Prevention Mode, you can evaluate product-setting recommendations from Trend Micro and modify them to suit your network. Policies implement product settings that block known virus-entry points.

When TrendLabs deploys Outbreak Prevention Policy, it is very likely that they are still testing the appropriate virus pattern. The Outbreak Prevention Policy settings, therefore allow you to protect your network during the critical period before TrendLabs releases a new pattern.

Before you start Outbreak Prevention Mode, set outbreak recipients and the notification method in the Event Center.

To start outbreak prevention answer the following:

- **How long do you want this policy to be active?**

  Specify how long the policy will remain active at the Policy in effect for list. The duration starts from the time you start Outbreak Prevention Mode. By default, Outbreak Prevention Policies remain active for two days.

Note: If you edit the policy, Control Manager resets and starts the duration on the day you applied the changes.

- **How to deploy the policy?**

  Select an appropriate Deployment Plan for this stage. The plan determines which segments of the Product Directory will receive the settings contained in the policy.

Note: If none of the existing Deployment Plans suits your needs, create a new plan. See Creating Deployment Plans.

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

  The products involved in this stage are:

  - InterScan Messaging Security Suite
  - ScanMail for Microsoft Exchange
  - ScanMail for Lotus Notes
  - InterScan eManager
  - ScanMail eManager
  - InterScan WebProtect for ICAP
  - ServerProtect for Windows
  - OfficeScan Corporate Edition
  - Firewall Management - NetScreen
  - Network VirusWall 1200

  If settings for a particular product are included in the policy, then Control Manager automatically selects the product's check box.

Note: If any of the above products do not belong to your Control Manager network, Control Manager ignores the settings for those products.

To evaluate or modify any of the product settings:

1. Click the product's link to view its settings.
2. To view the settings for all the products, click **View Settings**.
3. Click **Show/Hide Suggestion** to view product setting recommendations from Trend Micro. The suggestions appear in non-editable fields on the right side of the screen.
4. Use the left fields to modify the settings to suit your needs.

What Follow-Up Procedures Should I Use?

After completing the Outbreak Prevention tutorial, monitor the progress of the policy using Outbreak Prevention Mode history.

Tip: Manually stop Outbreak Prevention Mode after the policy duration expires. Otherwise, the Outbreak Prevention Mode Scheduled Update feature cannot automatically apply new Outbreak Prevention Policies.

Using Vulnerability Assessment

Vulnerability Assessment provides system administrators or other network security personnel with the ability to assess security risks to their networks. The information they generate by using Vulnerability Assessment gives them a clear guide as to how to resolve known vulnerabilities and secure their networks.

Use Vulnerability Assessment to:

- Configure tasks that scan any or all computers attached to a network. Scans can search for single vulnerabilities or a list of all known vulnerabilities.
- Run manual assessment tasks or set tasks to run according to a schedule.
- Request blocking for computers that present an unacceptable level of risk to network security.
- Create reports that identify vulnerabilities according to individual computers and describe the security risks those computers present to the overall network. The reports identify the vulnerability according to standard naming conventions so that security personnel can do further research to resolve the vulnerabilities and secure the network.
- View assessment histories and compare reports to better understand the vulnerabilities and the changing risk factors to network security.

Clicking **Services** from the Control Manager screen, opens the Services menu and displays the products and services that are accessible from the Control Manager console. Vulnerability Assessment appears on this screen.

Click **Vulnerability Assessment** to open the Vulnerability Assessment screen. It gives an overview of the essential features of the product and quick access to the most common functions.

Possible Actions

To enable a scheduled pattern file download:

1. Click **Scheduled pattern file download**. The Scheduled Download screen appears displaying a list of all Control Manager scheduled component downloads.
2. To edit the scheduled download for the pattern or engine, click **Patterns/rules** and **Engines** to download all components under the groups, or click **Patterns/rules > Vulnerability Assessment Pattern**, **Pattern/rules > Vulnerability Information Database**, and **Engines > Vulnerability Assessment engine** for individual component download. This opens the group's or Component's Configuration screen, which is divided into three groups: Schedule and frequency, Download settings, and Automatic deployment.
3. Select **Enable scheduled download** check box to enable scheduled download for the pattern.
4. Click **Save**.

To download a component manually:

1. Click **Download Now**. The Manual Download screen opens displaying the download settings.
2. To edit the manual download for the pattern or engine, click **Patterns/rules** and **Engines** to download all components under the groups, or click **Patterns/rules > Vulnerability Assessment Pattern**, **Pattern/rules > Vulnerability Information Database**, and **Engines > Vulnerability Assessment engine** for individual component download. The Download Response screen opens. The progress bar shows the download status.
3. If the settings are acceptable, click **Download Now**. A message appears to inform you that you will download a component to your computer. Click **OK** to start download.
4. The Download Response screen opens. The progress bar shows the download status.
5. Click **OK** to return to the Manual Download screen.

To view tasks:

Click **view all the scheduled tasks**. The Tasks screen opens. You can create and run task from this screen.

To create a task:

Click **add a new task**. The Create a Vulnerability Assessment Task screen opens. You can create a new task from this screen.

To search for a machine:

- See *Search for a Machine* on page 9-43, for more information.

Available Details

Service Status

SERVICE STATUS	DESCRIPTION
Vulnerability assessment pattern file and Vulnerability assessment engine	These are the most current engine and pattern. Trend Micro recommends that you frequently download the most up to date engine and pattern file.
Schedule pattern download	Click this link to open a screen that displays a list of all Control Manager scheduled component downloads
Download Now	Click Download Now to start a manual download.
Tasks	Click the links to open the tasks screen or create a new task.

TABLE 9-6. Service Status Details

Most Recent Vulnerability Assessment Results

RESULTS	DESCRIPTION
Task Name	Identifies the task. Click the task name to view a history of the task.
Completion Date/Time	Displays the date and time for each completed task The date and time is sorted in descending order. The task information appears in this window from the most recent instance at the top to the instance that happened the longest time ago at the end. This field may also display In progress if a task is currently running. click In progress to view information about the current task.
Assessment Results	The number of machines that present a certain level of security risk to the network. To view additional details about the task that gave this result, click the respective number.
Enforcement	The number of machines for which Vulnerability Assessment has requested blocking.
Unsupported	The number of machines Vulnerability Assessment found to be using incompatible operating system versions. To view additional details about the task that reported these unsupported machines, click the respective number.
Pattern File	The pattern file number used to perform a task

TABLE 9-7. Vulnerability Result Details

Performing a Vulnerability Assessment

The objective of performing a Vulnerability Assessment is to create an overview of the security risks to a network and then use that overview as a guideline to resolve those threats. Performing regular assessments and routinely resolving all security risks provides a baseline security for the network. Administrators and users can feel confident that potential attackers will be unable to exploit vulnerabilities on their network.

Features and Benefits of Vulnerability Assessment

Vulnerability Assessment identifies security risks based on vulnerabilities it finds on any given computer. If a vulnerability exists on one computer, then it threatens the entire network to which that computer is attached. A vulnerability is defined as a defect in a computer's software that makes it prone to attacks by viruses and other malicious code. This includes defects that are due to unapplied security patches. Finding and resolving these vulnerabilities is the primary goal of Vulnerability Assessment.

Example: Internet Explorer 5.5 has a vulnerability MS01-020. This vulnerability exists because Internet Explorer doesn't correctly handle unusual MIME types. An attacker could create an email message and specify it was one of these MIME types. The NIMDA.A worm exploits this vulnerability. It spreads via an attachment embedded in an email. NIMDA can compromise network security and overwrite files in the system directory.

Four Main Stages of the Vulnerability Assessment Process

- Planning an assessment and configuring Vulnerability Assessment.
- Setting up, running tasks, and generating reports.
- Resolving vulnerabilities to provide a baseline security for the network.
- Maintaining a baseline security on your network.

Planning an Assessment and Configuring Vulnerability Assessment

What you need before you can perform a Vulnerability Assessment:

- Administrator or Root access privileges for Control Manager
- The activation code for Vulnerability Assessment
- The name or IP address of all the computers on your network that you want to include in your task. The name can be either the domain name for every computer or the individual computer name. You need to have access privileges to all the computers.

To perform a Vulnerability Assessment

1. Activate the product.
2. Download the latest Vulnerability Assessment engine and Vulnerability Assessment pattern file.

3. Use the Account Management Tool to enter the name of all the computers you want to include in your Assessment Tasks.

You are now ready to set up and run Vulnerability Assessment tasks and collect data about the vulnerabilities on your network.

Setting up, Running Tasks, and Generating Reports

The process of assessing the vulnerabilities is centered on the assessment task. System administrators or other network security professionals use tasks to protect their networks in the following ways:

- They create and run tasks. Tasks can include any or all the computers on the network. They can be set up to run manually or according to a schedule and they can search for single known vulnerabilities or a complete list of known vulnerabilities.
- The assessment tasks log the results and store them on the Control Manager server. Administrators can view these results immediately or make queries and generate reports at a later date. Reports give information about the tasks or about the security risks that individual computers present to the network. Based on these reports the administrator can take appropriate actions to resolve the vulnerabilities and secure the network.

Perform the following actions to manage your tasks:

1. Create tasks
2. Select machines to include in tasks
3. Edit tasks
4. Delete tasks
5. Run tasks

Resolving Vulnerabilities to Provide Baseline Security for the Network

When Vulnerability Assessment runs a task, it creates results that provide you with valuable information for resolving vulnerability-based security risks. You can view specific vulnerability risks according to individual computers from the Task Details, Result Summary or Machine Status screen.

The Results Summary and the Machine Status screen display the Vulnerability Name for each computer at risk. The name is linked to the Trend Micro Web site (see below). You can use this information to learn more about the vulnerability and how to eliminate it.

Click the link to open the Trend Micro Web site:

`http://www.trendmicro.com/advisory/`

Example: You run a task and the result is 3 critical security risks. You click on the number next to Critical in the Assessment Results table. The Task Detail screen opens. You see three computers and their associated critical vulnerabilities. All of them have the MS03-026 vulnerability, which is associated with the potential threat, WORM_NACHI.A. You click MS03-025 and your browser displays the Security Information from Trend Micro, which advises you to download and apply a patch. The Web site provides a link to the patch.

Maintaining Baseline Security on Your Network

Typically, you use Vulnerability Assessment to quickly identify the security risks to your network and eliminate the identified vulnerabilities. After this procedure, you have established a baseline security for the network. Now your major concern is how to maintain the baseline network security.

Use the following features to maintain a baseline security:

MEASURES	DESCRIPTION
Scheduled tasks	Create and run scheduled tasks to regularly check for new vulnerabilities.
Task histories	View task histories to discover new vulnerabilities as they occur and measure the progress of your countermeasures.
Queries and reports	Create custom queries and generate reports to better understand security risks on your network.

TABLE 9-8. Maintain Baseline Security

Activating Vulnerability Assessment

You can activate Vulnerability Assessment during Control Manager Installation. Alternatively, activation can be performed after Setup using the Web console.

To activate Vulnerability Assessment:

1. Click **Administration** on the main menu.
2. On the left-hand menu under Registration, click **License Information**.
3. On the working area under Vulnerability Assessment License Information, click the **Activate the product** link.
4. Do the following:
   - If you don't have an Activation Code: click the **Register online** link and follow the instructions on the Online Registration Web site to obtain an Activation Code
   - If you have an Activation Code: in the New box, type your Activation Code
5. Click **Activate**.

Downloading Updates

Trend Micro recommends that you always have the most up to date Vulnerability Assessment Pattern file and Vulnerability Assessment Engine when you set up and run assessment tasks. The Vulnerability Assessment Pattern file and the Vulnerability Assessment Engine serve essential functions when an assessment task is run.

- The Vulnerability Assessment Pattern file determines what vulnerabilities can be identified and what kind of information to display about those vulnerabilities.
- The Vulnerability Assessment Engine does the actual scanning of the machines that you set up in your assessment tasks.

You can download the Vulnerability Assessment Pattern file and Vulnerability Assessment Engine manually or have Vulnerability Assessment download them automatically according to a schedule. You configure the manual and scheduled downloads from the Administration menu on the Control Manager Web console.

To manually download components:

1. Access the Manual Download screen. You can do this in the following ways:
   - Click **Download Now** in the Services Summary screen

- Click **Download Now** in the Vulnerability Assessment screen
- From the Control Manager console, Click **Administration > Manual Downloads**

The Manual Download screen opens displaying the download settings.

2. To edit the manual download for the pattern or engine, click **Patterns/rules** and **Engines** to download all components under the groups, or click **Patterns/rules > Vulnerability Assessment Pattern**, **Pattern/rules > Vulnerability Information Database**, and **Engines > Vulnerability Assessment engine** for individual component download. This opens the Group's or Component's Configuration screen, which is divided into three groups: Schedule and frequency, Download settings, and Automatic deployment.
3. Click **Download Now**, if the settings are acceptable. A message appears to inform you that you will download a component to your computer.
4. Click **OK** to start download. The download response screen opens. The progress bar shows the download status. View details from the Command Details screen or tracking information from the Command Tracking screen.
5. Click **OK** to return to the Manual Download screen.

Configuring Vulnerability Assessment

You must configure Vulnerability Assessment before creating and running tasks. Use the Account Management Tool to view, add, modify, or delete login credentials for the target machines that you want to include in your assessments.

Before configuring Vulnerability Assessment, ensure that you have the following information:

- Domain name and machine name
- Administrator account name
- Appropriate passwords

Vulnerability Assessment requires you provide this information for all the computers on your network that you want to include in your Assessment Tasks.

Running a Vulnerability Assessment Task

After setting up and saving a task, you can run it manually or according to a schedule. Use the Tasks screen to run your tasks. Manually run a task at any time regardless of its predefined schedule. Scheduled tasks run according to the schedule that you set when you created them. Click Stop to interrupt a task when it is running. You can edit or delete a task.

When a task runs it scans all the machines included in your task for vulnerabilities. It logs the results of the scan and stores the results on the Control Manager server. You can view these results immediately or make queries and generate reports at a later date.

Vulnerability Assessment enables you to do the following:

- View Current Task
- Run a task now
- Run a scheduled task

View Current Task

At any time Vulnerability Assessment may be running a previously scheduled task or it may be running a manual task that requires time to complete. The Current Task screen displays information about these tasks. It also displays information about scheduled tasks that are waiting to run.

To see the updated status of the current Vulnerability Assessment task, click Refresh. This updates the data in window based on the results from the most recent task. This screen is also refreshed automatically every 2 minutes.

When a task is running you will see Stop at the top of the window. Click Stop to stop a current Vulnerability Assessment task, which is In progress. When a task is interrupted in this way, it updates the status of the machines that have already been assessed, but it cannot update the status of the machines that have not yet been assessed.

Task Status

The task status displays the results of the most recent assessment including information about the number and level of security risks to the network and the enforcement action taken. If there is a current task running, then it displays

information about the progress of that task. You can also view the following information about the current task status:

TASK STATUS	DESCRIPTION
Assessment result	This displays the results in progress of the assessment task. It gives the number and severity of the vulnerabilities of your network. The Total includes the machines for which the task was unable to deploy.
Enforcement result	This shows the number of machines which are blocked from the network.
Unsupported machines	This shows the number of machines which are not supported. Vulnerability Assessment cannot display any information about these machines. It redirects that users of these machines to a reassessment web page.
In progress	When a current task is running, this shows the amount of machines pending assessment.
Percentage complete	When a current task is running, this shows the percentage of the task that is complete.

TABLE 9-9. Current Task Status Information

Task Details

The Task Details shows information about the actual task, not the assessment information the task provides.:

TASK STATUS	DESCRIPTION
Task status	The status of the current Vulnerability Assessment task can be: • In progress: task is still running • Finishing: user stopped the task while it was in progress • Finished: task is complete
Task name	Displays the name of each completed task
Action	The action the task performs; Assessment only or Assessment with enforcement.
Schedule	Shows the selected schedule of a task; if a task is on hold, it will not run until the user manually starts it

TABLE 9-10. Current Task Status Information

TASK STATUS	DESCRIPTION
Issued by	The user who created the task; for example, the administrator
Vulnerability Assessment pattern file	The Vulnerability Assessment pattern file used to perform the task
Vulnerability Assessment engine	The Vulnerability Assessment engine used to perform the task

TABLE 9-10. Current Task Status Information

Current Queued Tasks

This table shows the names and the actions of the tasks that are scheduled to run in the future.

Run a Task Now

To run a task from the Task screen:

1. Click **Tasks** to open the Task screen.
2. Select the task you want to run.
3. Click **Run Now**. The Current Task screen displays to report the progress of the task.

To run a task from the Task History screen:

1. Click **History** to open the Task History screen.
2. Select the task to run from the Show task history of list and click **View ...**. The Task History screen appears.
3. Click **Run Now**. The Current Task screen displays to report the progress of the task.

Run a Scheduled Task

Scheduled tasks run automatically according to the schedule you set up when you created the task.

To run a task from the Task screen:

1. Click **Tasks** to open the Task screen.
2. Select the task to run.

3. Click **Run Now**. The Current Task screen displays to report the progress of the task.

To run a task from the Task History screen:

1. Click **History** to open the Task History screen.
2. Select the task to run from the Show task history of list and click **View ...**. The Task History screen appears.
3. Click **Run Now**. The Current Task screen displays to report the progress of the task.

Viewing Results

When a task runs, it scans all the machines included in your task for vulnerabilities. Vulnerability Assessment display results according to tasks or according to machines. You create and run tasks and Vulnerability Assessment records data based on the parameters that you set when you created them. The Control Manager server stores the results of the scan as task logs, which you can view according to their history and details, or according to individual computers in a results summary.

You can view these assessment results in a number of ways:

YOU CAN VIEW RESULTS ACCORDING TO...	FROM...
The most recent assessment task	• Current Task • Vulnerability Assessment
Any single assessment task	• Task History • Task Details
The number and level of security risks	Security Summary
Individual machines	• Results Summary • Machine Status • Custom Query Result

TABLE 9-11. View Assessment Results

Additionally, you can display the results of assessment tasks by using History to make log queries and generate customized and detailed reports that display the results any or all of your assessment tasks.

Understanding Results

What do the Results Mean?

After performing an assessment task, Vulnerability Assessment displays the results. It displays all results based on the risk level that individual computers present to the network. Risk levels are determined according to the number of vulnerabilities and the severity of the vulnerabilities on each computer. The Total field displays the number of machines for which the deploy failed.

What is a Vulnerability?

Vulnerabilities are defined as defects in a computer's software that makes them prone to attacks by viruses and other malicious code. This includes defects that are due to unapplied security patches.

Example: Internet Explorer 5.5 has a vulnerability MS01-020. This vulnerability exists because Internet Explorer doesn't correctly handle unusual MIME types. An attacker could create an email message and specify it was one of these MIME types. The NIMDA.A worm exploits this vulnerability. It spreads via an attachment embedded in an email. NIMDA can compromise network security and overwrite files in the system directory.

Note: For a complete listing of all the known vulnerabilities refer to the Trend Micro Web site at:

`www.trendmicro.com/advisory`

What is the Security Risk?

The security risk is an estimate of the risk that a machine attached to the network presents to the network. The number and severity of vulnerabilities that are located on the machine determines the overall security risk level.

Note: All vulnerabilities that are known to be exploited by malicious code are automatically promoted to critical risk level.

The following are descriptions of security risk levels:

RISK LEVEL	DESCRIPTION
Highly critical	The computers in this task have at least one vulnerability with a highly critical damage potential. Additionally, they may have other vulnerabilities that present lower risk levels. Example: The computer has the MS03-020 vulnerability which is exploited by WORM_KLEZ.H.
Critical	The computers in this task have at least one vulnerability with a critical damage potential. Additionally, they may have other vulnerabilities that present lower risk levels. They present an important risk level to network security.
Important	The computers in this task have at least one vulnerability with an important damage potential. Additionally, they may have other vulnerabilities that present lower risk levels.
Moderate	The computers in this task have at least one vulnerability with a moderate damage potential.
Risk free	These computers have no known vulnerabilities and present no risk to network security.
Deploy failed	This is the number of machines Vulnerability Assessment attempted to - but failed to - assess due to connection problems or incorrect login credentials. Refer to the Account Management Tool Tutorial for instructions about how to configure Vulnerability Assessment. Example: An administrator configures Vulnerability Assessment using the Account Management Tool, but fails to enter a password for a machine that he or she wants to include in the tasks. When you create and run a task that includes this machine, the task will give a result of Deploy failed for that machine.

TABLE 9-12. Security Risk Levels

Resolving Security Risks

When Vulnerability Assessment runs a task, it creates results that provide you with valuable information for resolving vulnerability-based security risks. You can view specific vulnerability risks according to individual computers from the Task Details, Result Summary or Machine Status screen.

The Results Summary and the Machine Status screens display the Vulnerability Name for each computer at risk. The name is linked to the Trend Micro Web site (see

below). You can use this information to learn more about the vulnerability and how to eliminate it.

Click the link to open the Trend Micro Web site:

`www.trendmicro.com/advisory`

Example: You run a task and the result is 3 critical security risks. You click on the number next to Critical in the Assessment Results table. The Task Detail screen opens. You see three computers and their associated critical vulnerabilities. All of them have the MS03-026 vulnerability which is associated with the potential threat, WORM_NACHI.A. You click MS03-025 and your browser displays the Security Information from Trend Micro which advises you to download and apply a patch. The Web site provides a link to the patch.

Maintaining Network Security

Typically, you use Vulnerability Assessment to quickly identify the security risks to your network and eliminate the identified vulnerabilities. After this procedure, you have established a baseline security for the network. Now your major concern is how to maintain the baseline network security.

Use the following features to maintain a baseline security:

ACTION	DESCRIPTION
Scheduled tasks	Create and run scheduled tasks to regularly check for new vulnerabilities.
Task histories	View task histories to discover new vulnerabilities as they occur and measure the progress of your countermeasures.
Queries and reports	Creating custom queries and generate reports. Better understand the nature of the security risks on your network.

TABLE 9-13. Maintain Baseline Security with Vulnerability Assessment

Understanding Enforcement

What is enforcement?

Enforcement means that a machine is quarantined from the network, or blocked. Blocked machines can only access a secure Web site where they can receive a reassessment. Based on the result of the assessment, machines which no longer present an unacceptable level of risk are released from quarantine and can reconnect to the network.

Vulnerability Assessment does not block or release computers itself, but is assisted by Network VirusWall. Network VirusWall queries Vulnerability Assessment on a regular basis and blocks and releases computers based on the query information. The frequency is configurable through Network VirusWall, but it can be as frequent as every 30 seconds (this is the default for computers that are not in compliance with Network VirusWall policies).

When does enforcement happen?

The system administrator sets the machines to which enforcement applies when he or she creates tasks. In each task, the administrator selects the machines to include and requests an enforcement action on machines that present an unacceptable level of risk to the network. Additionally, system administrators can access the Global Settings screen where they can set global enforcement policies. These policies can automatically perform enforcement against unsupported or deploy failed machines. Global exceptions, also set through the Global Settings screen, override any enforcement setting.

I set enforcement, but the machines are not blocked, why?

Enforcement actions depend on whether or not Vulnerability Assessment has access to Network VirusWall. Network VirusWall blocks all machines that are selected for enforcement by Vulnerability Assessment.

WARNING! *If you have set exceptions in Network VirusWall not to block certain computers, then it does not block those computers. Additionally, if Network VirusWall is not installed or if it is currently not functioning, it cannot block computers.*

What do these icons mean?

ICON	DESCRIPTION
	This machine is blocked and cannot access the network. To have the machine reconnect to the network, provide the URL for the Manual Assessment page. The machine can access this page where the user can initiate a manual vulnerability assessment after he or she has resolved the security risk. The default URL for the Manual Assessment page is: http://CM Server/ControlManager/cgi-bin/va/CGIvax.exe Where "CM Server" is the name of the name of the Control Manager Server where Vulnerability Assessment is installed.
	Vulnerability Assessment has marked this machine for blocking, but it has not been blocked yet. If you have installed Network VirusWall on your server, it will shortly block this machine. Network VirusWall queries Vulnerability Assessment on a regular basis. The frequency is configurable through Network VirusWall, but it can be as frequent as every 30 seconds (this is the default for computers that are not in compliance with Network VirusWall policies). It blocks and releases computers based on the query information. When viewing the results of a task, this icon appears briefly until the blocked icon replaces it when Network VirusWall blocks the machine. However, when you query the database, the flag icon is always displayed, showing the status of the machine immediately following the assessment task (not yet blocked).
	Vulnerability Assessment has assessed this machine. The computer is not blocked, based on the enforcement action you set. However, it could have vulnerabilities that present a significant risk to the network.
	This icon displays when you have manually released a machine, but it has not been released yet. When you manually release a machine you request Network VirusWall to stop blocking it. The next time that Network VirusWall queries Vulnerability Assessment, it will release the machine.

TABLE 9-14. Vulnerability Assessment Icons

Understanding Manual Assessment

There are two situations in which a computer must be manually assessed.

- A computer is Unsupported, Deploy failed or cannot be assessed by Vulnerability Assessment (Unassessed). The computer may or may not be blocked as a result of the vulnerabilities found by an assessment task. The system administrator

provides a URL to the user. The URL links to the Trend Micro Manual Vulnerability Assessment Tool. The user or the system administrator uses the Tool to manually assess the computer.

For more information, refer to *Using the Manual Vulnerability Assessment Tool* on page 9-40.

- A computer is blocked by Network VirusWall. When it attempts to communicate with the network, Network VirusWall displays a Web page in the computer's browser. The page explains how to resolve the vulnerability and manually assess the computer.

  For more information, refer to the *Using the Network VirusWall Manual Assessment Page* on page 9-41.

Using the Manual Vulnerability Assessment Tool

Trend Micro provides a Manual Vulnerability Assessment Tool for the following Microsoft Windows based machines:

- Windows ME/98/95
- Windows XP Home or Professional Edition
- Windows NT 4 Server/Workstation with Service Pack 6 or later
- Windows 2000 Professional/Server/Advanced Server with Service Pack 3 or later
- Windows 2003 Server Standard/Enterprise Edition

The system administrator can make this tool available to users who are using computers that have the Unsupported, Deploy failed or Unassessed status. Users can then manually assess their own machines.

To perform a manual assessment:

1. From the client machine you wish to cleanup, go to the following URL:

   `http://CM Server/ControlManager/cgi-bin/va/CGIvax.exe`

   Where "CM Server" is the name of the name of the Control Manager Server where Vulnerability Assessment is installed. The Trend Micro Manual Vulnerability Assessment page appears.

2. Click **Start Vulnerability Assessment** to run an Assessment Task on the local machine. The assessment progress bar appears displaying the name of the target machine and the status of the task. Click **Stop** to interrupt the task.

WARNING! *When you click **Start Vulnerability Assessment**, ActiveX controls deploy to your computer to perform the assessment. The Security Settings in your browser must be set to medium for Internet and Medium for local intranet to allow ActiveX controls to download (these are the default settings for Internet Explorer 6). Refer to Internet Explorer help for more information about setting your browser security level)*

When the task is complete, it displays the result of the Assessment Task and lists the names of the vulnerabilities it found.

Note: The Vulnerability Assessment task log is updated based on the manual Assessment Task. This log is stored on the Control Manager server. You can view the updated status by creating a custom query that includes the computer that was manually assessed.

Using the Network VirusWall Manual Assessment Page

When a user attempts to connect to the network using a blocked computer, Network VirusWall displays a Web page in the user's browser to announce the blockage. It identifies the vulnerabilities that have resulted in the block and instructs the user to click a link to get redirected to a secure page for downloading a security patch or performing an action to resolve the vulnerability.

When a user resolves the vulnerability and manually assesses his or her computer, Vulnerability Assessment updates the assessment results for that computer. The next time that Network VirusWall queries Vulnerability Assessment, it will find no reason to continue blocking the computer and so release it.

To perform a manual assessment:

1. Click the link to obtain a security patch or learn about how to resolve the vulnerability.

2. When you have resolved the vulnerability, return to the manual assessment page and click **Start reassessment**. The status bar appears showing you the progress of the reassessment.

   When the assessment is complete, the OK button appears.

WARNING! *When you click Start reassessment, ActiveX controls deploy to your computer to perform the reassessment. The Security Settings in your browser must be set to medium for Internet and Medium for local intranet to allow ActiveX controls to download (these are the default settings for Internet Explorer 6). Refer to Internet Explorer help for more information about setting your browser security level).*

   Click **Stop** to interrupt the assessment. The data from the current assessment will be discarded.

3. Click **OK** to close the Web page.

View Security Summary

Clicking Security Summary opens the Security Summary screen, which gives an overview of the security risks for your network. It displays results of all of the tasks for all of the machines. You can also use the Search for Machine to find a specific machine or vulnerability.

You can view details about the following:

- Assessment Result
- Enforcement Status
- Additional Information

Assessment Result

This table displays results from all of the assessment tasks for all of the machines on your network. The results are displayed according to the security risk they present to the network.

- **Machine Count:** The number of machines that present a certain level of risk.
- **Percentage:** The percent of machines that present a certain level of risk. A high percentage warns that there is a significant risk.

Click the underlined numbers to view more detailed information about the security risks.

Enforcement Status

This table displays enforcement status information. click the underlined number to learn more about blocked computers or computer for which Vulnerability Assessment has requested blocking.

Additional Information

Click the links in this table to display more detailed information about your Top 10 vulnerabilities and unsupported machines. The Top 10 Vulnerabilities are the most frequent vulnerabilities on your network.

Search for a Machine

You can use the search feature from the Security Summary screen to search for machines according to:

- Individual machines
- Number of machines that have a single vulnerability
- Number of machines that have a number of vulnerabilities.

To search for a machine:

1. Type your query in the space provided.
   - **IP address:** Type the IP address of the computer you want to find in the space provided. Use the tab key to navigate the fields.
   - **Machine name:** Type a single name to find one particular computer or a number of names to find a list of computers.

- **Vulnerability name:** Type the name or a list of names of known vulnerabilities in the space provided.

2. Click **Search**.

Select Machines

Use this section to select the machines Vulnerability Assessment scans during an Assessment Task. Select machines by machine name or IP address. The default setting is by machine name. Before proceeding with machine selection, the login credentials for these machines should be added in the Account Management Tool first. See *Account Management Tool Tutorial* on page 9-74.

Note: This section will not display correctly, unless the browser's privacy level is set to Medium.

There are two ways to add machines to a task: by machine name or by IP address. Choose one method and follow the directions below. If you change the method you are using to input machines, a message appears informing you that your current selections will be discarded. To discard your selections, click OK. To keep these selections, click Cancel. You return to Select Machines.

To select machines by name

1. Click **By machine name**.
2. Select a specific machine, and/or domain (all machines under the selected domain will be selected too) in the left hand tree. To select multiple machines and/or domains, push the shift and control keys while selecting. To view the machines which are part of a domain, click the desired domain.
3. Click **Add>** to add a machine or a domain. Alternatively, click **Add All >>** to add all machines and domains in the right hand tree. After adding the machines and domains they will appear in the right hand tree.
4. Click **Save** to save these selections and return to Create a Vulnerability Assessment Task. Click **Cancel** to discard the changes and return to Create a Vulnerability Assessment Task.

To remove machines by machine name

1. Select a specific machine or a domain in the right hand tree (all machines under the selected domain will be selected too). To select multiple machines and/or

domains, push the shift and control keys while selecting. To view the machines which are part of a domain, click the domain.

2. Click **<Remove** to remove a machine or domain. Alternatively, click **<< Remove All** to remove all visible machines and domains. After removing the machines or domains, they will appear in the right hand tree.
3. Click **Save** to save these selections and return to Create a Vulnerability Assessment Task. Click **Cancel** to discard the changes and return to Create a Vulnerability Assessment Task.

To select machines by IP address

1. Click **By IP address**.
2. Type the first IP address in **IP address:**. It is important that all target machines that are part of the specified range have the same login credentials. Press **Delete** to modify a value or Tab to type the next value. Valid addresses follow the following format: xxx xxx xxx xxx, for example: 192.168.1.12
3. Click > next to IP address : to add the IP address to the list. The IP address appears in the right-hand box.
4. Click **Save** to save these selections and return to Create a Vulnerability Assessment Task. Click **Cancel** to discard the changes and return to Create a Vulnerability Assessment Task.

To select machines by range of IP addresses

1. Click **By IP address**.
2. Type the first IP address in **IP address from:**. It is important that all target machines part of the specified range have the same login credentials. Press **Delete** to modify a value or Tab to type the next value. Valid addresses follow the following format: xxx xxx xxx xxx For example: 192.168.1.12
3. Type a subnet value in **IP address to:** (the subnet value is the last set of numbers in an IP address). The subnet value of the first IP address should be inferior than the corresponding value of the last IP address. The valid subnet values are 1 through 255. Press the **Delete** to modify a value.
4. Click > next to **IP address from:** and **IP address to:** to add the range specified above. After adding a range, the first and last IP addresses will appear in the right hand box.

5. Click **Save** to save these selections and return to Create a Vulnerability Assessment Task. Click **Cancel** to discard the changes and return to Create a Vulnerability Assessment Task.

Create a Task

You create tasks using three steps. First you select machines that you want to include in the task, next you set the schedule for the task and then you select the enforcement actions that you want the task to perform. After you create a regular task you can save it and run it manually. Vulnerability Assessment displays all saved tasks in the Vulnerability Assessment Tasks screen.

Note: Tasks provide central reporting back to the Control Manager server

---

To create a task:

1. Click **Tasks** to open Vulnerability Assessment Tasks and then click **Add a New Task ...**. Alternatively, click the **add a new task** link from Vulnerability Assessment. Create a Vulnerability Assessment Task appears.
2. Type the name of the task in the **Name** field. Valid names are alphanumeric and can be up to 48 characters long. For example, iT#3-01-03-2004-mP.
3. In **Step 1 of 3**, click **Select Machines** to select the target machines for this task. After machine selection, the target machines will appear under Selected Machines.

   There are three ways to add machines to a task: by machine name, by IP address and by IP address range. Choose one method and follow the directions below.

   If you change the method you are using to input machines, a message appears informing you that your current selections will be discarded. To discard your selections, click OK. To keep these selections, click Cancel. You return to Select Machines.

   To add machines by name:

   a. Click **By machine name**.

   b. Select a specific machine, and/or domain (all machines under the selected domain will be selected too) in the left hand tree. To select multiple machines and/or domains, push the shift and control keys while selecting. To view the machines which are part of a domain, click the desired domain.

c. Click **Add>** to add a machine or a domain. Alternatively, click **Add All >>** to add all machines and domains in the right hand tree. After adding the machines and domains they will appear in the right hand tree.

d. Click **Save** to save these selections and return to Create a Vulnerability Assessment Task. Click **Cancel** to discard the changes and return to Create a Vulnerability Assessment Task.

To add machines by IP address:

a. Click **By IP address**.

b. Type the first IP address in **IP address:**. It is important that all target machines that are part of the specified range have the same login credentials. Press **Delete** to modify a value or Tab to type the next value. Valid addresses follow the following format: xxx.xxx.xxx.xxx, for example: 192.168.1.12

c. Click > next to **IP address:**, to add the IP address to the list. The IP address appears in the right hand box.

d. Click **Save** to save these selections and return to Create a Vulnerability Assessment Task. Click **Cancel** to discard the changes and return to Create a Vulnerability Assessment Task.

To specify a range of IP addresses:

a. Click **By IP address**.

b. Type the first IP address in **IP address from:**. It is important that all target machines part of the specified range have the same login credentials. Press **Delete** to modify a value or Tab to type the next value. Valid addresses follow the following format: xxx.xxx.xxx.xxx For example: 192.168.1.12

c. Type a subnet value in **IP address to:** (the subnet value is the last set of numbers in an IP address). The subnet value of the first IP address should be inferior than the corresponding value of the last IP address. The valid subnet values are 1 through 255. Press the Delete button to modify a value.

d. Click > next to **IP address:** and **To IP address:** to add the range specified above. After adding a range, the first and last IP addresses will appear in the right-hand box.

e. Click **Save** to save these selections and return to Create a Vulnerability Assessment Task. Click **Cancel** to discard the changes and return to Create a Vulnerability Assessment Task.

4. **Step 2 of 3** is for Creating Scheduled Task. Ignore this step if you are creating a regular task.

   a. Select one of the following schedules:

   - **One time on month - day - year:** Select this option to specify one exact date when a task runs.

     Select a month, day, and year from each drop down menu.

     Example: Selecting January 01 2003 runs the task once each January 01, 2003.

   - **Every day:** Select this option to run a task every day.
   - **Every number of weeks on day of week:** Select this option to specify a regular interval on which to run a task.

     Select the number of weeks (1 through 4)

     Select the day of the week (Sunday through Saturday)

     Example: Selecting 2 weeks and Sunday runs the task once every 2 weeks on Sunday.

   - **Every month on day of month:** Select this option to run a task once on a specific day of each month.

     Select the day of the month (first through last) from the drop down menu.

     Example: Selecting 12th day of the month runs the task on the 12th day of each and every month.

   - **On hold:** Select this option to create a regular task without specifying when it will run; when selecting this option, the task will only run if the user clicks **Run Now** in Tasks.

   b. Select a time

   Select the starting time for the task from the two drop down menus. The first drop down menu shows the hours (hh). The second drop down menu displays the minutes (mm).

   Enter the time according to the 24 hour clock.

Example: To set a time for 11:34 P.M., select 23 in the hours drop down menu, and 34 in the minutes drop down menu.

5. Complete **Step 3 of 3** to set the actions the task will perform.

   Select one of two actions for the task to perform:

   - **Assessment by all vulnerability names**

     The task scans for all the known vulnerabilities in the current Vulnerability Assessment pattern file.

     For a complete listing of all the known vulnerabilities refer to the Trend Micro Web site at http://www.trendmicro.com/advisory/.

     When you select this action you can also request enforcement on machines according to the risk they present to the network. Select Enable enforcement on machines that are and then select a security risk level to set an enforcement for this task. The task applies enforcement policies to all machines that present vulnerabilities of the identified risk level.

   - **Assess by the selected vulnerability name(s) only**

     The task scans for only those vulnerabilities that you identify in the list. To include a vulnerability in the list, type the vulnerability name in the box. Click > to add vulnerability names to the task list and **Remove** to remove names from the list.

     When you select this action you can also request enforcement on machines according to the vulnerability names. Select **Enable enforcement on machines with any of the selected vulnerability name(s)**. The task will apply enforcement policies to all machines that contain the vulnerabilities identified in the scan.

     Regardless of the action option that you choose, you can also select **Enable Damage Cleanup Services for this task with ...**. When you select this option, the Vulnerability Assessment task that you create runs at the same time as a Damage Cleanup Services task. An icon appears next to the task to indicate that Damage Cleanup Services is now enabled. However, if at a later time you decide to stop sharing the task, then both tasks can no longer run at the same time. When this situation exists, one task is queued to immediately follow the other task.

   You can select to enable Damage Cleanup Services for tasks that perform the following actions:

- **Assessment only:** the shared task performs both a Vulnerability Assessment and a Damage Cleanup Services assessment. It does not perform any cleanup functions.
- **Cleanup:** the shared task performs a Vulnerability Assessment and a Damage Cleanup Services assessment. It also performs cleanup services on any damage it finds on the machines.

Note: Refer to the *Damage Cleanup Services 3 Administrator's Guide* for more information about the Damage Cleanup Services assessment and cleanup functions.

---

6. Click **Save** to save the task and run it at some later time. Click **Cancel** to close the screen without saving the task.

Edit a Task

To edit a task:

1. Click **Tasks** to open Vulnerability Assessment Tasks. Select a task and click **Edit ....**
2. Type the name of the task in the **Name** field. Valid names are alphanumeric and can be up to 48 characters long. For example, iT#3-01-03-2004-mP.
3. In **Step 1 of 3**, click **Select Machines** to select the target machines for this task. After machine selection, the target machines will appear under Selected Machines.

   There are three ways to add machines to a task: by machine name, by IP address and by IP address range. Choose one method and follow the directions below.

   If you change the method you are using to input machines, a message appears informing you that your current selections will be discarded. To discard your selections, click OK. To keep these selections, click Cancel. You return to Select Machines.

   To add machines by name:

   a. Click **By machine name**.

   b. Select a specific machine, and/or domain (all machines under the selected domain will be selected too) in the left hand tree. To select multiple machines and/or domains, push the shift and control keys while selecting. To view the machines which are part of a domain, click the desired domain.

c. Click **Add>** to add a machine or a domain. Alternatively, click **Add All >>** to add all machines and domains in the right hand tree. After adding the machines and domains they will appear in the right hand tree.

d. Click **Save** to save these selections and return to Create a Vulnerability Assessment Task. Click **Cancel** to discard the changes and return to Create a Vulnerability Assessment Task.

To add machines by IP address:

a. Click **By IP address**.

b. Type the first IP address in **IP address:**. It is important that all target machines that are part of the specified range have the same login credentials. Press **Delete** to modify a value or Tab to type the next value. Valid addresses follow the following format: xxx.xxx.xxx.xxx, for example: 192.168.1.12

c. Click > next to **IP address:**, to add the IP address to the list. The IP address appears in the right hand box.

d. Click **Save** to save these selections and return to Create a Vulnerability Assessment Task. Click **Cancel** to discard the changes and return to Create a Vulnerability Assessment Task.

To specify a range of IP addresses:

a. Click **By IP address**.

b. Type the first IP address in **IP address from:**. It is important that all target machines part of the specified range have the same login credentials. Press **Delete** to modify a value or Tab to type the next value. Valid addresses follow the following format: xxx.xxx.xxx.xxx For example: 192.168.1.12

c. Type a subnet value in **IP address to:** (the subnet value is the last set of numbers in an IP address). The subnet value of the first IP address should be inferior than the corresponding value of the last IP address. The valid subnet values are 1 through 255. Press the Delete button to modify a value.

d. Click > next to **IP address:** and **To IP address:** to add the range specified above. After adding a range, the first and last IP addresses will appear in the right-hand box.

e. Click **Save** to save these selections and return to Create a Vulnerability Assessment Task. Click **Cancel** to discard the changes and return to Create a Vulnerability Assessment Task.

4. **Step 2 of 3** is for Creating Scheduled Task. Ignore this step if you are editing a regular task.

   a. Select one of the following schedules:

   - **One time on month - day - year:** select this option to specify one exact date when a task runs

     Select a month, day, and year from each drop down menu.

     Example: Selecting January 01 2003 runs the task once each January 01, 2003.

   - **Every day:** select this option to run a task every day
   - **Every number of weeks on day of week:** select this option to specify a regular interval on which to run a task.

     Select the number of weeks (1 through 4)

     Select the day of the week (Sunday through Saturday)

     Example: Selecting 2 weeks and Sunday runs the task once every 2 weeks on Sunday.

   - **Every month on day of month:** select this option to run a task once on a specific day of each month.

     Select the day of the month (first through last) from the drop down menu.

     Example: Selecting 12th day of the month runs the task on the 12th day of each and every month.

   - **On hold:** select this option to create a regular task without specifying when it will run; when selecting this option, the task will only run if the user clicks **Run Now** in Tasks.

   b. Select a time

   Select the starting time for the task from the two drop down menus. The first drop down menu shows the hours (hh). The second drop down menu displays the minutes (mm).

   Enter the time according to the 24 hour clock.

Example: To set a time for 11:34 P.M., select 23 in the hours drop down menu, and 34 in the minutes drop down menu.

5. Complete **Step 3 of 3** to edit the actions the task will perform.

   Select one of two actions for the task to perform:

   - **Assessment by all vulnerability names**

     The task scans for all the known vulnerabilities in the current Vulnerability Assessment pattern file.

     For a complete listing of all the known vulnerabilities refer to the Trend Micro Web site at http://www.trendmicro.com/advisory/.

     When you select this action you can also request enforcement on machines according to the risk they present to the network. Select Enable enforcement on machines that are and then select a security risk level to set an enforcement for this task. The task applies enforcement policies to all machines that present vulnerabilities of the identified risk level.

   - **Assess by the selected vulnerability name(s) only**

     The task scans for only those vulnerabilities that you identify in the list. To include a vulnerability in the list, type the vulnerability name in the box. Click > to add vulnerability names to the task list and **Remove** to remove names from the list.

     When you select this action you can also request enforcement on machines according to the vulnerability names. Select **Enable enforcement on machines with any of the selected vulnerability name(s)**. The task will apply enforcement policies to all machines that contain the vulnerabilities identified in the scan.

     Regardless of the action option that you choose, you can also select **Enable Damage Cleanup Services for this task with ...**. When you select this option, the Vulnerability Assessment task that you create runs at the same time as a Damage Cleanup Services task. An icon appears next to the task to indicate that Damage Cleanup Services is now enabled. However, if at a later time you decide to stop sharing the task, then both tasks can no longer run at the same time. When this situation exists, one task is queued to immediately follow the other task.

You can select to enable Damage Cleanup Services for tasks that perform the following actions:

- **Assessment only:** the shared task performs both a Vulnerability Assessment and a Damage Cleanup Services assessment. It does not perform any cleanup functions.
- **Cleanup:** the shared task performs a Vulnerability Assessment and a Damage Cleanup Services assessment. It also performs cleanup services on any damage it finds on the machines.

Note: Refer to the *Damage Cleanup Services 3 Administrator's Guide* for more information about the Damage Cleanup Services assessment and cleanup functions.

---

6. Click **Save** to save the task and run it at some later time. Click **Cancel** to close the screen without saving the task.

Delete a Task

To delete a task:

1. Open the **Tasks** screen and select a task.
2. Click **Delete**. A confirmation message appears.
3. Click **OK** to confirm the delete action and proceed to Delete a Task. Click **Cancel** to cancel the delete action and return to Vulnerability Assessment Tasks.
4. Click **OK** on the Delete a Task screen to return to Vulnerability Assessment Tasks.

Note: You cannot delete a running task.

Set Task Actions

When you create a task you choose one of the following actions.

- **Assessment by all vulnerability names**

  The task scans for all the known vulnerabilities in the current Vulnerability Assessment pattern file.

For a complete listing of all the known vulnerabilities refer to the Trend Micro Web site at http://www.trendmicro.com/advisory/.

When you select this action you can also request enforcement on machines according to the risk they present to the network. Select Enable enforcement on machines that are and then select a security risk level to set an enforcement for this task. The task applies enforcement policies to all machines that present vulnerabilities of the identified risk level.

- **Assess by the selected vulnerability name(s) only**

  The task scans for only those vulnerabilities that you identify in the list. To include a vulnerability in the list, type the vulnerability name in the box. Click > to add vulnerability names to the task list and **Remove** to remove names from the list.

  When you select this action you can also request enforcement on machines according to the vulnerability names. Select **Enable enforcement on machines with any of the selected vulnerability name(s)**. The task will apply enforcement policies to all machines that contain the vulnerabilities identified in the scan.

  Regardless of the action option that you choose, you can also select **Enable Damage Cleanup Services for this task with ...**. When you select this option, the Vulnerability Assessment task that you create runs at the same time as a Damage Cleanup Services task. An icon appears next to the task to indicate that Damage Cleanup Services is now enabled. However, if at a later time you decide to stop sharing the task, then both tasks can no longer run at the same time. When this situation exists, one task is queued to immediately follow the other task.

You can select to enable Damage Cleanup Services for tasks that perform the following actions:

- **Assessment only:** The shared task performs both a Vulnerability Assessment and a Damage Cleanup Services assessment. It does not perform any cleanup functions.
- **Cleanup:** The shared task performs a Vulnerability Assessment and a Damage Cleanup Services assessment. It also performs cleanup services on any damage it finds on the machines.

Note: Refer to the *Damage Cleanup Services 3 Administrator's Guide* for more information about the Damage Cleanup Services assessment and cleanup functions.

Enable Damage Cleanup Services for a Vulnerability Assessment Task

Vulnerability Assessment and Damage Cleanup Services offer two complementary services accessible from the Control Manager console that can greatly increase network security.

- Vulnerability Assessment provides you with the ability to assess security risks to your network. You can use it to set up and run tasks that report on the security risks. You can use the reports to resolve the vulnerabilities and remove the security risks to your network.
- Damage Cleanup Services offers the ability to assess damages due to malware attacks and cleanup the damages done by the attacks, including cleaning virus remnants that persist after the virus has been removed.

Use Both Separately

Vulnerability Assessment and Damage Cleanup Services are both available from the Control Manager console. You can use them both separately to perform two complementary tasks: one to assess damages done by malware and then cleanup the damage and one to assess vulnerabilities and remove them or enforce security measures against the offending machines.

Enable Damage Cleanup Services for a Vulnerability Assessment Task

Alternatively, you can use both services together. From the Create a Vulnerability Assessment task screen select **Enable Damage Cleanup Services for this task with ...** to set this task. An icon appears next to the task to indicate that Damage Cleanup Services is now enabled. When you run this task, the Vulnerability Assessment task runs at the same time as a Damage Cleanup Services task.

Note: If, at a later time, you decide to disable Damage Cleanup services, then both tasks can no longer run at the same time. When this situation exists, one task is queued to immediately follow the other task.

To enable Damage Cleanup Services for a Vulnerability Assessment task:

1. Use Vulnerability Assessment to create a task.
2. Ensure that you select **Enable Damage Cleanup Services for this task with ...** and save the task.
3. Use Vulnerability Assessment to run the task.

Note: Refer to the *Damage Cleanup Services 3 Administrator's Guide* for more information about the Damage Cleanup Services assessment and cleanup functions.

Set Global Enforcements and Exceptions

You can access the Global Settings screen to set global enforcement and exception policies. You can set enforcement policies that automatically apply to Unsupported, Deploy failed or Unassessed machines. When a task has an action set that conflicts with the global enforcement action, the global enforcement action overrides the action. Exceptions can be set according to machine name, IP address or IP address range. The exceptions override all other settings - even global enforcement settings.

Note: Unassessed machines are not excluded from enforcement.

Example: Using the Account Management Tool, you configure a computer by the name of "Boss1". The IP address for this computer is 130.140.150.123, but you do not know the password. Later, you create an Assessment Task that scans machines in the IP range from 130.140.150.120 to 130.140.150.130 (which included "Boss1") and blocks all Deploy failed machines. If you run this task you would discover that "Boss1" is Deploy failed, therefore, blocked. However, if you do not want to block this machine you could set a global exception for "Boss1". When the global exception is set, and the task is run, "Boss1" is not blocked (even though it is Deploy failed). All other Deploy failed machines remain blocked.

You can also use this screen to configure actions for machines that use the Manual Vulnerability Assessment Tool. Machines must use the tool when they are Unsupported or Deploy failed and Vulnerability Assessment cannot assess them. In these cases, the system administrator provides a URL to the user which links to the Trend Micro Manual Vulnerability Assessment Tool. The user or the system administrator can use the tool to manually assess the computer.

For more information, refer to *Account Management Tool Tutorial* on page 9-74.

To set Auto Enforcement Settings

1. Select one or all of the following:
   - **Deploy failed machines** - Vulnerability Assessment automatically requests blocking against **Deploy failed** machines
   - **Unsupported machines** - Vulnerability Assessment automatically requests blocking against unsupported machines
   - **Unassessed machines** - Vulnerability Assessment automatically requests blocking against machines that have never before been assessed.

To set Exceptions

1. Select **Exclude the following machines during enforcement** from the Exception list table.
2. Add machines by name, IP address or IP address range:

   By name:

   a. Type the machine name to add next to Machine name

   b. Click > to add the machine to the list of machines. Vulnerability Assessment does not apply any enforcement action against the machines on this list.

   By IP address:

   a. Type the IP address. Each box contains three numbers in the IP address. Click the appropriate field or use the Tab key to move through the fields. Valid addresses follow the following format: xxx.xxx.xxx.xxx, for example: 192.168.1.12

   b. Click to add the machine to the list of machines. Vulnerability Assessment does not apply any enforcement action against the machines on this list.

By IP address range:

a. Type the first IP address in the address range in **IP Address From:**. Click the appropriate field or use the tab key to move through the fields. Valid addresses follow the following format: xxx.xxx.xxx.xxx, for example: 192.168.1.12

b. Type the last IP address in the address range in **IP Address To:**. The subnet value of the first IP address must be a lower value than the corresponding value of the last IP address. The valid subnet values are 1 through 255. Press the **Delete** to modify a value.

c. Click > next to **IP Address From:** and **IP Address To:**. to add the range specified to the list. After adding a range, the first and last IP addresses will appear in the right hand box. Vulnerability Assessment does not apply any enforcement action against the machines on this list.

3. Click **Save** to save your exceptions.

To configure actions for machines that use the Manual Vulnerability Assessment Tool:

- **Assessment by all vulnerability names**

  The task scans for all the known vulnerabilities in the current Vulnerability Assessment pattern file.

  For a complete listing of all the known vulnerabilities refer to the Trend Micro Web site at http://www.trendmicro.com/advisory/.

  When you select this action you can also request enforcement on machines according to the risk they present to the network. Select Enable enforcement on machines that are and then select a security risk level to set an enforcement for this task. The task applies enforcement policies to all machines that present vulnerabilities of the identified risk level.

- **Assess by the selected vulnerability name(s) only**

  The task scans for only those vulnerabilities that you identify in the list. To include a vulnerability in the list, type the vulnerability name in the box. Click > to add vulnerability names to the task list and **Remove** to remove names from the list.

  When you select this action you can also request enforcement on machines according to the vulnerability names. Select **Enable enforcement on machines with any of the selected vulnerability name(s)**. The task will apply

enforcement policies to all machines that contain the vulnerabilities identified in the scan.

Regardless of the action option that you choose, you can also select **Enable Damage Cleanup Services for this task with ...**. When you select this option, the Vulnerability Assessment task that you create runs at the same time as a Damage Cleanup Services task. An icon appears next to the task to indicate that Damage Cleanup Services is now enabled. However, if at a later time you decide to stop sharing the task, then both tasks can no longer run at the same time. When this situation exists, one task is queued to immediately follow the other task.

View Tasks

The Tasks screen displays all the tasks that you created and saved. You can use this screen to create and manage your tasks.

View information about the following topics:

INFORMATION SOURCES	DESCRIPTION
Task Name	The names of all the tasks that you created and saved.
Action	The action that a task performs. This can be Assessment or Assessment with enforcement or both.
Schedule	The schedule on which the task runs. When you choose Run Now, you override the schedule for the task.
On hold	If a task is on hold, it will not run until the user manually starts it.
Last Completed	The last date and time on which the task ran.

TABLE 9-15. Task Screen Information

Select a task and choose one of the following options:

TASKS	DESCRIPTION
Edit	Click to edit a task.

TABLE 9-16. Task Screen Tasks

TASKS	DESCRIPTION
Delete	Click to delete a task.
Run Now	Click to run a task immediately, regardless of its schedule. Running a task makes it the current task.

TABLE 9-16. Task Screen Tasks

View a Current Task

At any time Vulnerability Assessment may be running a previously scheduled task or it may be running a manual task that requires time to complete. The Current Task screen displays information about these tasks. It also displays information about scheduled tasks that are waiting to run.

To see the updated status of the current Vulnerability Assessment task, click **Refresh**. This updates the data in window based on the results from the most recent task. This screen is also refreshed automatically every 2 minutes.

When a task is running you will see Stop at the top of the window. Click **Stop** to stop a current Vulnerability Assessment task, which is In progress. When a task is interrupted in this way, it updates the status of the machines that have already been assessed, but it cannot update the status of the machines that have not yet been assessed.

The Current Queued Tasks shows the names and the actions of the tasks that are scheduled to run in the future.

View Task Status Details

The task status displays the results of the most recent assessment including information about the number and level of security risks to the network and the enforcement action taken. If there is a current task running, then it displays

information about the progress of that task. You can also view the following information about the current task status:

STATUS DETAILS	DESCRIPTION
Assessment result	This displays the results in progress of the assessment task. It gives the number and severity of the vulnerabilities of your network. The total includes the machines for which the task failed to deploy.
Enforcement result	This shows the number of machines which are blocked from the network.
Unsupported machines	This shows the number of machines which are not supported. Vulnerability Assessment cannot display any information about these machines.
In progress	When a current task is running, this shows the amount of machines pending assessment.
Percentage complete	When a current task is running, this shows the percentage of the task that is complete.

TABLE 9-17. Task Status Details

View Task Details information

The Task Details shows information about the actual task, not the assessment information the task provides.

TASK DETAILS	DESCRIPTION
Task status	The status of the current Vulnerability Assessment task can be: • **In progress:** Task is still running • **Finishing:** User stopped the task while it was in progress • **Finished:** Task is complete
Task name	Displays the name of each completed task
Action	The action the task performs; Assessment only or Assessment with enforcement
Schedule	Shows the selected schedule of a task; If a task is on hold, it will not run until the user manually starts it

TABLE 9-18. Task Details Screen

TASK DETAILS	DESCRIPTION
Issued by	The user who created the task; for example, the administrator
Vulnerability Assessment Pattern File	The Vulnerability Assessment pattern used to perform the task
Vulnerability Assessment Engine	The Vulnerability Assessment engine used to perform the task

TABLE 9-18. Task Details Screen

Use the Vulnerability Assessment History

Administrators can use the History page to generate and save reports. Reports are based on customized queries. The queries gather data from the logs that Vulnerability Assessment has generated when it performed Assessment Tasks. Assessment reports give administrators the ability to better understand assessment tasks and the changing risk factors to network security.

The Vulnerability Assessment History provides the following capabilities:

Create Log Queries Based on Task History

Query results show a history of when a task was performed and the changes to security risks from one task to the next. This provides a useful progress report on whether known vulnerabilities are being reduced.

Create Customized Log Queries

Queries can include many variables such as Task Date, Status, Machine name and Vulnerability name. You can export the query result to a comma-separated values file format.

Generate Comparative Reports

You can select two occurrences of one task to compare in a single report. The query result displays comparative information based on logs and individual machines. You can export the result to a comma-separated values file format.

View Task History

You can view the history of a single task from the Task History screen. The Task History lists all the times a task ran since it was created. For each instance of the task, it displays information about the number and type of security risks that the task identified. It also shows information about the number of machines that are subject to enforcement policies or unsupported.

Viewing the information combined in the Task History and Task Detail screens enables you to quickly resolve vulnerability risks. First, you can use the Task History to see if there are any new security risks appearing on your network. Next, you can click a particular security risk to see which specific machines are presenting that risk. Finally, you can click a machine name to read detailed information about the vulnerabilities on each machine to learn how to resolve the vulnerability.

Tip: If a mobile machine temporarily attaches to your network you can see it in the Task History.

Choose **Run Now** to run the task immediately instead of according to its schedule. When you choose **Run Now**, the Current Tasks screen appears and displays information about the task you selected.

Navigating Through the Screens

- Click **Back** to close the screen and return to the previous screen
- The number of machines available for viewing is shown in the upper right hand corner, for example 1 - 20 of 48 indicates you are viewing the first 20 logs of a total of 48. Click the right arrows to move to the next page of results and the left arrow to move to the previous page of results. Click the arrows furthest to the right or left, respectively, to move to the end of the list or the beginning of the list.
- Click **Next>>** to view the next page in the series.
- To see a specific page, type the page number in the space provided and click Go.
- Click any underlined number in a table to open a screen with more details.

Viewing the Task History Details

You can view the following details about the history of the task.

The Task Name identifies the task that the history is about.

- **Completion Date/Time:** displays the date and time for each completed task

  The date and time is sorted in descending order. The task information appears in this window from the most recent instance at the top to the instance that happened the longest time ago at the end.
- **Assessment Results:** the number of machines that present a certain level of security risk to the network. To view additional details about these machines, click the respective number.
- **Enforcement:** the number of machines for which Vulnerability Assessment has requested blocking.
- **Unsupported Machines:** the number of machines Vulnerability Assessment found to be using incompatible operating system versions. To view additional details about the unsupported machines, click the respective number.
- **Pattern File Number:** the pattern file number used to perform a task

View Task Details

Task Details screen displays information about a specific security risk. It provides a list of each machine with that risk. It identifies the machines by name and identifies vulnerabilities that cause risks and the name of the attacks associated with the vulnerabilities. When you click a machine name, the Machine Status screen appears.

Viewing the information combined in these screens enables you to quickly resolve vulnerability risks. First, you can use the Task History to see if there are any new security risks appearing on your network. Next, you can click a particular security risk to open the Task Details screen and see the specific machines that are presenting the risk. Finally, you can click a machine name to open the Machine Status screen and read detailed information about the vulnerabilities on each machine to learn how to resolve the vulnerability.

Navigating through the screens

- Click **Back** to close the screen and return to the your previous screen
- The number of machines available for viewing is shown in the upper right hand corner, for example 1 - 20 of 48 indicates you are viewing the first 20 logs of a total of 48. Click the right arrows to move to the next page of results and the left arrow to move to the previous page of results. Click the arrows furthest to the

right or left, respectively, to move to the end of the list or the beginning of the list.

- Click **Next>>** to view the next page in the series.
- To see a specific page, type the page number in the space provided and click **Go**.
- Click any underlined number in a table to open a screen with more details.

View details about the task

The top part of the screen gives a summary of the task and the actions of that task.

- **Task Name:** the Task Details screen displays information about this task
- **Action:** states the action (assessment or assessment with enforcement) the administrator set for the task when he or she created it.
- **Issued by:** identifies the person who ran the task
- **Vulnerability Assessment Pattern File:** the number of the pattern file that this task used
- **Vulnerability Assessment Engine:** the engine that Vulnerability Assessment used to complete the task
- **Completion date/time:** states the date and time on which the task finished

View details about the results

The bottom part of the screen provides more detailed information about the results of the task according to the individual machines.

- **Status:** machines have one of four statuses indicated by icons. - blocked, blocking requested or normal. Blocked machines cannot access the network. Blocking requested machines have blocking pending. Normal machines have normal access to the network.
- **IP Address:** the IP Address of the machine that has the vulnerability.
- **Machine:** the name of the machine that has the vulnerability. When you click the name, the Machine Status screen appears.
- **Result:** the result of the assessment according to the risk level that the machine presents to the network. The security risk is determined by the number and severity of the vulnerabilities the machine has.
- **Vulnerability name:** the machine has this vulnerability. The name gives you a standardized reference if you want to do further research about the vulnerability.

- **Potential Malware:** This shows the malware that is known to frequently attack the vulnerability. Malware includes such things as viruses, worms and Trojans.

View Result Summary

You can view details of all Vulnerability Assessment tasks in the Result Summary screen. You can also view results about Deploy failed, Unsupported and Blocked machines in the Result Summary screen.

Icons for reference indicate the status of machines. Machines have one of four modes which indicate the enforcement status of the machines: Blocked, Blocking requested, Not blocked or Release requested.

The Result Summary displays all the results according to individual machines and by security risk level. The number and the severity of the vulnerabilities on each machine determines the risk level. You can use this screen to quickly identify the security risk that each machine presents to the network and learn about the vulnerabilities of specific machines. You can also use this screen to learn which machines on your network are Unsupported or Blocked.

Result Summary Information

- **Status:** The status of the machine is indicated by an icon.
- **IP Address:** the IP Address of the machine that has the vulnerability.
- **Machine:** the name of the machine that has the vulnerability. When you click the name, the Machine Status screen appears.
- **Result:** the result of the assessment according to the risk level that the machine presents to the network. The security risk is determined by the number and severity of the vulnerabilities the machine has.
- **Vulnerability name:** the machine has this vulnerability. The name gives you a standardized reference if you want to do further research about the vulnerability.
- **Potential Malware:** This shows the malware that is known to frequently attack the vulnerability. Malware includes such things as viruses, worms and Trojans.
- **Task Name:** the name of the Assessment Task that identified the virus.
- **Completion Date/Time:** the date on which the task that identified the virus ran.

Result Summary Actions

Navigating through the results summary information

- Click **Back** to close the Results Summary screen and return to the your previous screen
- The Results Summary shows the number of tasks available for viewing in the upper right hand corner, for example 1 - 20 of 48 indicates you are viewing the first 20 logs of a total of 48. Click the right arrows to move to the next page of results and the left arrow to move to the previous page of results. Click the arrows furthest to the right or left, respectively, to move to the end of the list or the beginning of the list.
- To see a specific page, type the page number in the space provided and click **Go**.

Blocking machines

When you block a machine, Vulnerability Assessment marks the machine for blocking by Network VirusWall. Network VirusWall queries Vulnerability Assessment and blocks all computers for which Vulnerability Assessment requests blocking. The next time that the computer attempts to communicate with the network, Network VirusWall blocks it and prevents it from contacting the network.

To block a machine:

1. Select the machines you want to block.
2. Click **Block**.

Releasing machines

When you release a machine, Network VirusWall no longer blocks the computer. It is free to reestablish communications with the network.

To release a machine:

1. Select the machines you want to release.
2. Click **Release**.

WARNING! *When you manually release the machine, you override all other enforcement policies.*

Viewing the Top Ten Vulnerabilities

You can view the most frequent vulnerabilities on your network from the Your Top 10 Vulnerabilities screen. It displays the names of ten vulnerabilities on your network and the number of machines that have the vulnerability. It also gives some brief details about the vulnerabilities.

You can view the following detailed information:

- **Rank:** This displays the rank from 1 to 10.
- **Damage Potential:** The damage potential is the based on the damage that the vulnerability presents to the machine on which it is located. When there is a high level or number of damage potential on a machine, VAS shows a high level risk to the network (such as critical or important).
- **Vulnerability Title:** The title gives a brief description of the vulnerability and the possible consequences of having that vulnerability.
- **Vulnerability Name:** The name Vulnerability Assessment uses is an industry standard. This makes it easy to obtain further information on the vulnerability and quickly learn how to resolve it.
- **Machine Count:** The number of machines that have this vulnerability.
- **Potential Malware:** The virus that frequently exploits this vulnerability. Vulnerability Assessment uses an industry standard name to make it easy to obtain further information on the virus.
- **Affected Software:** This is a list of software that the vulnerability is known to affect.

View Machine Status

Vulnerability Assessment reports the results of its assessments according to the security risks to the network. These security risks are based on the number and severity of vulnerabilities of individual computers. You can view the status of individual machines from the Machine Status screen, which provides a quick way to investigate the most important risks to your network and learn how to resolve these risks.

View Machine Details

IP Address and Machine identify the computer that has the vulnerability.

- **Status:** Icons indicate the status of the computer. The status is based on the actions you set when you created the assessment task.
- **Result:** This describes the level of security risk that this computer presents to the network. The number and severity of vulnerabilities on each computer determine the results.

Task Name, Action and Completion date/time describe the task that generated the results that Vulnerability Assessment displays in this window.

View Security Summary

This gives a brief summary of the number and severity of the vulnerabilities on this computer. They are organized according to the damage potential that each vulnerability represents to this computer. Details for these risks are given below.

View Vulnerability Details

- **Damage Potential:** The damage potential is the based on the damage that the vulnerability presents to the machine on which it is located. When there is a high level or number of damage potential on a machine, Vulnerability Assessment shows a high level risk to the network (such as critical or important).
- **Vulnerability Title:** The title gives a brief description of the vulnerability and the possible consequences of having that vulnerability.
- **Vulnerability Name:** The name Vulnerability Assessment uses is an industry standard. This makes it easy to obtain further information on the vulnerability and quickly learn how to resolve it.
- **Potential Malware:** This shows the malware that is known to frequently attack the vulnerability. Malware includes such things as viruses, worms and Trojans.
- **Affected Software:** This is a list of software that the vulnerability is known to affect.
- **CVE/CAN Number:** The Common Vulnerability and Exposures number and the Candidate number (a vulnerability pending naming standardization) are alternate identifiers for the vulnerability. This makes it easy to obtain further information on the vulnerability and quickly learn how to resolve it.

Create a query

Vulnerability Assessment creates a log when it runs a task. The results of the scan are logged and stored on the Control Manager server. The log contains all the results of the assessment and the status of the machines that it assessed. You can create reports based on these logs. You can use the Custom Query from the History screen to query the logs and generate reports.

To create a customized log query:

1. In Task date select either all dates to include all the results from when the first task was run or set a range of dates. When you set a range of dates only the results that the tasks generated between those dates are included in your report.
2. In Result select the risk level results of the machines you want to include in your report.
3. In Status select blocking requested to include machines that Vulnerability Assessment blocked as a consequence of your enforcement policy in your report. When you select normal, your report displays all non-blocked machines.
4. In Task name select the name of a task you want to query. Your query report includes only results from this task.
5. In Domain name(s), specify logs by typing one or more valid Windows domain names (Fully Qualified Domain Names are not valid); for example, Domain1;Domain2.
6. In Machine name(s), specify logs by typing one or more valid Windows NetBIOS machine names; for example, Machine1;Machine2.
7. In Vulnerability name(s), type the name of the vulnerabilities to include in your report. If Vulnerability Assessment generated results based on that vulnerability name, it will be shown in your report.
8. Potential Malware(s): This shows the malware that is known to frequently attack the vulnerability. Malware includes such things as viruses, worms and Trojans.
9. In Vulnerability Assessment Pattern File select a version of the pattern file. If Vulnerability Assessment used this pattern file to perform an assessment task, it will show that in your report.
10. In Vulnerability Assessment Engine select a version of the scan engine. If Vulnerability Assessment used this engine to perform an assessment task, it will show that in your report.
11. In Logs per page, type the number of logs that will appear per page.

12. Click **Query** to perform the query. Alternatively, click **Back**, to return to Vulnerability Assessment History. To reset this form, click **Reset**.

View Query Results

The Query Results screen displays all the results of your log query. The type of information displayed in this screen depends on the options you selected in the Create Custom Query.

Query Results displays detailed information about the following:

- **Completion Date/Time:** the date on which the task ran.
- **Result:** the result according to the risk level that the machine presents to the network.
- **Status:** machines have one of three statuses indicated by icons. - blocked, blocking requested or normal. Your report, never shows the status of blocked because it only shows status results as they were logged immediately following the assessment task. At that time, Vulnerability Assessment had requested blocking, but blocking had not yet been performed.
- **Domain name:** the domain name of the machine that has the vulnerability.
- **Machine:** the name of the machine that has the vulnerability. When you click the name, the Machine Status screen appears.
- **Vulnerability name:** the machine has this vulnerability. The name gives you a standardized reference if you want to do further research about the vulnerability.
- **Potential Malware:** This shows the malware that is known to frequently attack the vulnerability. Malware includes such things as viruses, worms and Trojans.
- **Task Name:** the name of the Assessment Task that identified the virus.
- **Pattern:** the pattern file that Vulnerability Assessment used to perform the task.
- **Engine:** the engine version that Vulnerability Assessment used to perform the task.

Generate Comparative Reports

The Vulnerability Assessment creates a log when it runs a task, and the Control Manager server logs and stores the results. You can use Vulnerability Assessment to generate reports that compare two logs from the same task.

Viewing comparative reports allows you to ...

- See if the task has changed from one occurrence to the next
- Measure the progress of removing vulnerabilities from your network
- See if new vulnerabilities have been introduced to your network

To generate a comparative report:

1. From the Task History screen, click Generate ... to open the Generate Comparative Report screen.
2. Select the task that you in your report, then click Next >.
3. Select two logs that you want to use in your report, then click Next >. Information about the task and the logs you selected then appears in a new screen.

View Comparative Reports Results

From the Task History screen you can generate a comparative report, and this screen shows the results.

General Comparative Statistics

This portion of the screen provides statistics about two logs of the same task divided into two columns according to the date and time that each occurrence of the task.

You can view the following details:

- Total assessment time. The time that it took to run the task.
- Vulnerability assessment engine and the Vulnerability assessment pattern file used to perform the assessment task.
- Total machines assessed. The total number of machines the task assessed.
- Security risk levels of the machine. The number of machines for each risk level. The risk level is determined by the number and the severity of vulnerabilities on each computer.
- Unsupported Machines: the number of machines Vulnerability Assessment found to be using incompatible operating system versions. To view additional details about the task that reported these unsupported machines, click the respective number.
- Blocking requested machines The number of machines for which Vulnerability Assessment has requested blocking.

Machine Differences

This portion of the screen compares individual machines assessed during the two different occurrences of the task. The first column describes the machine by its IP address, name and latest risk level. The last two columns provide information about the specific vulnerabilities identified during each incidence of the task.

You can view the following details:

- IP Address: the IP Address of the machines included in task.
- Machine: the name of the machine that was included in the task.
- Latest Risk Level: the result of the assessment according to the risk level that the machine presents to the network. The security risk is determined by the number and severity of the vulnerabilities the machine has.
- Vulnerability name: the machine has this vulnerability. The name gives you a standardized reference if you want to do further research about the vulnerability.

Account Management Tool Tutorial

This tutorial shows how to use the account management tool. Use this tool to view, add, modify, or delete login credentials for the target machines and domains you want to add in the Select Machines. See also *Select Machines* on page 9-44.

This tool is only accessible from the machine hosting the Control Manager Server. When using the account management tool, you cannot input IP addresses.

Note: The account management tool is a global tool used by several services including Damage Cleanup Services and Vulnerability Assessment. Adding, editing, or deleting entries will impact all services using this tool.

Viewing All Existing Domains and Machines

To view all existing domains and machines:

1. Click **Start** > **Program Files** > **Trend Micro Control Manager** > **Account Management Tool** to open the account management tool.
2. Select **Domain** or **Machine** next to Type to view all existing domains and machines and the available description. The default is Domain.

3. Click **Exit** to close the tool.

Adding a Domain or Machine

To add a domain or machine:

1. Click **Start** > **Program Files** > **Trend Micro Control Manager** > **Account Management Tool** to open the account management tool.
2. Click **Add...** to add a domain or machine. The Add a New Account screen appears.
3. Select **Domain** or **Machine** next to Type. The default is Domain.
4. Do one of the following:

   If you selected Domain in step 3:

   a. Type the Windows domain name you wish to add next to Domain name.

   b. Type the domain administrator account next to Domain administrator account.

   c. Type the password for the domain administrator account next to **Password**.

   d. Retype the password entered in step 3 next to **Confirm password**.

   e. Type a description for this account next to **Description**.

   If you selected Machine in step 3:

   a. Type the machine name you wish to add next to **Machine name**.

   b. Type the machine administrator account next to **Administrator account**.

   c. Type the password for the machine administrator account next to **Password**.

   d. Retype the password entered in step 3 next to **Confirm password**.

   e. Type a description for this account next to **Description**.
5. Click **Apply**.
6. Click **OK** to save this setting.
7. Click **OK**. The domain appears in the list under Accounts.
8. Click **Exit** to close the tool.

Deleting a Domain or Machine

To delete a domain or machine:

1. Click **Start > Program Files > Trend Micro Control Manager > Account Management Tool** to open the account management tool.
2. Select Domain or Machine next to Type to view all existing domains and machines and the available description. The default is Domain.
3. Do one of the following:

   If you selected Domain in step 2:

   a. Click the domain you wish to delete in the Accounts list.

   b. Click **Delete**.

   c. Type the password for the domain administrator account.

   If you selected Machine in step 2:

   a. Click the machine you wish to delete in the Accounts list.

   b. Click **Delete**.

   c. Type the password for the machine administrator account.
4. Click **OK** to save this setting.
5. Click **OK** in the confirmation screen.
6. Click **Exit** to close the tool.

Modifying Domain or Machine Information

To modify domain and machine information:

1. Click **Start > Program Files > Trend Micro Control Manager > Account Management Tool** to open the account management tool.
2. Select **Domain** or **Machine** next to Type to view all existing domains and machines and the available description. The default is Domain.
3. Do one of the following:

   If you selected Domain in step 2:

   a. Click the domain you wish to modify in the Accounts list.

   b. Click **Modify**.

c. Type the updated domain information in **Domain name**, **Domain administrator account**, and **Description**. To change the password, type the new password in **New password**, and in **Confirm new password**.

d. Type the pre-existing password in **Old Password**.

If you selected Machine in step 2:

a. Click the machine you wish to modify in the Accounts list.

b. Click **Modify**.

c. Type the updated domain information in **Machine name**, **Administrator account**, and **Description**. To change the password, type the new password in **New password**, and **Confirm new password**.

d. Type the pre-existing password in **Old Password**.

4. Click **OK** to save this setting.
5. Click **OK** in the confirmation screen.
6. Click **Exit** to close the tool.

Chapter 10

Using Control Manager Tools

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

Control Manager houses most tools at the following location:

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

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

- *Agent Migration Tool (AgentMigrateTool.exe)* on page 10-2
- *Cascading Management Structure Tool (CasTool.exe)* on page 10-2
- *IIS Restoration Tool (SetupPatch.exe)* on page 10-5
- *Web Server and Port Configuration Tool (CMWebCfg.bat)* on page 10-6
- *Using the Control Manager MIB File* on page 10-7
- *Using the NVW 1.x SNMPv2 MIB File* on page 10-7
- *Using the NVW Enforcer SNMPv2 MIB File* on page 10-8
- *Use the NVW System Log Viewer* on page 10-8
- *Use the NVW 1.x Rescue Utility* on page 10-8

Agent Migration Tool (`AgentMigrateTool.exe`)

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

- Generates a migration list (see *Generate a Migration List* on page 5-16), 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.

- Migrates 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, and MCP Agents* on page 5-14)

  Run `AgentMigrateTool.exe` directly on the destination server.

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

For older agents, like TVCS or Control Manager 2.x agents, the Agent Migration Tool can only migrate Windows-based agents. Please contact Trend Micro Support for migrating non-Windows based agents (see *Contacting Technical Support* on page 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
castool `/p`:{parent server name:port}	To specify the parent server that the child server will register to. For example: `castool /p:SAGADA_SRV1:2061` Use `/p` with other CasTool child server registration commands. Do not use it separately.
castool `/n`:{parent server user account}	To specify the user account to register a child server to a parent server. {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. For example: `castool /n:root` Trend Micro suggests the use of the parent server root account created during the Control manager installation. Use `/n` with other CasTool child server registration commands. Do not use it separately.

TABLE 10-1. `CasTool.exe` commands

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

TABLE 10-1. `CasTool.exe` commands

COMMAND	USAGE
castool /s	To specify that an HTTPS connection exists between parent and child server. The command retrieves the E2EPublic.dat key from the parent server. For example: castool /n:root /p:cm.test.com:8080 /c:"child_01" /s 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. Use /s with CasTool registration commands. Do not use it separately.
castool /d	To enable CasTool.exe debugging. CasTool.exe saves debug logs in <root>:\Program Files\Trend Micro\Control Manager\debuglog folder. Use/d with CasTool registration and unregistration commands. Do not use it separately.

TABLE 10-1. 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.

Chapter 11

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 11-2
- *Remove a Windows-Based Control Manager Agent* on page 11-2
- *Manually Removing Control Manager* on page 11-6

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.

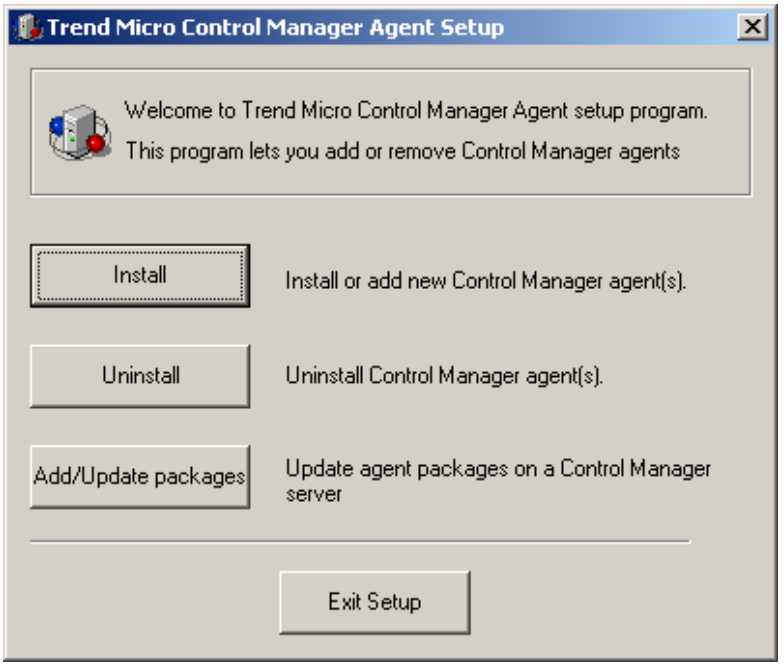


FIGURE 11-1. Trend Micro Agent setup program

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

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

FIGURE 11-2. 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.

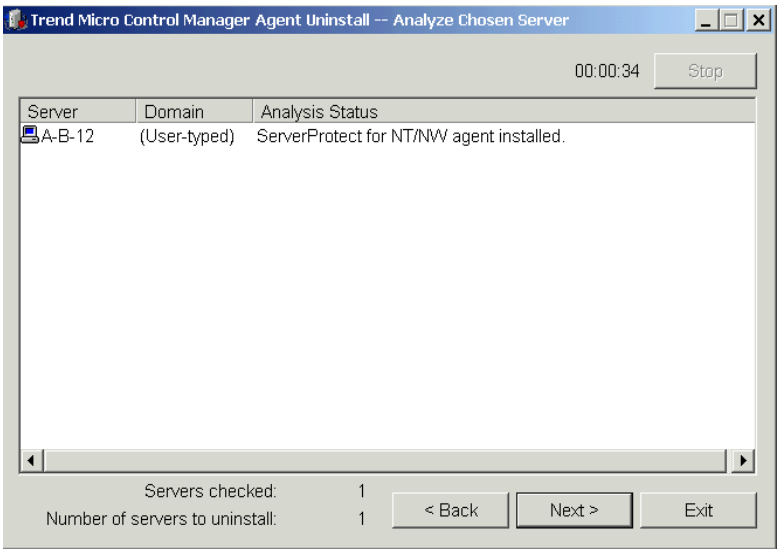


FIGURE 11-3. Analyze chosen Control Manager

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`

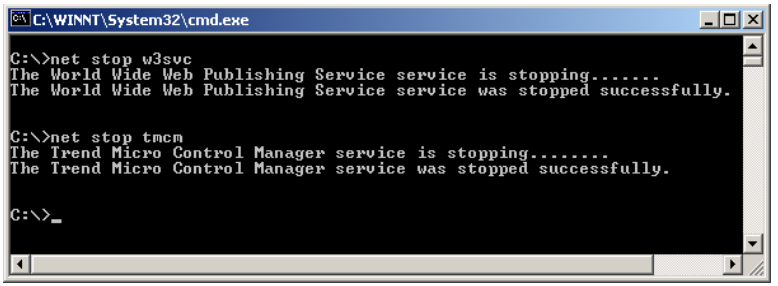


FIGURE 11-4. View of the command line with the necessary services stopped

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\TMCM`
- `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\TMCM
- 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). 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`

Chapter 12

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 12-2
- *Contacting Technical Support* on page 12-2
- *TrendLabs™* on page 12-3
- *Other Useful Resources* on page 12-3

Before Contacting Technical Support

Before contacting technical support, here are two things you can quickly do to try and find a solution to your problem:

- **Check your documentation**: the manual and online help provide comprehensive information about Control Manager. Search both documents to see if they contain your solution.
- **Visit our Technical Support Web site**: our Technical Support Web site contains the latest information about all Trend Micro products. The support Web site has answers to previous user inquiries.

  To search the Knowledge Base, visit

  `http://esupport.trendmicro.com/support`

Contacting Technical Support

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

- Email support

  `support@trendmicro.com`

- On-line help - configuring the product and parameter-specific tips
- Readme - late-breaking product news, installation instructions, known issues, and version specific information
- Knowledge Base - technical information procedures provided by the Support team:

  `http://esupport.trendmicro.com/support`

- Product updates and patches

  `http://www.trendmicro.com/download/`

To locate the Trend Micro office nearest you, open a Web browser to the following URL:

`http://www.trendmicro.com/en/about/contact/overview.htm`

To speed up the problem resolution, when you contact our staff please provide as much of the following information as you can:

- Product serial number
- Control Manager Build version
- Operating system version, Internet connection type, and database version (for example, SQL 2000 or SQL 7.0)
- Exact text of the error message, if any
- Steps to reproduce the problem

TrendLabs™

Trend Micro TrendLabs 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
```

Other Useful Resources

Trend Micro offers a host of services via its Web site, www.trendmicro.com.

Internet-based tools and services include:

- The World Virus Tracking Center - monitor virus incidents around the world
- HouseCall™ - Trend Micro online virus scanner
- Virus risk assessment – the Trend Micro online virus protection assessment program for corporate networks

Chapter 13

Troubleshooting and FAQs

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 sections:

- *Troubleshooting* on page 13-2
- *FAQs* on page 13-21

Troubleshooting

The troubleshooting section of this chapter includes the following:

- *General Troubleshooting* on page 13-2
- *Troubleshooting MCP* on page 13-14
- *Troubleshooting Reporting* on page 13-15
- *Troubleshooting the Cascading Environment* on page 13-15
- *Troubleshooting Installation* on page 13-17
- *Troubleshooting Update Manager* on page 13-19

General Troubleshooting

Troubleshooting CasTool.exe

The following table lists the most common CasTool.exe error messages:

CasTool Error Message	Reason / What To Do
Unable to establish a cascading relationship.	TMI.cfg may be corrupt. Restore a backup, if available. Otherwise, reinstall Control Manager.
Unable to write information to TMI.cfg. The file may be corrupted.	TMI.cfg may be corrupt. Restore a backup, if available. Otherwise, reinstall Control Manager.
The configuration file TMI.cfg contains an invalid GUID, the file may be corrupt.	TMI.cfg may be corrupt. Restore a backup, if available. Otherwise, reinstall Control Manager.
Unable to copy authentication information to TMI.cfg.	TMI.cfg may be corrupt. Restore a backup, if available. Otherwise, reinstall Control Manager.
Unable to initialize the child server cascading status.	The network may be congested or broken. Adjust the QueryTimeOut value of CastoolConfiguration.xml.

CasTool Error Message	Reason / What To Do
Unable to create the configuration file, DMRegisterInfo.xml.	Check the CasTool parameters you provided as well as the network connection, and then try again.
Unable to obtain result from the child server. A timeout error has occurred.	Check the network connection and try again. You may need to adjust the NetworkTimeOut value in CastoolConfiguration.xml.

Adjusting CastoolConfiguration.xml Parameters

Modify the CastoolConfiguration.xml parameters to adjust the network, query, and restart service time-out values.

Note: Use care when modifying Control Manager *.xml or *.cfg files. To ensure that you can rollback to the original settings, backup CastoolConfiguration.xml.

To modify CastoolConfiguration.xml:

1. Open <root>\Program Files\Trend Micro\Control Manager\CastoolConfiguration.xml using a text editor (for example, Notepad.exe).
2. Adjust the values for the following parameters:
   - NetworkTimeOut — indicates the timeout followed whenever CasTool downloads the public key from the parent server
     - Minimum allowable value: 10 seconds
     - Maximum allowable value: 300 seconds
   - QueryTimeOut — indicates the timeout followed whenever CasTool queries the child or parent server
     - Minimum allowable value: 75 seconds
     - Maximum allowable value: 300 seconds
   - RestartServiceTimeOut — indicates the timeout followed whenever CasTool restarts the Control Manager services for both the child and parent servers
     - Minimum allowable value: 150 seconds
     - Maximum allowable value: 300 seconds

Note: The Control Manager services, found in Windows Services panel, have a default restart time-out value of 3 minutes (180 seconds).

3. Save and close CastoolConfiguration.xml.

Adjusting AgentMigrationTool.ini Parameters

You can adjust the following AgentMigrationTool.ini:

Parameter	Minimum Allowable Value (in seconds)	Maximum Allowable Value (in seconds)
TMCM_SERVICE_TIMEOUT	60	600
TMI_SERVICE_TIMEOUT	30	300

Note: Making incorrect changes to the configuration file can cause serious system problem. Backup AgentMigrationTool.ini to restore your original settings.

POP3 email notification does not work. What should I do?

You configured Control Manager to send notification to a POP3 account (for example, my_email@yahoo.com). However, Control Manager does not send notifications to my_email@yahoo.com.

To troubleshoot why email notification to a POP3 account is not working:

1. Check if the Exchange Server is an internal or a production Exchange Server.

   If the Exchange server is an internal server, meaning the Internet Mail Service has not been installed, then the Exchange Server will not be able to send an email outside of the Exchange Server.

2. Check if the Internet Mail Service (Microsoft Exchange™ 5.5) or Connector for SMTP Connector (Microsoft Exchange 2000) is installed on the Exchange Server.

3. Verify if the Exchange server is able to send messages to an account not belonging to the organization:

   a. From the Control Manager server, open a mail client (for example, Outlook Express™).

b. Create new mail message and send it to a POP3 account.

c. Using Windows Explorer™, open the POP3 account Inbox and check if it receives the mail from the Control Manager server.

- If the POP3 account receives the email, the Exchange server has the Internet Mail Service or Connector already configured
  - **i.** Access the Control Manager management console.
  - **ii.** Configure the notification method settings.
  - **iii.** On the working area under SMTP Server, check if the Exchange server hostname, port, and email address.
- If the POP3 account did not receive the email, the Exchange server has no Internet Mail Service or Connector configured

d. Install the Exchange server Internet Mail Service to send email notification to a POP3 account.

Control Manager is unable to establish connection to the TMI message routing framework. What should I do?

This message appears either because:

- The Control Manager server is turned off
- There is no network connection
- The Control Manager services are stopped

Check if any of the above cases is true and then try to resolve the issue by restarting the Control Manager server or establishing the network connection.

Installing the Control Manager server without reinstalling its agents

The Control Manager server lost connection to its managed products. This happens because the SQL Server crashed and there is no backup of the Control Manager database that can be used to restore the original Control Manager server-agent configuration. Complete the following procedures to reinstall the Control Manager server without reinstalling the Control Manager agents managed by the server.

Note: These procedures will only work if you will install the Control Manager server on the same server, where it was previously installed. This means that when

reinstalling, make sure that you will use the same IP address and hostname you used during the original installation.

To reinstall the Control Manager server without having to reinstall the Control Manager agents:

1. Using Windows Services, check that the SQL Server service is running.
2. Using Windows Explorer, back up the <root>\Program Files\Trend Micro\CmkeyBackup folder.

   The CmkeyBackup folder contains the following files:

   - Authinfo.ini
   - TVCS_Cert.pem
   - TVCS_Pri.pem
   - TVCS_Pub.pem

   These are the Control Manager encryption keys.
3. Uninstall the original Control Manager server using Start > Programs > Trend Micro Control Manager > Uninstalling Trend Micro Control Manager.
4. Reboot the server.
5. Reinstall the Control Manager server. Specify the same IP address and hostname during the installation.
6. After the installation, use Windows Services to stop the Control Manager services in the following order:
   - Trend Micro Common CGI
   - Trend Micro Management Infrastructure
   - Trend Micro Control Manager
7. Copy the CmkeyBackup backup file to the <root>\Program Files\Trend Micro\Control Manager folder.
8. After replacing backup files, use Windows Services to restart the Control Manager services in the following order:
   - Trend Micro Common CGI
   - Trend Micro Management Infrastructure
   - Trend Micro Control Manager

9. Using Windows Services, stop and restart the Control Manager agent service, this allows the agent to report to the same Control Manager server.
   - Restart Trend Micro Management Infrastructure for Control Manager 2.x agents
   - Restart Trend VCS Agent for Trend VCS 1.8x agents

Manually Removing Control Manager

If you are unable to remove a Control Manager server using the Windows Start menu or the Windows Control Panel, you can manually remove Control Manager. However, Trend Micro recommends trying the automatic methods before attempting to manually remove the product.

To complete the manual uninstallation of Control Manager, perform the following procedures:

Step 1: Stop Control Manager services.

Step 2: Remove the Control Manager Internet Information Services (IIS) settings.

Step 3: Delete Control Manager files/directories and registry keys.

Step 4: Remove Crystal Reports.

Step 5: Remove database components.

Step 1: To stop Control Manager services:

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

Step 2: To remove the Control Manager 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-hand menu, double-click the server name to expand the console tree.
4. Double-click **Default Web Site**.
5. Delete the following virtual directories:
   - ControlManager

- TVCSDownload
- Viewer9
- TVCS
- Jakarta

6. Right-click the IIS Web site you set during installation.
7. Click **Properties**.
8. Click the **ISAPI Filters** tab.
9. Delete the following ISAPI filters:
   - TmcmRedirect
   - CCGIRedirect
10. Click **OK**.

Step 3: To manually remove a Control Manager server:

1. Delete the following directories:
   - `...\Trend Micro\Control Manager`
   - `...\Trend Micro\COMMON\ccgi`
   - `...\Trend Micro\COMMON\TMI`
2. Delete the following Control Manager registry keys:
   - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TVCS\…`
   - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TMCM`
   - `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\TMCM`
   - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro Infrastructure\…`
   - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendCCGI`

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro_NTP`

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

   `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\DamageCleanupService\...`

Step 4: To remove Crystal Reports:

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

Step 5: Removing the Control Manager database components requires the completion of the following steps:

1. Remove Control Manager ODBC settings:
   a. On the Control Manager server, click **Start** > **Run**.
   b. In the Open box, type:

      `odbcad32.exe`

   c. On the ODBC Data Source Administrator window, click the **System DSN** tab.
   d. Under Name, select **ControlManager_Database**.
   e. Click **Remove**, and click **Yes** to confirm.
2. Remove the Control Manager MSDE database:
   a. On the Control Manager server, stop the following services:
      - MSDE service (MSSQLServer service)
      - SQL Service Manager
   b. Delete the `...\Trend Micro\MSDE` directory.
   c. Delete the following registry keys:
      - HKLM\SW\Microsoft\MSSQLServer
      - HKLM\SW\Microsoft\MSDE
      - HKLM\SW\Microsoft\Windows\CurrentVersion\Uninstall\MSDE

- HKLM\CCS\Services\MSSQLServer

Removing the Control Manager IIS Settings

Remove the Internet Information Services settings after stopping the Control Manager services.

Tip: Trend Micro recommends attempting to remove Control Manager using the Windows Start menu or the Windows Control Panel. Use the manual removal instructions as the last resort.

To remove the Control Manager 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-hand menu, double-click the server name to expand the console tree.
4. Double-click **Default Web Site**.
5. Delete the following virtual directories:
   - ControlManager
   - TVCSDownload
   - Viewer9
   - TVCS
   - Jakarta
6. Right-click the IIS Web site you set during installation.
7. Click **Properties**.
8. Click the **ISAPI Filters** tab.
9. Delete the following ISAPI filters:
   - TmcmRedirect
   - CCGIRedirect
10. Click **OK**.

Deleting Control Manager Files/Directories and Registry Keys

If you are unable to remove a Control Manager server from the Windows Start menu or using the Windows Control Panel, you can manually remove a Control Manager server.

Tip: Trend Micro recommends attempting to remove Control Manager using the Windows Start menu or the Windows Control Panel. Use the manual removal instructions as the last resort.

To manually remove a Control Manager server:

1. Delete the following directories:
   - `...\Trend Micro\Control Manager`
   - `...\Trend Micro\COMMON\ccgi`
   - `...\Trend Micro\COMMON\TMI`
2. Delete the following Control Manager registry keys:
   - HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TVCS\….
   - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TMCM`
   - `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\TMCM`
   - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro Infrastructure\…`
   - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendCCGI`
   - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro_NTP`
3. Delete all the Damage Cleanup Services registry keys at the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\DamageCle
anupService\...
```

Removing 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, then click **Remove** to remove the Crystal Reports related files automatically.

Removing Database Components

After manually removing the Control Manager server, you also need to remove related database components.

Tip: Trend Micro recommends attempting to remove Control Manager using the Windows Start menu or the Windows Control Panel. Use the manual removal instructions as the last resort.

Removing the Control Manager database components requires the completion of the following steps:

1. Remove Control Manager ODBC settings:
   a. On the Control Manager server, click **Start** > **Run**.
   b. In the Open box, type:

      ```
      odbcad32.exe
      ```

   c. On the ODBC Data Source Administrator window, click the **System DSN** tab.
   d. Under Name, select **ControlManager_Database**.
   e. Click **Remove**, and click **Yes** to confirm.
2. Remove the Control Manager MSDE database:
   a. On the Control Manager server, stop the following services:

- MSDE service (MSSQLServer service)
- SQL Service Manager

b. Delete the `...\Trend Micro\MSDE` directory.

c. Delete the following registry keys:

- HKLM\SW\Microsoft\MSSQLServer
- HKLM\SW\Microsoft\MSDE
- HKLM\SW\Microsoft\Windows\CurrentVersion\Uninstall\MSDE
- HKLM\CCS\Services\MSSQLServer

Reducing the Database Size

This topic explains how to reduce the size of the transaction log if db_controlmanager is taking up a lot of disk space.

Specifically, the db_controlmanager_log.ldf is using 24GB while the db_controlmanager.mdf is only using 300MB.

How can the size of this transaction log be reduced?

The size of the log files are physically reduced when:

- A DBCC SHRINKDATABASE statement is executed.
- A DBCC SHRINKFILE statement referencing a log file is executed.
- An autoshrink operation occurs.

Option 1: Truncate the TB_invalid Log

Type the following SQL command:

```
truncate table tb_invalidlog
```

Option 2: Configure the Database

The following configuration will help in truncating the log automatically.

The log will be truncated every 30 min (SQL 2000 default) if the record is done after Checkpoint.

Execute the following commands on the SQL Server:

- Alter Database db_controlManager set recovery simple
- Alter Database db_controlManager set auto_shrink on

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

Option 3: Manually Truncate the Log

DBCC shrinkDatabase(db_controlManager)

Backup log db_controlManager with truncate_only

Unable to Deploy Components to Managed Product after Changing the Control Manager Host Name

After changing the Control Manager host name, the Control Manager server is unable to deploy components to its managed product.

To resolve this issue, run the CmWebCfg.bat tool to automatically renew the Control Manager Web server and port.

Troubleshooting MCP

How do I verify Control Manager is using two-way communication for MCP?

If an agent is configured to use two-way communication, Control Manager auto-detects the two-way connection and uses CGI notifications to communicate with MCP agents.

To verify Control Manager is using two-way communication with MCP agents, check the Control Manager database table CDSM_Entity. For more information, see *Verify the Communication Method Between MCP and Control Manager* on page 8-21.

How do I verify that the MCP agent received the notification for two-way communication from Control Manager?

Complete the following:

1. Trigger a command to the agent.
2. Check the cmdHandlerTVCSCommand.log and search for **SendHTTPNotify**. That means Control Manager sent a notification to the agent.
3. Check the agent debug log and search for **Got command Notification !!!**. That means the agent received the notification.

The MCP agent cannot use HTTPS to register to the Control Manager server. What should I do?

First, check the values in Agent.ini:

- TMCM_Server_Port=443
- TMCM_Certificate=C:\TMCM_CA_Cert.pem
- SSL_Enable=1

TMCM_CA_Cert.pem is Control Manager certificate file. It is located at `<TMCM root>\Certificate\CA\`. However, for security consideration, Control Manager does not provide Web download for this certificate. Control Manager administrators should give the file to managed products in a secure manner.

Finally, if the value of the TMCM_Certificate is blank, the agent can still register to Control Manager, but in this situation the agent will always trust the communication from Control Manager.

Troubleshooting Reporting

I do not want to send reports in zip file format. What can I do?

Some mail server policies require passwords for zip files, but Control Manager also supports to sending attachments without zipping the files.

To configure Control Manager to send reports with out zipping the files:

1. Open <Control Manager directory>.
2. Open the SystemConfiguration.xml file and change the value to from 1 to 0 in the following line:

   ```
   <P Name="m_iZipReportAttachment" Value="1"/>
   ```

Troubleshooting the Cascading Environment

When does a child server upload logs to the parent server?

A child server can upload logs to the parent server when the followings are true:

- The cascading management structure relationship is set to enable
- Log upload is either scheduled or set to on demand

When does a child server upload report profiles to the parent server?

A child server can communicate with the parent server if the cascading management structure relationship is set to enable.

A child server uploads new or updated report profiles to the parent server whenever the following occur on the child server:

- Generates new reports
- Modifies report profiles
- Deletes report profiles

How many child servers and managed products can a parent server support?

Trend Micro tested a parent server with an Intel Pentium 4 1.6GHz and 256MB PC-133 SDRAM. With the above hardware specifications, Control Manager can support 10,000 managed products and 200 child servers with 10,000 managed products registered.

Which child Control Manager server versions are parent Control Manager 3.5 servers compatible with in the cascading management structure?

Control Manager 3.5 parent server can manage the following Control Manager child server versions:

- Control Manager 3.5
- Control Manager 3.0 SP5
- Control Manager 3.0 SP4
- Control Manager 3.0 SP3
- Control Manager 3.0

You cannot register a Control Manager 3.5 server as a child server to a previous version of a Control Manager server

Troubleshooting Installation

How do I reinstalling the Control Manager server without reinstalling the Control Manager agents?

You may want to reinstall the Control Manager server due to a lost connection to the server's managed products. This occurs when the SQL Server crashes and there is no backup of the Control Manager database that you can use to restore the original Control Manager server-agent configuration. Complete the following procedures to reinstall the Control Manager server without reinstalling the Control Manager agents managed by the server.

Note: This procedure will only work if you install the Control Manager server on the same server, where the server was previously installed. This means that when reinstalling, make sure that you will use the same IP address and hostname you used during the original installation.

To reinstall the Control Manager server without having to reinstall the Control Manager agents:

1. Using Windows Services, check that the SQL Server service is running.
2. Using Windows Explorer, back up the `<root>\Program Files\Trend Micro\CmkeyBackup` folder.

   The CmkeyBackup folder contains the following files:

   - Authinfo.ini
   - TVCS_Cert.pem
   - TVCS_Pri.pem
   - TVCS_Pub.pem

   The files are the Control Manager encryption keys.
3. Uninstall the original Control Manager server using **Start > Programs > Trend Micro Control Manager > Uninstall Trend Micro Control Manager**.
4. Reboot the server.
5. Reinstall the Control Manager server. Specify the same IP address and hostname during the previous installation.
6. After the installation, use Windows Services to stop the Control Manager services in the following order:

- Trend Micro Common CGI
- Trend Micro Management Infrastructure
- Trend Micro Control Manager

7. Copy the CmkeyBackup backup file to the `<root>\Program Files\Trend Micro\Control Manager` folder.
8. After replacing backup files, use Windows Services to restart the Control Manager services in the following order:
   - Trend Micro Common CGI
   - Trend Micro Management Infrastructure
   - Trend Micro Control Manager
9. Using Windows Services, stop and restart the Control Manager agent service, this allows the agent to report to the same Control Manager server.
   - Restart Trend Micro Management Infrastructure for Control Manager 2.x agents
   - Restart Trend VCS Agent for Trend VCS 1.8x agents

How do I manually remove Control Manager database components?

After manually removing the Control Manager server, you also need to remove related database components.

Tip: Trend Micro recommends attempting to remove Control Manager using the Windows Start menu or the Windows Control Panel. Use the manual removal instructions as the last resort.

Removing the Control Manager database components requires the completion of the following steps:

- Removing Control Manager ODBC settings:
- Removing the Control Manager MSDE database:

To remove Control Manager ODBC settings:

1. On the Control Manager server, click **Start** > **Run**.
2. In the Open box, type the following: `odbcad32.exe`
3. On the ODBC Data Source Administrator window, click the **System DSN** tab.

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

To remove the Control Manager MSDE database:

1. On the Control Manager server, stop the following services:
   - MSDE service (MSSQLServer service)
   - SQL Service Manager
2. Delete the `...\Trend Micro\MSDE` directory.
3. Delete the following registry keys:
   - HKLM\SW\Microsoft\MSSQLServer
   - HKLM\SW\Microsoft\MSDE
   - HKLM\SW\Microsoft\Windows\CurrentVersion\Uninstall\MSDE
   - HKLM\CCS\Services\MSSQLServer

How can I remove Crystal Reports?

You can automatically remove Crystal Reports using the Add/Remove Programs feature.

To remove Crystal Reports automatically:

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

Troubleshooting Update Manager

When a "General failure on source network" error occurs, how do I resolve the issue?

There are several reasons why this issue occurs:

- Specific files were not found (For example the server.ini was not found)
- Network issues (proxy connection issues, timeout)
- ActiveUpdate server issue (ActiveUpdate server inaccessible)

An "Invalid zip file" error occurs. How do I resolve the issue?

There could be an inconsistency between the server.ini file and the size of the component file.

Updating by UNC is consistently unsuccessful. How do I resolve the issue?

First check the results from the ActiveUpdate log, `TmuDump.txt` in the AU_Log folder.

If you are getting the "WNet Unknown error", the following may be the reason why:

- Wrong account information
  - Wrong account name or password
  - No Account on the ActiveUpdate server
  - No READ permission on the shared folder of the ActiveUpdate server (this might cause WWW-authentication failure)
- Account name without domain name
  - domain_name\user_name

Where can I get more information about updates and when they occur?

Check the ActiveUpdate log, `TmuDump.txt` in the AU_Log folder for more information on updates and when updates occur.

What do I do when I cannot successfully deploy components to managed products?

Verify the following:

- The connection between Control Manager and managed products is working properly
- The **When new updates found** option is checked or cleared when setting Automatic deployment settings
- READ permission is granted on the shared folder of ActiveUpdate for Control Manager. For example: C:\Program files\Trend Micro\Control Manger\WebUI\Donwload\ActiveUpdate

FAQs

This section covers the following topics:

- *General FAQs* on page 13-21
- *Directory Manager FAQs* on page 13-24
- *Active Directory Accounts FAQs* on page 13-25
- *Reporting FAQs* on page 13-25
- *Agent Migration Tool FAQs* on page 13-26
- *Update and Deploy Components FAQs* on page 13-27
- *Product Registration FAQs* on page 13-28
- *Installation FAQs* on page 13-28
- *Product Registration FAQs* on page 13-28

General FAQs

Where is the public encryption key for Trend Micro Control Manager 3.5 located?

Control Manager 3.5 keeps the public encryption key, E2EPublic.dat, in the <root>\Program Files\Trend Micro\Control Manager\WebUI\download folder. Use the download link available in the Control Manager management console.

When does a child server upload logs to the parent server?

A child server can upload logs to the parent server when the following are true:

- The cascading management structure relationship is set to enable
- Log upload is either scheduled or set on demand

When does a child server upload report profiles to the parent server?

A child sever can communicate with the parent server if the cascading management structure relationship is set to enable.

Child server upload new or updated report profiles to the parent server whenever the former:

- Generates new reports

- Modifies report profiles
- Deletes report profiles

How many child servers and managed products can a parent server support?

Trend Micro has tested that a parent server with Intel Pentium 4 1.6GHz and 256MB PC-133 SDRAM Standard hardware specifications can support 10,000 managed products and 200 child servers with 10,000 managed products registered.

How can I verify the Control Manager server and build?

There are two methods to verify the Control Manager server and build versions:

To check the Control Manager management console

1. Log on to the management console.
2. On the header menu, select **About**. The About window provides the product and build version information.

To check the registry editor

1. On the Start menu, click Run.
2. Type Regedit and then click OK.
3. Go to the HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TVCS hive.
4. Check the BuildVersion key.

How can I verify the Control Manager agent version and build?

Check the Control Manager registry hive to verify the Control Manager agent version.

To verify the Control Manager agent version and build:

1. Using a text editor (for example, Notepad), open Entity.cfg, which is located in the directory where Control Manager agent is installed.
2. Check the values of the following keys:

   ENTITY_build

   ENTITY_version

What agents do Control Manager 3.5 servers support?

Control Manager 3.5 supports Trend VCS 1.8x, Control Manager 2.5x and MCP agents.

Why are Trend VCS agents still needed?

Trend VCS agents are needed for legacy product support. Control Manager agents released in the 3rd quarter of 2002, for the most part, did not support older versions of their products.

For example, the Control Manager 2.5 agent for OfficeScan could only be relied on to work with OfficeScan Corporate Edition 5.5 or later. OfficeScan versions prior to 5.5, especially those installed on NetWare servers, require use of the Trend VCS 1.86 agent that comes with Control Manager.

Why am I unable to access some management console options?

Some management console options are accessible to only one user at a time. Refer to *The Function-locking Mechanism* on page 6-4 for details.

Why does a managed product appear twice in the product directory?

This can occur if you replace a Network Interface Card (NIC) on the product's server. In this situation, Control Manager "thinks" the server is a new machine, and will re-register the products on that server to the Control Manager server — thereby duplicating their records, and creating a new managed product.

The product registration mechanism monitors the Media Access Control (MAC) address of your NIC. If it detects that the MAC address of your NIC does not have a corresponding record on the Control Manager server, it will automatically register the entities that use that NIC, as though they had not been registered before.

If you encounter this situation, take note of the following:

- The original managed icon will be tagged as abnormal

  You cannot use the original managed product to control the product.

- Logs that were associated with the original icon will not be automatically transferred to the new managed product icon

  As far as Control Manager is concerned, the new managed product is different from the original — even though they are in fact the same.

- Deleting the original managed product will not adversely affect control of the product via the new managed product

What happens if I delete the User ID used for registering a product?

If the User ID used to register a managed product is deleted, all the products that you registered under this account will not be able to re-register or unregister themselves from the Control Manager server.

Agents re-register themselves when their services are re-started or when they detect that their records on the Control Manager database are either missing, or not current.

Unregistration occurs when the agent is removed from the server of the managed product. If the agent is unable to unregister itself, its remains on the Product Directory.

Which user account can I use when I register a product with Control Manager?

When the agent setup program prompts you for a user name that will manage the account, specify a permanent Control Manager account. Trend Micro recommends using the root account during the Control Manager agent installation.

Directory Manager FAQs

In the Communicator screen, the communicator displays the "Active" icon, while the managed product displays the "Inactive" icon. Why does this occur?

This occurs during product off-hour or logoff periods. The icons of the communicator and product entity have different meanings.

For the computer: The icon indicates connection status to Control Manger.

	Computer active (Even if agent status is logoff/off-hour)
	Computer abnormal (disconnected)

For product agents:

	Agent active
	Agent status is logoff or off-hour
	Agent disconnected

On the Communicator screen, there are two communicators displayed, but there is only one entry on the Communicator Scheduler screen. Why does this occur?

If any product with a TMI agent (Control Manager 2.x agent) is installed in the same machine with a Control Manager server or Cascading server, there is not way to configure the Working hour/Offhour period.

Active Directory Accounts FAQs

A machine joins a domain. Then a user logs in to Windows with a domain account. However, the user is always redirected to the Control Manager Logon screen and the log in is unsuccessful. Why does this occur?

Internet Explorer will always pass current Windows login user credentials, such as “domain\user_name” to the CGI. Control Manager rejects the credentials for the account if the account has not been added to Control Manager.

Add the user to Control Manager and login again.

Reporting FAQs

Can Control Manager generate reports about OfficeScans's firewall logs?

No, Control Manager does not support report generation for OfficeScan firewall logs.

I cannot read figures and tables properly on my computer when reports generate in rich-text format (*.rtf)?

Microsoft Word needs to be present on the computer trying to view files in RTF format.

Control Manager receives security logs from a managed product, then I create a scheduled report profile without using the calendar day feature. I generate a report, but the report contains no data or does not contain all the uploaded data. Why does this occur?

It's because the date range is end at the hour of report generated time. Ex: if report generates at 5:31 pm the date range ends at 5:00 pm.

Agent Migration Tool FAQs

Can I migrate agents from multiple source servers to one Control Manager 3.5 server at once?

No, you cannot. This tool only supports migrating from one source server at a time.

Does the Agent Migration Tool support Linux agent migrations?

The Agent Migration Tool supports migrating both Linux and Windows-based MCP agents. The Agent Migration Tool supports migrating only Windows-based agents for Control Manager 2.5x and TVCS 1.8x agents.

Does Control Manager separate spyware/grayware from the virus count when upgrading Control Manager 3.0 + SP3 and SP4 to Control Manager 3.5 server?

Yes, Control Manager 3.5 separates spyware/grayware items from the virus count when upgrading a previous version to Control Manager 3.5. Agent Migration Tool recounts these logs when migrating logs

Update and Deploy Components FAQs

Can each component have different a download source in Scheduled Download?

Yes, each component can have its own schedule and download source settings.

How do I configure Control Manger to perform downloads by HTTPS?

To configure Control Manager to perform downloads by HTTPS:

1. Click **Administration** > **System Settings**. The System Settings screen appears.
2. Select **Enable HTTPS for the default update download source** in ActiveUpdate settings.

How do I setup Control Manager as an internal ActiveUpdate server?

To configure Control Manager as an update source modify the parameter `m_iDuplicateAl` on SystemConfiguration.xml in Control Manager folder. Set the value as 1.

When performing manual download with any selected components, Control Manager duplicates all components from the update source. Remember to modify the value of `m_iDuplicateAl` to 0 for normal download.

How do I turn on Digital Signature checking during component updates?

ActiveUpdate provides a security mechanism to verify downloaded components. ActiveUpdate uses the certificate and private key to sign SIG files and Control Manager will use the public key for validation. Modify the value of **m_iCheckDigitalSignature** as 1 in `SystemConfiguration.xml` to enable security checking.

How do I configure Control Manager to support UNC downloads?

To configure Control Manager to use UNC downloads, see *Enable UNC Download* on page 6-60.

Why does the message "File downloaded" appear, even when the selected components are up-to-date?

When performing a download, the ActiveUpdate module still tries to download ActiveUpdate patch files. If the ActiveUpdate module downloads a patch file for itself the "File downloaded" message appears.

What is the MetaDataMergeApp.exe?

This tool is provided to update component knowledge for Control Manager. After using the tool you can view new component information on the Home/Administration screen and update the components.

Product Registration FAQs

Can OPS/VA/DCS upgrade their components when their licenses have expired?

No, update functions will be blocked when the OPS/VA/DCS license expires. Other functions still function if the license expires.

What should I do if the Activation Code expires?

If you use a full version Activation Code, you can renew the product license online. If you use a trail version Activation Code, you can convert to the full version through the Trend Micro Web site.

Installation FAQs

How do I install MCP agents?

MCP agents install with their managed product. There is no separate installtion for MCP agents. Refer to your managed product's documentation for instructions on installing the MCP agent.

If I manually reuse a Control Manager database when installing Control Manager 3.5 and choose the "recount" log option, why does it take such a long time to complete the recount process?

Prior to Control Manager 3.5, spyware/grayware were included in the virus category. When installing Control Manager 3.5 spyware/grayware the installation program separates the spyware/grayware items from the virus logs. The length of time the process requires depends on the number of virus logs in the database. If there are more logs in the database, the process takes more time.

Why have I lost some settings after upgrading Control Manager?

The Control Manager upgrade is actually a reinstallation process. Control manager retains some settings after upgrading: entity info, logs and reports.

Why are Trend VCS agents still supported?

Trend VCS agents are needed for legacy product support. Control Manager agents released in the 3rd quarter of 2002, for the most part, do not support older versions of their products.

For example, the Control Manager 2.5 agent for OfficeScan could only be relied on to work with OfficeScan Corporate Edition 5.5 or later. OfficeScan versions prior to 5.5, especially those installed on NetWare servers, require use of the Trend VCS 1.86 agent that comes with Control Manager.

Appendix

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		

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
IP address	10.1.104.225	
Fully Qualified Domain Name (FQDN)	server.company.com	
NetBIOS (host) name	yourserver	
SQL-based Control Manager database information		
IP address	10.1.114.225	
Fully Qualified Domain Name (FQDN)	server.company.com	
NetBIOS (host) name	sqlserver	
Proxy server for component download		
IP address	10.1.174.225	
Fully Qualified Domain Name (FQDN)	proxy.company.com	
NetBIOS (host) name	proxyserver	
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	
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

Control Manager Conventions

Refer to the following conventions applicable for Control Manager installation or management console configuration.

User ID

Max. length	32 characters
Allowed	A-Z, a-z, 0-9, -, _

Folder name

Max. length	40 characters
Not allowed	/ < > & "

Note: For the Control Manager server hostname, Setup supports servers with underscores ("_") as part of the server name.

Control Manager Core Process and Configuration Files

Control Manager uses XML data sources to save system configuration setting and temporary files.

These are the configuration files used by the Control Manager server:

Configuration File	Description
AuthInfo.ini	Configuration file that contains information about private key file names, public key file names, certificate file names, and the encrypted passphrase of the private key as well as the host ID and port.
aucfg.ini	ActiveUpdate configuration file
TVCS_Cert.pem	Certificate used by SSL authentication.

Configuration File	Description
TVCS_Pri.pem	Private Key used by SSL.
TVCS_Pub.pem	Public Key used by SSL.
CasTool.exe	A command line program used to establish a cascading Control Manager environment.
ProcessManager.exe	"Trend Micro Control Manager" service. It launches and stops other Control Manager core processes.
CmdProcessor.exe	Sends XML instructions, formed by other processes, to managed products, processes product registration, sends alerts, performs scheduled tasks, and applies Outbreak Prevention Policies.
UIProcessor.exe	Processes and transforms user input, made at the Control Manager management console, into actual commands.
LogReceiver.exe	Receives managed product logs and messages.
LogRetriever.exe	Retrieves and saves logs in the Control Manager database.
ReportServer.exe	Generates Control Manager reports.
MsgReceiver.exe	Receives messages from the Control Manager server, managed products, and child servers.
EntityEmulator.exe	Allows Control Manager to use Trend VCS agents.
CasProcessor.exe	Allows a Control Manager server (a parent server) to manage other Control Manager servers (child servers).
DCSProcessor.exe	Performs Damage Cleanup Services functions.
Ntpd.exe	Network Time Protocol service.
inetinfo.exe	Microsoft Internet Information Service process.
jk_nt_service.exe java.exe	Java server side extensions used to build Web-based user interface by defining the interface instead of using a lot of standalone CGI programs.
cm.exe	Manages dmserver.exe and mrf.exe.
mrf.exe	The Communicator process.
dmserver.exe	Provides the Control Manager management console log on page and manages the Product Directory (Control Manager server-side).

Configuration File	Description
LWDMServer.exe	Manages the Product Directory (client-side — managed products).
ssleay32.dll	Handles the Control Manager security levels.
TMUpdate.dll	Performs ActiveUpdate functions.
ProcessManager.xml	Used by ProcessManager.exe.
CmdProcessorEventHandler.xml	Used by CmdProcessor.exe.
UIProcessorEventHandler.xml	Used by UIProcessor.exe.
DMRegisterinfo.xml	Used by CasProcessor.exe.
DataSource.xml	Stores the connection parameters for Control Manager processes.
CastoolConfiguration.xml	Used by CasTool.exe.
SystemConfiguration.xml	Control Manager system configuration file
CascadingLogConfiguration.xml	Log upload configuration file used for child servers
TMI.cfg	Trend Micro Infrastructure configuration file.
Entity.cfg	Managed product configuration file.

Control Manager Communication and Listening Ports

These are the default Control Manager communication and listening ports.

Type	Communication Port
Internal communication	10198
External communication	10319
Damage Cleanup Services and Vulnerability Assessment communication	20901, 20902

Service	Service Port
ProcessManager.exe	20501
CmdProcessor.exe	20101
UIProcessor.exe	20701
LogReceiver.exe	20201
LogRetriever.exe	20301
ReportServer.exe	20601
MsgReceiver.exe	20001
EntityEmulator.exe	20401
CasProcessor.exe	20801
DcsProcessor.exe	20903

Trend 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							●	●

Features	TVCS	Control Manager						
	1.84	2.0	2.1	2.5	3.0 Ent	3.0 Std	3.5 Ent	3.5 Std
Spyware/grayware detection, reporting, and cleanup							●	●
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		●	●	●	●	●	●	●

FEATURES	TVCS	CONTROL MANAGER						
	1.84	2.0	2.1	2.5	3.0 ENT	3.0 STD	3.5 ENT	3.5 STD
Control Manager MIB files (previously called HP OpenView MIB)		●	●	●	●	●	●	●
Improved Navigation			●	●	●	●	●	●
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			●	●	●	●	●	●

FEATURES	TVCS	CONTROL MANAGER						
	1.84	2.0	2.1	2.5	3.0 ENT	3.0 STD	3.5 ENT	3.5 STD
Outbreak Commander / Outbreak Prevention Services (OPS)			●	●	●	●	●	●
Passive Support for 3rd Party Product	●				●		●	
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 MCP agents							●	●
User Manager			●	●	●	●	●	●
Vulnerability Assessment					●	●	●	●

FEATURES	TVCS	CONTROL MANAGER						
	1.84	2.0	2.1	2.5	3.0 ENT	3.0 STD	3.5 ENT	3.5 STD
Work-hour control		●	●	●	●	●	●	●

Index

Symbols

"Log on as batch job" policy 6-60

A

access
  System settings 6-57
access rights
  Configure 6-11
  Edit Directory 6-12
  Execute 6-11
  setting 6-11
  View 6-11
activating
  Control Manager 3-13, 3-32–3-33
  Damage Cleanup Services 3-13–3-14
  Outbreak Prevention Services 3-13–3-14
  services 3-13
  Vulnerability Assessment 3-13–3-14, 9-29
activating Control Manager 3-34
Activation Code 3-34
Activation Codes 3-13
Active Directory
  see AD
Active Directory users
  importing 6-16
AD
adding
  user accounts 6-12
  user groups 6-20
address, checklist A-1
Administrator's Guide i-ix
  about i-x
AG. See Administrator's Guide
agent 4-5
  Control Manager
    installation 4-14
    setup program *See RemoteInstall.exe*
  installation 4-5
    checklist A-4
    programs 4-6
  InterScan Messaging Security Suite 4-6
  package *See RemoteInstall.xml*
  Trend VCS
    installation 4-22
    setup program. *See CMAgentsetup.exe*
Agent Migration Tool 10-2
  migrating agents 10-2
  migration list 10-2
AgentMigrateTool.exe. See Agent Migration Tool
agents
  installation tool 4-5
  installing 4-5
  installing Control Manager 4-1
  NetScreen Firewall 4-37
  obtaining packages 4-7
  obtaining required files 4-6
  preparing for installation 4-3
  remote installation 4-4
  removing Windows-based 11-2
  verifying successful installation 4-39
audience i-xi
Automatic Deployment
  configuring 6-45
automatic deployment settings
  Scheduled Download 6-55

B

back up. See backing up Control Manager 2.5/3.0 information
baseline security 9-28

C

calling CasTool.exe 10-3
cascading management structure
  child servers 6-27
  feature comparison 6-27
  parent server 6-27
Cascading Management Structure Tool 10-2
  commands 10-3
    /c 10-4
    /d 10-5
    /f 10-4
    /n 10-3
    /p 10-3
    /s 10-5
cascading structure tree tabs 6-28
CasTool.exe

commands 8-46
CasTool.exe commands 10-3
CasTool.exe. See Cascading Management Structure Tool
CCGI *See Common CGI*
checklist
agent installation A-4
ports A-3
server address A-1
child server 8-44
child servers
configuring 6-28
managing 6-27, 8-42
registering 6-30, 8-45
tab 6-28
unregistering 6-31, 8-45
client logs 7-22
cluster node 1-6
CMAgentSetup.exe 4-5, 4-23
CMWebCfg.bat 10-6
CMWebCfg.bat. See Web Server and Port Configuration Tool
command polling
MCP 2-23
command prompt
Common CGI, stopping service from 11-11
Control Manager, stopping service from 11-7
Trend Micro Management Infrastructure, stopping service from 11-10
Command Tracking 7-4
query and view commands 7-6
Common CGI
command prompt, stopping service from 11-11
location, files 11-11
registry key 11-11
remove 11-10
communication
one-way 1-6
parent-child server 8-44
two-way 1-6, 8-21
communication security i-iv
comparison
cascading management structure 6-27
Enterprise edition and Standard edition 1-7
compatible
antivirus and content security products 2-11
components
downloading 6-32
configuration
Web server 2-29
configuring 6-44, 6-53
child servers 6-28
managed products 8-26
Manual Download and Automatic Deployment settings 6-45
MCP two-way communication 8-19
Outbreak Prevention Mode download settings 9-16
Scheduled Download
automatic deployment settings 6-55
Scheduled Download Exceptions 6-46
Scheduled Download Settings 6-54
Scheduled Downloads 6-47
System Settings 6-56
user accounts 3-32, 6-8
Vulnerability Assessment 9-30
Control Manager 1-1
accounts 6-8
activating 3-13, 3-32–3-34
Administrator's Guide i-ix
agent 1-10
installation 4-14
antivirus and content security components 6-32
architecture 1-9
basic features 1-2
child servers 8-42
command prompt, stopping service from 11-7
compatible antivirus and content security products 2-11
configuring accounts 6-8
installation steps 3-9
installing 3-1, 3-10
installing agents 4-1, 4-3, 4-5
latest documentation i-ix
mail server 1-9
managed product 6-23
management console 6-2
manually removing 11-6
MCP 1-9
migrating database 5-16

new features in version 3.0 1-7
notifications 7-13
PDF documentation i-x
preparing for agent installation 4-3
registering 3-13, 3-32–3-33
remove manually 11-7
removing overview 11-1
removing server 11-2
removing Windows-based agent 11-2
report server 1-9
report types 7-30
reports 7-30
security levels 3-17, 3-20
server 1-9
SQL database 1-9
supported operating systems 2-9
system requirements 3-2
testing pilot deployment 2-13
Trend Micro Infrastructure 1-10
understanding remote installation 4-4
verifying agent installation 4-39
verifying installation 3-31
Web server 1-9
Web-based management console 1-10
Control Manager 2.5x agent migration flow 5-13
Control Manager 3.0
service pack i-viii
Control Manager agent for NetScreen Firewall 4-37
Certificate Name 4-37
determine Certificate Name 4-37
installing the agent 4-38
Control Manager agents 4-2
supported operating systems 2-10
Control Manager antivirus and content security components
Anti-spam rules 6-32, 6-34
Engines 6-32, 6-35
Pattern files/Cleanup templates 6-32–6-33
convention
document i-xi
convert
full version 3-34
creating
folders 8-34
tasks 9-46
user groups 6-20
users 6-12
customizing
notification messages 7-11

D

Damage Cleanup Services
activating 3-13–3-14
data storage
plan 2-27
database
recommendations 2-28
deleting
user accounts 6-19
user groups 6-23
deployment
architecture and strategy 2-2
multiple-site 2-5
single-site 2-2
Directory Manager 6-26, 8-32
grouping managed products 6-26
disable notifications 7-14
disabling
user accounts 6-19
documentation i-ix
download components
manually 6-37
downloading and deploying components 6-32

E

E2EPublic.dat *See encryption key*
editing
Outbreak Prevention policies 9-13
tasks 9-50
user accounts 6-18
user groups 6-22
email 7-13
eManager
updating 2-26
enable notifications 7-14
enable Scheduled Component Downloads 6-47
enabling
HTTPS download 6-59
UNC download 6-60
encryption key

agent, installation 4-22
obtaining 4-7
obtaining the 4-7
purpose 4-7
Enterprise edition
features 1-7
Enterprise Protection Strategy 9-3
evaluating existing policies 9-19
Event Center 7-9
Alert 7-9
Damage Cleanup Services 7-9
Outbreak Prevention Services 7-9
Unusual 7-10
Update 7-9

F

firewall traversal support 1-4
flow
migrating Control Manager 2.5x agent 5-13
migrating MCP agents 5-13
migrating Trend VCS 1.8x agent 5-12
folders
creating 8-34
moving 8-34
renaming 8-34
full version
convert 3-34

G

generating on-demand scheduled reports 7-45
global reports 7-30

H

Header menu 6-3
heartbeat
MCP 2-23
TMI 2-18
HTTPS download
enabling 6-59

I

IIS Restoration Tool 10-5
using SetupPatch.exe 10-6
importing
Active Directory users 6-16
initializing CasTool.exe. See calling CasTool.exe
installation i-x
agent
Control Manager 4-14
InterScan Messaging Security Suite 5.1 4-27
flow 2-9
Trend VCS agent 4-22
Installation Guide i-ix
installation steps
Control Manager 3-9
installing
agents 4-5
Control Manager 3-1, 3-10
Control Manager agents 4-1
MCP agents 4-2
steps 3-9
Trend VCS agents 4-11
verifying Control Manager server 3-31
Interscan
updating 2-25

K

Knowledge Base i-ix
URL i-ix

L

local reports 7-30
location
Common CGI files 11-11
Microsoft Data Engine files 11-12
Trend Micro Management Infrastructure files 11-10
logs 7-22
traffic 2-22

M

Main menu 6-3
managed products 6-23
configuring 6-23, 8-26
default folder 6-25
issue tasks 8-27
moving 8-34
recoving 8-29
renaming 8-34
searching for 8-31
support i-vii
tabs 6-26

using the Product Directory 6-23
viewing logs 8-28
viewing status 8-25
Management Communication Protocol
see MCP
management console
access 6-5
access HTTPS 6-7
accessing locally 6-5
accessing remotely 6-5
assigning HTTPS 6-5
function-locking mechanism 6-4
managing
child servers 8-42
third party products 8-39
manual
remove
Common CGI 11-10
MSDE 11-11
Trend Management Infrastructure 11-9
Manual Assessment 9-39
Manual Download 6-44
manual download
configuring settings 6-44
manual download settings 6-44
Manual Vulnerability Assessment Tool 9-40
manually
remove Control Manager 11-7
manually download components 6-37
manually uninstalling 11-6
MCP 1-9
command polling 2-23
configuring two-way communication 8-19
heartbeat 2-23
migration flow 5-13
policies 2-23
understanding 1-3
MCP agents
installing 4-2
MCP benefits
HTTPS support 1-5
NAT and firewall traversal 1-4
one-way and two-way communication 1-5
reduced network loading and package size 1-3
menu
Header 6-3
Main 6-3
MIB file
Control Manager 10-7
NVW 1.x SNMPv2 10-7
NVW Enforcer SNMPv2 10-8
MIBs browser 7-13
Microsoft
Data Engine
location, files 11-12
migrating 5-8
Control Manager 2.5x agent migration flow 5-13
Control Manager SQL 2000 5-17
database 5-16
different servers/agents 5-11
generate a migration list 5-16
MCP agents 5-13
phased upgrade 5-9
rapid upgrade 5-8
scenarios 5-11
single-server migration 5-11
steps 5-13
strategy 5-8
Trend VCS 1.8x agent migration flow 5-12
Trend VCS, Control Manager 2.x, and MCP Agents 5-14
migration list 5-16
minimum system requirements 3-2
monitoring
security level 7-2
system information 7-2
monitoring the Control Manager environment 7-2
moving
folders 8-34
managed products 8-34
MSDE 2000 i-viii
multiple-site deployment
understanding 2-5

N

NAT traversal support 1-4
NetScreen Firewall 4-37, 8-39
network traffic
sources 2-22
network traffic plan 2-17

notification messages
customizing 7-11
notifications 7-13
configure recipients 7-16
configuring 7-15
enabling or disabling 7-14
special virus alert settings 7-19
test notification delivery 7-16
virus outbreak alert settings 7-18
NVW 1.x Rescue Utility 10-8
NVW System Log Viewer 10-8

O

obtaining
agent packages 4-7
encryption key 4-7
ODBC
settings, Control Manager 11-11
OfficeScan
Trend VCS agent for 4-23
updating 2-26
on-demand scheduled reports 7-45
one-way communication 1-5–1-6
online help i-ix
operating systems
supported 2-9
Outbreak Prevention Mode 9-9
configuring download settings 9-16
setting automatic 9-14
starting 9-12
stopping 9-16
viewing history 9-17
Outbreak Prevention policies
editing 9-13
policies
Outbreak Prevention 9-10
updating 9-11
Outbreak Prevention Services i-viii, 9-6
accessing 9-10
activating 3-13–3-14, 9-7
benefits 9-7
viewing status 9-8
outbreaks
identify the source 9-18

P

pager 7-13
parent and child server feature comparison 6-27
parent server 6-27, 8-44
performing
Vulnerability Assessment 9-26
phased upgrade 5-9
pilot deployment
testing 2-13
policies
MCP 2-23
TMI 2-23
port
checklist A-3
post installation i-x
preface i-i
pre-installation i-x
preparing
Control Manager agent installation 4-3
Product Directory 8-22
deploying components 8-25
Product Directory tabs 6-26
product registration
traffic 2-24
profiles. See report profiles
proxy server
communicating with Trend VCS agents 3-25
connecting to the Internet 3-24
public encryption key 4-7

Q

querying commands 7-6

R

rapid upgrade 5-8
readme file i-ix
recommendations
database 2-28
recommended system requirements 3-3
recoving
managed products 8-29
register online 3-13
registering
child servers 8-45
Control Manager 3-13, 3-32–3-33

registering a child server 6-30
Registration Key 3-14, 3-34
registry key
  Common CGI 11-11
  Microsoft Data Engine 11-13
  Trend Micro Management Infrastructure 11-10
Remote Agent Setup tool 4-14
RemoteInstall.exe 4-5, 4-14
RemoteInstall.xml 4-9
remove
  manual
    Control Manager 11-7
    Microsoft Data Engine 11-11
    Trend Management Infrastructure 11-9
removing
  Control Manager manually 11-6
  Control Manager server 11-2
  Control Manager Windows-based agent 11-2
renaming
  folders 8-34
  managed products 8-34
renew product maintenance 3-35
report templates 7-31
reports 7-30
  global 7-30
  local 7-30
  on-demand scheduled 7-45
  report profiles 7-37
    ActiveX 7-37
    Contents 7-38
    creating 7-37
    Frequency 7-40
    PDF 7-37
    Recipient 7-42
    RPT 7-37
    RTF 7-37
    Targets 7-39
  viewing generated reports 7-46
resolving
  vulnerabilities 9-27
re-verification frequency
  changing 8-30
rolling back
  to Control Manager 2.5 server 5-7
  to Trend VCS 1.8x server 5-7
root account 6-10
root-level share 4-24
running SetupPatch.exe. See using SetupPatch.exe

S

ScanMail
  updating 2-25
Scheduled Download
  configuring
    automatic deployment settings 6-55
Scheduled Download Exceptions
  configuring 6-46
Scheduled Download Frequency
  configuring 6-53
Scheduled Download Schedule
  configuring 6-53
Scheduled Download Schedule and Frequency 6-53
Scheduled Download Settings
  configuring settings 6-54
Scheduled Downloads 6-47
  configuring 6-47
scheduled reports 7-45
searching
  managed products 8-31
security levels 3-19
server
  address, checklist A-1
server distribution plan 2-15
server logs 7-22
ServerProtect
  updating 2-26
setting
  access rights 6-11
SetupPatch.exe. See IIS Restoration Tool
single sign-on
  see SSO
single-site deployment
  undertsanding 2-2
sizing recommendations 3-4
Small Network Management Protocol. See SNMP
SNMP 7-13
SolutionBank-see Knowledge Base i-ix
spyware/grayware
  detection and cleanup i-iii
  special alert settings 7-18

SQL
  Service Manager 11-12
SSO 1-6
Standard edition
  features 1-7
starting
  Outbreak Prevention Mode 9-12
stopping
  Outbreak Prevention Mode 9-16
system requirements 3-2
  minimum 3-2
  recommendations 3-4
  recommended 3-3
System Settings
  configuring 6-56
System settings
  access 6-57

T

tabs
  cascading structure tree 6-28
  Product Directory 6-26
task
  creating 9-46
  editing 9-50
Temp 8-36
third party products
  managing 8-39
TMI
  heartbeat 2-18
  policies 2-23
TMI *See Trend Micro Management Infrastructure*
tool
  AgentMigrateTool.exe 10-2
  CasTool.exe 10-2
  CMWebCfg.bat 10-6
  Control Manager MIB file 10-7
  NVW 1.x Rescue Utility 10-8
  NVW 1.x SNMPv2 MIB file 10-7
  NVW Enforcer SNMPv2 MIB file 10-8
  NVW System Log Viewer 10-8
  SetupPatch.exe 10-5
traffic, network 2-17
traversal support
  NAT and firewall 1-4
Trend Micro Management Infrastructure
  command prompt, stopping service from 11-10
  location, files 11-10
  registry key 11-10
  remove 11-9
Trend Micro services 9-2
Trend VCS
  agent
    installation 4-22
Trend VCS 1.8x agent migration flow 5-12
Trend VCS agents 4-2
  installing 4-11
Trigger Application 7-13
two-way communication 1-5–1-6, 8-21

U

UNC download
  enabling 6-60
understanding
  Control Manager remote installation 4-4
  multiple-site deployment 2-5
  single-site deployment 2-2
unregistering
  child servers 8-45
unregistering a child server 6-31
Update Manager 6-32
updates
  deploying 2-24
updating
  eManager 2-26
  eManager products 2-21
  OfficeScan Corporate Edition 2-21
  OfficeScan Corporate Edition and ServerProtect 2-26
  Outbreak Prevention policies 9-11
  ScanMail and InterScan products 2-20
  ScanMail and Interscan products 2-25
  ServerProtect 2-21
upgrading 5-2
  backing up Control Manager 2.5 information 5-4
  considerations 5-2
  Control Manager 2.5 servers 5-3
  Trend VCS 1.8x servers 5-3
URLs
  Knowledge Base i-ix

user account
Access 6-8
user accounts
adding 6-12
configuring 3-32
deleting 6-19
disabling 6-19
editing 6-18
user groups
adding 6-20
deleting 6-23
editing 6-22
User Manager 6-10
users
adding accounts 6-12
adding groups 6-20
deleting accounts 6-19
deleting groups 6-23
disabling accounts 6-19
editing accounts 6-18
editing groups 6-22

V

verifying
agent installation 4-39
communication method between MCP and Control Manager
MCP
verifying communication method 8-21
Control Manager server installation 3-31
version
agent package 4-10
viewing
managed products logs 8-28
managed products status 8-25
Outbreak Prevention Mode history 9-17
Outbreak Prevention Services status 9-8
viewing commands 7-6
viewing generated reports 7-46
vulnerabilities
resolving 9-27
Vulnerability Assessment 9-22
activating 3-13–3-14, 9-29
configuring 9-30
performing 9-26
running a task 9-31

W

Web server
configuration 2-29
plan 2-29
who should read this document
audience i-xi
Windows event log 7-13
World Virus Tracking 3-15
World Virus Tracking Program 9-5