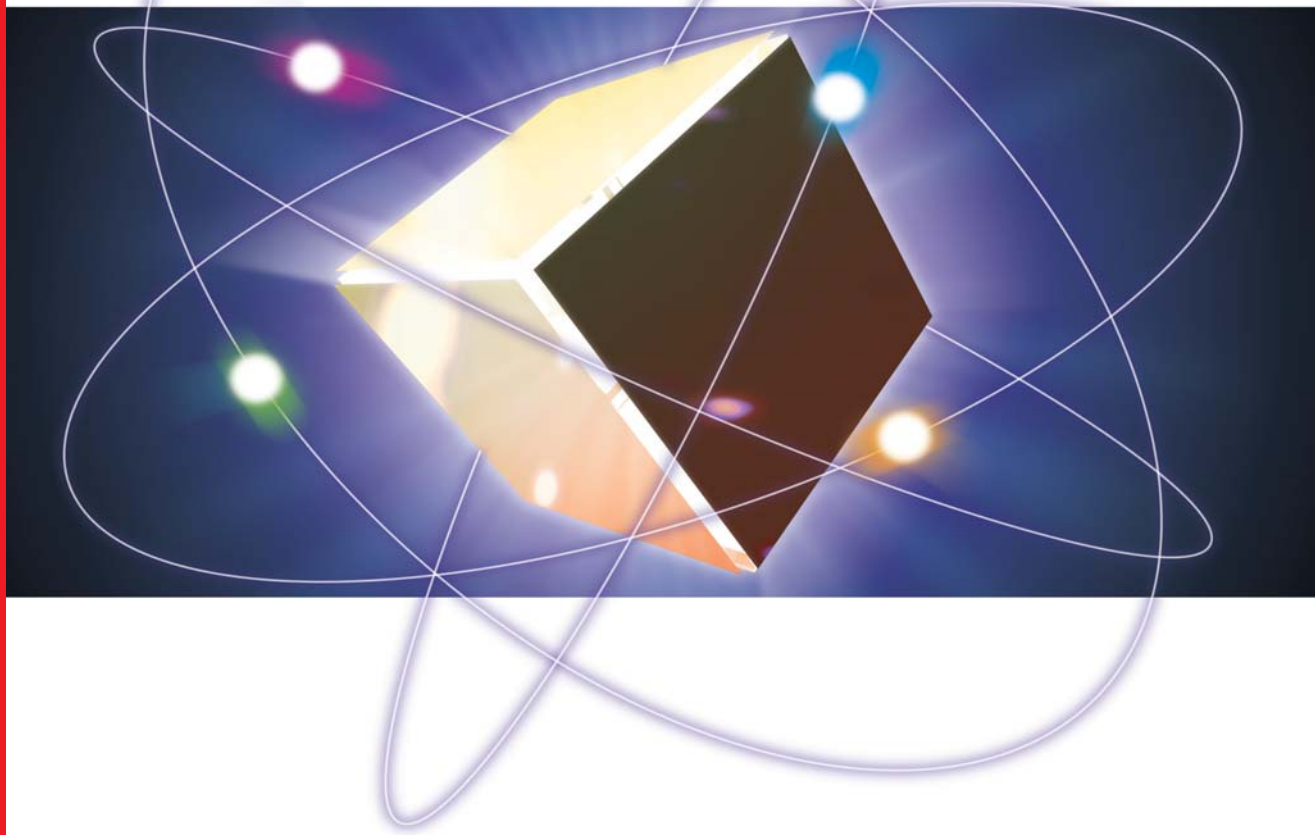
TREND MICRO
Control Manager™ 3

Enterprise Virus Outbreak and Content Security Management

Getting Started Guide



TREND MICRO™

Document Part No. TMEM31864/40414

Release Date: April 2004

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 10-2 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

Audience ii
Document Conventions ii

Chapter 1: Introducing Trend Micro Control Manager™ 3.0

Control Manager Basic Features 1-2
What's New in Version 3.0 1-3
Standard and Enterprise editions 1-4
Control Manager 3.0 Standard and Enterprise Editions 1-7
Control Manager Architecture 1-8

Chapter 2: Planning and Implementing the Control Manager Deployment

Supported Operating Systems 2-2
Server Distribution Plan 2-2
Network Traffic Plan 2-3
Data Storage Plan 2-7
Administration Plan 2-8
Web Server Configuration 2-9
Identify Deployment Architecture and Strategy 2-10
Test Control Manager Deployment at one Location 2-16

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

System requirements 3-2
Installing a Control Manager server 3-6
Installing Control Manager agents 3-25
Verifying successful installations 3-48
Post-installation configuration 3-50
Registering and activating your software 3-51

Chapter 4: Upgrading Servers or Migrating Agents to Control Manager 3.0

Upgrading to Control Manager 3.0 4-2
Planning Trend VCS or Control Manager agent migration 4-8
Migrate the Control Manager database 4-14

Chapter 5: Getting Started with Control Manager

Use the management console 5-2
Configure Control Manager user accounts and groups 5-7
Administer managed products 5-16
Manage child servers 5-19
Download and deploy new components 5-25
Monitor the Control Manager environment 5-37

Chapter 6: Using Trend Micro Damage Cleanup Services™

Features and Benefits 6-3
Activating Damage Cleanup Services 6-4
Accessing Damage Cleanup Services 6-5
Downloading Updates 6-6
Configuring Damage Cleanup Services 6-7
  Using the manual Damage Cleanup tool 6-15
Checking the status of a current task 6-16
Using the damage cleanup history (task logs) 6-16

Chapter 7: Introducing Trend Micro Vulnerability Assessment™

What is Vulnerability Assessment? 7-2
What Are the Benefits and Capabilities
of Vulnerability Assessment? 7-3
Activating Vulnerability Assessment 7-4
Accessing Vulnerability Assessment 7-5
Downloading Updates 7-5
Configuring Vulnerability Assessment 7-6
Using Vulnerability Assessment 7-6
  Creating and Running Tasks 7-7
  Understanding Enforcement 7-9
  Managing Vulnerability Assessment tasks 7-12
  Using Current Task 7-20

Setting Global Enforcement and Exceptions 7-22

Chapter 8: Using Tools

Agent Migration Tool (AgentMigrateTool.exe) 8-2
Cascading Management Structure Tool (CasTool.exe) 8-2
IIS Restoration Tool (SetupPatch.exe) 8-5
Web Server and Port Configuration Tool (CMWebCfg.bat) 8-6

Chapter 9: Removing Trend Micro Control Manager

Remove a Control Manager server 9-2
Remove a Windows-based Control Manager agent 9-2
Manually removing Control Manager 9-6

Chapter 10: Getting Support

Before Contacting Technical Support 10-2
Contacting Technical Support 10-2
TrendLabs™ 10-3
Other Useful Resources 10-3

Appendix A: System Checklists

Server address checklist A-1
Ports checklist A-3
Agent installation checklist A-4

Appendix B: Trend Virus Control System and Trend Micro Control Manager Feature Comparison

Index

Preface

This Getting Started Guide introduces Trend Micro Control Manager™ 3.0, guides you through the installation planning and steps, and then walks you through the basics of configuring Control Manager to function according your needs.

It provides the following information:

- An overview of the product and description of all new features in this release (*Introducing Trend Micro Control Manager™ 3.0* starting on page 1-1)
- Recommendations for implementing and deploying Control Manager 3.0 (*Planning and Implementing the Control Manager Deployment* starting on page 2-1)
- Step-by-step instructions on how to install Control Manager 3.0 (*Installing Trend Micro Control Manager for the First Time* starting on page 3-1)
- Recommendations for migrating agents and databases to Control Manager 3.0 (*Upgrading Servers or Migrating Agents to Control Manager 3.0* starting on page 4-1)
- Procedures to get started with Control Manager (*Getting Started with Control Manager* starting on page 5-1)
- Instructions on how to remove Control Manager (*Removing Trend Micro Control Manager* starting on page 9-1)
- Details on the available Control Manager 3.0 utilities (*Using Tools* starting on page 8-1)

- Instructions on how to get more information (*Getting Support* starting on page 10-1)

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
	Represents Control Manager 3.0 Enterprise edition topics
Note: or 	Provides configuration notes or recommendations

TABLE 1. Conventions used in Control Manager Documentation

Chapter 1

Introducing Trend Micro Control Manager™ 3.0

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
- *What's New in Version 3.0* on page 1-3
- *Control Manager 3.0 Standard and Enterprise Editions* on page 1-7
- *Control Manager Architecture* on page 1-8

Control Manager Basic Features

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

Major Control Manager features include:

- Centralized configuration - using the Product Directory and cascading management structure, these functions allow you to coordinate virus-response and content security efforts from a single management console

  This helps ensure consistent enforcement of your organization's virus and content security policies.
- Proactive outbreak prevention - with Outbreak Prevention Services (OPS), take proactive steps to secure your network against an emerging virus outbreak
- Secure communication infrastructure - Control Manager uses a communications infrastructure built on the Secure Socket Layer (SSL) protocol

  Depending on the security settings used, Control Manager can encrypt messages or encrypt them with authentication.
- Secure configuration and component download - these features allow you to configure secure management console access and component download
- Task delegation - system administrators can give personalized accounts with customized privileges to Control Manager management console users

  User accounts define what the user can see and do on a Control Manager network. Track account usage via user logs.
- Command Tracking - this feature allows you to monitor all commands executed using the Control Manager management console

  Command Tracking is useful for determining whether Control Manager has successfully performed long-duration commands, like virus pattern update and deployment.
- On-demand product control - control managed products in real-time

  Control Manager immediately sends configuration modifications made on the management console to the managed products. System administrators can run manual scans from the management console. This command system is indispensable during a virus outbreak.

- Centralized update control - update virus patterns, anti-spam rules, scan engines, and other antivirus or content security components to help ensure that all managed
- Centralized reporting - get an overview of the antivirus and content security product performance using comprehensive logs and reports

  Control Manager collects logs from all its managed products; you no longer need to check the logs of each individual product.

What's New in Version 3.0

Trend Micro Control Manager 3.0 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 3.0:

- Standard and Enterprise editions
- Control of multiple Control Manager servers from a single management console
- Agent-free Damage Cleanup Services
- System vulnerability scanning using Vulnerability Assessment
- Prevention of virus and other malware outbreak using Outbreak Prevention Services
- Microsoft Data Engine (MSDE) 2000 support for Control Manager database
- Support for Trend Micro Online Registration system
- HTTPS management console and ActiveUpdate
- Enhanced Update Manager options
- New report templates to support InterScan Messaging Security Suite and OfficeScan Corporate Edition information
- New Event Center events
- Support for MSN Messenger notification
- Latest component version update via TrendLabs Message Board

Standard and Enterprise editions

Control Manager is now available in Standard and Enterprise editions to better satisfy the needs of different enterprises.

The Standard edition provides powerful management and configuration features that allow you to manage your corporate antivirus and content security.

The Enterprise edition is for large enterprises and xSPs. This edition adds a variety of advanced features to the Standard edition - such as cascading console support and reporting functions.

Control of multiple Control Manager servers from a single management console

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

Agent-free Damage Cleanup Services

Damage Cleanup Services (DCS) is a comprehensive cleaning service that offers infection assessment and system repair for malicious remnant such as Worms and Trojans. The service provides system administrators an easy approach for system cleaning without the use of any software locally installed on the client machines.

System vulnerability scanning using Vulnerability Assessment

Vulnerability Assessment is a service that assesses network security risks. It scans for system vulnerabilities that are associated with known virus and malware attacks and recommends actions to take to eliminate the vulnerabilities.

Prevention of virus and other malware outbreak using Outbreak Prevention Services

Outbreak Prevention Services (OPS) delivers notification of new threats as well as 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.

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.

Support for Trend Micro Online Registration system

Use a Registration Key and an Activation Code to register Control Manager to the Trend Micro Online Registration system.

HTTPS management console and ActiveUpdate

Use HyperText Transport Protocol Secure (HTTPS) to access the Control Manager Management Console and download updates from Trend Micro ActiveUpdate server.

Enhanced Update Manager options

Update Manager now includes the following:

- Separate downloads for update components (for example, virus patterns and anti-spam rules)
- Digital signature checking - by default, Control Manager implements this feature whenever it downloads components from the Trend Micro ActiveUpdate server
- UNC download - configure Manual or Scheduled download to get the latest antivirus or content security components from a shared folder located somewhere in your network (see *Enable UNC download* on page 5-31)

New report templates to support InterScan Messaging Security Suite and OfficeScan Corporate Edition information

The Enterprise edition provides the reporting functions. If you have InterScan Messaging Security Suite or OfficeScan registered as a managed product, Control Manager can generate reports with contents based on the following new report templates:

- Filter Events by Frequency Report
- Filter Events by Policy Report
- Spam Summary for Recipients Report
- Spam Summary for Domains Report
- OfficeScan Deployment Status
- OfficeScan Deployment Non Current

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 5-39).

Support for MSN Messenger notification

Control Manager 3.0 provides MSN Messenger notification to inform recipients of events that occur on the Control Manager network. Specify the recipient's MSN Messenger passport when creating a new user. The user can then receive Control Manager notifications via MSN Messenger.

Latest component version update via 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.

Control Manager 3.0 Standard and Enterprise Editions

There are two versions of Control Manager:

- 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 - such as 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
HTTPS ActiveUpdate	Yes	Yes
Trend Micro Network VirusWall 1200 and InterScan Web Security Service integration	Yes	Yes
MSN Messenger notification	Yes	Yes

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

The Control Manager Standard edition provides management of antivirus and content security products without the reporting feature.

The Control Manager Enterprise edition features cascading management structure that 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. With the exception of the Feature List Comparison, the Control Manager online help and Getting Started Guide do not distinguish between the two versions.

Control Manager Architecture

Trend Micro Control Manager is a management solution that provides control of Trend Micro products and services, and third-party antivirus and content security products from a central location. This application simplifies the administration of a corporate virus and content security policy.

Control Manager uses the following components:

- **Control Manager server** - acts as a repository for all data collected from the agents. It can be a Standard or Enterprise edition server. A Control Manager server includes the following features:
  - An SQL **database** that stores managed product configurations and logs

    Control Manager uses the Microsoft SQL Server database (`db_ControlManager.mdf`) to store data included in logs, Communicator schedule, managed product and child server information, user account, network environment, and notification settings.
  - A **Web server** that hosts the Control Manager **management console**
  - A **mail server** that delivers event **notifications** via email

    Control Manager can send notifications to individuals or groups of recipients about events that occur on the Control Manager network. Configure **Event Center** to send notifications through email, Windows event log, MSN Messenger, SNMP, pager, or any in-house/industry standard application used by your organization to send notification.
  - A **report server**, present only in the Enterprise edition, that generates antivirus and content security product reports

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

- **Trend Micro Infrastructure** - handles the Control Manager server interaction with managed products

  The Communicator, or the Message Routing Framework, is the communication backbone of the Control Manager system. It is a component of the Trend Micro Infrastructure (TMI). Communicators handle all communication between the Control Manager server and managed products. They interact with Control Manager agents to communicate to managed products.

- **Agent** - receives commands from the Control Manager server and sends status information and logs to the Control Manager server

  The Control Manager agent is an application installed on a managed product server that allows Control Manager to manage the product. Agents interact with the managed product and Communicator. An agent serves as the bridge between managed product and communicator. Hence, you must install agents on the same machine as managed products.

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

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

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:

- *Supported Operating Systems* on page 2-2
- *Server Distribution Plan* on page 2-2
- *Network Traffic Plan* on page 2-3
- *Data Storage Plan* on page 2-7
- *Administration Plan* on page 2-8
- *Web Server Configuration* on page 2-9
- *Identify Deployment Architecture and Strategy* on page 2-10
- *Test Control Manager Deployment at one Location* on page 2-16

Supported Operating Systems

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

Control Manager server

- Microsoft™ Windows™ 2000 Server
- Windows 2000 Advanced Server
- Windows NT 4.0 + SP6a or later
- Windows 2003, 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	Solaris™ v2.6, 2.7, 2.8 AIX™ Red Hat™ Linux 6.2, 7.1, 7.2 Turbolinux™ 6.5, 7.0 SuSE™ Linux 6.3, 7.2, 7.3 AS/400 OS390 Others: Linux 6.x Kernel

Server Distribution Plan

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

Note: Now that Control Manager supports multiple user accounts, segregation that was necessary for Trend Virus Control System (Trend VCS) is no longer needed. For information on merging multiple Trend VCS servers under a single Control Manager server, see *Migration scenarios Trend VCS 1.8x or Control Manager 2.5x agents* on page 4-9.

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

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

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

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

For information on the traffic that a Control Manager network generates, see *Network Traffic Plan* on page 2-3.

Network Traffic Plan

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

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

Sources of network traffic

The following Control Manager sources generate network traffic:

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

Log traffic

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

Log	Contains Information About
Virus	Detected viruses and other malware.
Security	Violations reported by content security products.
Web Security	Violations reported by web security products.
Event	Miscellaneous events that are not included in the aforementioned logs (for example, component updates, generic security violations, etc.).
Status	The environment of a managed product. The Status tab of the Product Directory displays this information.
Network Virus	Outbreaks occurred on networks.
Network Outbreak Monitor	Virus detected in network packets.

Trend Micro Management Infrastructure policies

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

- Communicator Heartbeat
- Work-hour policy

Communicator

The Communicator, the commercial name for the Message Routing Framework of TMI, polls the Control Manager server at regular intervals. This ensures that the Control Manager console displays the latest information, and that the connection between the managed product and the Control Manager server is functional.

Work-hour policy

The work-hour policy defines when a Communicator sends information to the Control Manager server. Use the Communication Scheduler to define this policy; a user can set three periods of inactivity – also called 'off-hour' periods.

Two types of information, however, do not follow the Communicator Scheduler:

- Emergency messages
- Prohibited messages

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

Product registration traffic

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

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

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

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

Traffic frequency

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

- Logs
- Trend Micro Management Infrastructure policies

Logs

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

Trend Micro Management Infrastructure (TMI) policies

By default, TMI sends heartbeat messages every sixty minutes. This can be adjusted to anywhere from 5 to 480 minutes (8 hours). When choosing a Heartbeat setting, choose a balance between the need to display the latest Communicator status information and the need to manage system resources.

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

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

For example, if a connection problem with a Communicator is resolved between heartbeats, it then becomes possible to communicate with a Communicator–even if its status appears as "Inactive" or "Abnormal".

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

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

Data Storage Plan

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

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

Database recommendations

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

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

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

ODBC drivers

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

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

Authentication

Control Manager uses mixed-mode authentication for accessing the SQL database, not Windows authentication.

Administration Plan

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

Follow one of these administration models:

- **Centralized management**

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

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

- **Decentralized management**

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

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

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

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

Refer to *Group managed products using Directory Manager* on page 5-19 for details on how to group managed products.

Web Server Configuration

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

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

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

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

Where:

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

  ```
  Pattern/vsapi.zip
  ```

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

Identify Deployment Architecture and Strategy

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

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

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

- **Single-site deployment**

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

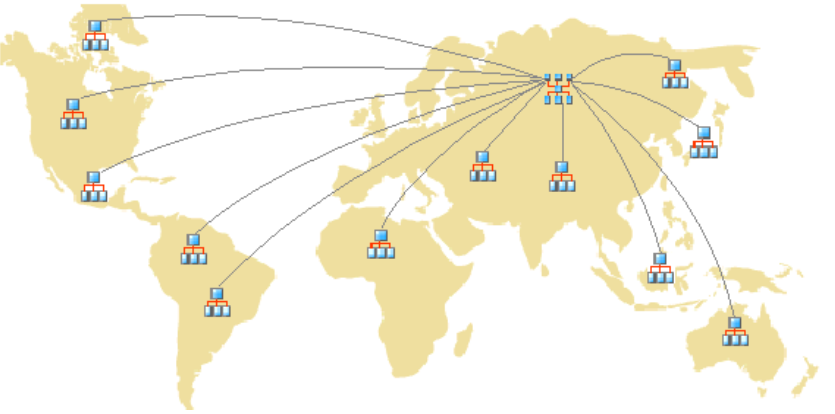


FIGURE 2-1. A single-server deployment using Enterprise Control Manager parent server and child servers.

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

- Determine the number of managed products and cascading structures

  Determine how many managed products and cascading structures you plan to manage with Control Manager. You will need this information to decide what kind and how many Control Manager servers you need to deploy, as

well as where to position these servers on your network to optimize communication and management.

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

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

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

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

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

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

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

  When selecting a server 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.

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.

- **Multiple-site deployment**

  Multiple-site deployment refers to distributing and managing Control Manager servers in an organization that has main offices in different geographical locations.

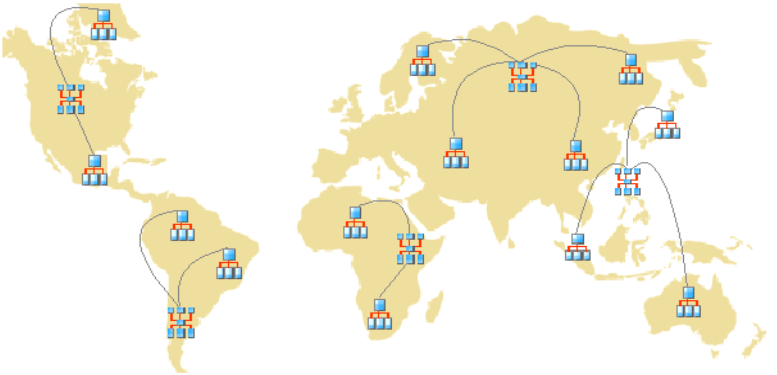


FIGURE 2-2. A multi-site deployment using multiple Enterprise Control Manager parent server and mixed child servers.

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

Specifically, you need to:

- Group managed products or child servers

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

- Company network and security policies

  If different access and sharing rights apply to the company network, group managed products and child servers according to company network and security policies.

- Organization and function

  Group managed products and child servers according to the company's organizational and functional division. For example, have two Control Manager servers that manage the production and testing groups.

- Geographical location

  Use geographical location as a grouping criterion if the location of the managed products and child servers affects the communication between the Control Manager server and its managed products or child servers.

- Administrative responsibility

  Group managed products and child servers according to system or security personnel assigned to them. This allows group configuration.

- Determine the number of sites

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

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

- Determine the number of managed products and child servers

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

- Plan for network traffic

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

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

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

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

Refer to *Network Traffic Plan* on page 2-3 for more information.

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

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

  Once you know the number of clients and the number of servers you need to install, decide 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 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 the majority of the managed products and child servers in an organization are located. The central office is sometimes referred to as "headquarters", "corporate office", or "corporate headquarters". A central office can have other smaller offices or branches (referred to as ’remote offices’ in this guide) in other locations.

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

- Remote office

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

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

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

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

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

Test Control Manager Deployment at one Location

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

Testing Control Manager at one location accomplishes the following:

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

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

A Control Manager test deployment consists of the following tasks:

- Preparing for the test deployment

  Complete the following activities during the preparation stage:

  a. Decide the Control Manager server and agent configuration for the test environment.

  b. Establish TCP/IP connectivity among all systems in a heterogeneous trial configuration.

  c. Verify bidirectional TCP/IP communications by sending a ping command to each agent system from the manager system and vice versa.

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

  e. Complete the System Checklists to be used for the test deployment.

- Selecting a test site

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

- Creating a rollback plan

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

- Beginning the test deployment

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

- Evaluating the test deployment

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

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

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 3-6
- *Installing Control Manager agents* on page 3-25
- *Verifying successful installations* on page 3-48
- *Post-installation configuration* on page 3-50
- *Registering and activating your software* on page 3-51

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.

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	300MB for Control Manager Standard Version 350MB for Control Manager Enterprise Version 300MB for MSDE 2000 (Optional)

TABLE 3-1. Control Manager server hardware system requirements

Software Specifications	Minimum Requirements
Operating system	Microsoft™ Windows™ Server 2003 Standard / Enterprise Edition, Microsoft Windows 2000 Server / Advanced Server with Service Pack 3, Microsoft Windows NT 4 with Service Pack 6a
Web server	Microsoft Internet Information Server (IIS) 4.0 or higher

TABLE 3-2. Control Manager server software system requirements

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

TABLE 3-2. Control Manager server software 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 are recommendations for the indicated network sizes for a single

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)
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	

Control Manager Server	Environment	Recommendation
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	
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

Control Manager server.

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

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 in the appendix 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 to be used 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: Register and activate the product and services

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

Step 3: Choose and configure database information

Step 4: Set up root account and configure proxy server

Step 5: Configure notification settings

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 3.0* on page 4-2.

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 4-8.

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

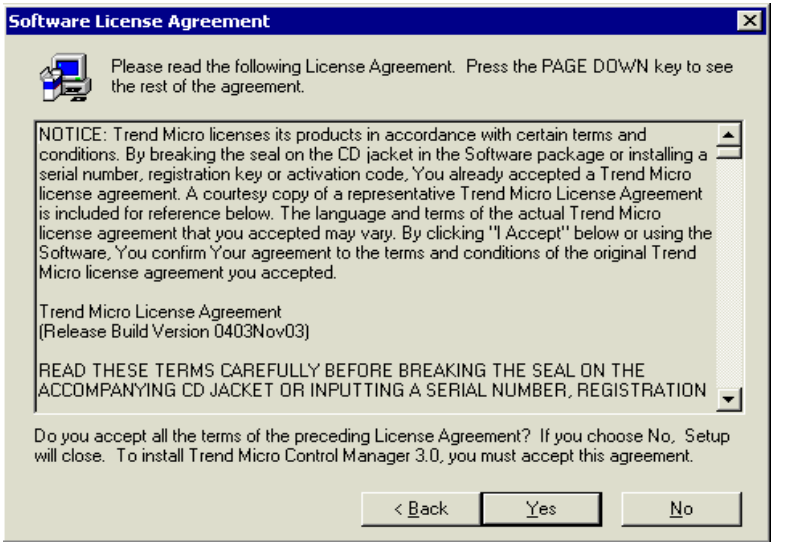


FIGURE 3-1. Choose Yes to agree with the License Agreement

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.

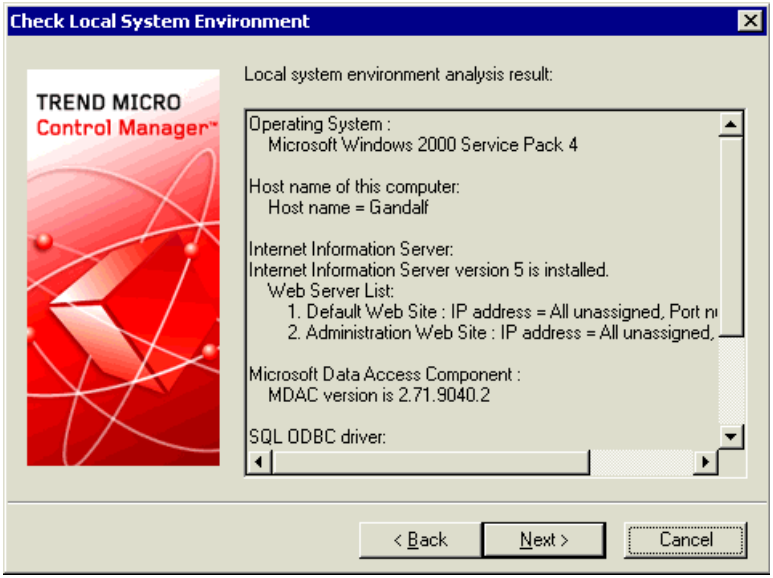


FIGURE 3-2. Displays local system environment information

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

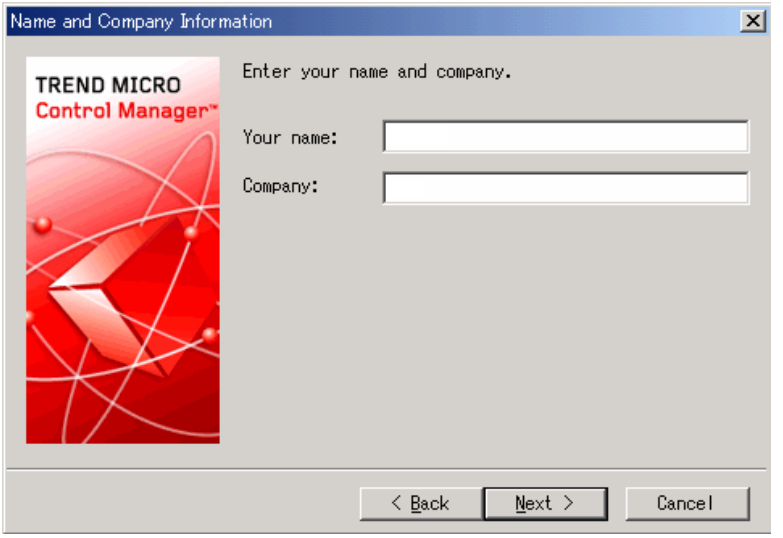


FIGURE 3-3. Enter your name and company

4. Type your name and company.
5. Click **Next**. The Product Activation screen (Step 1) appears.

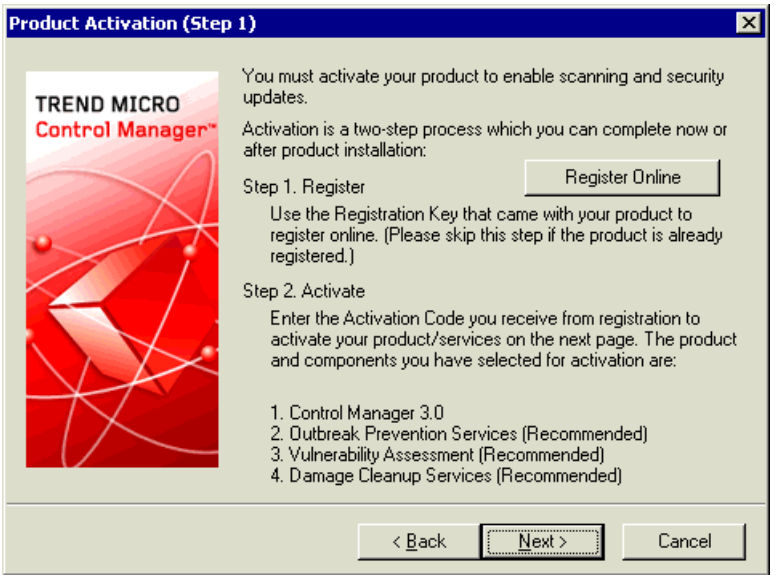


FIGURE 3-4. Register online to obtain an Activation Code

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.

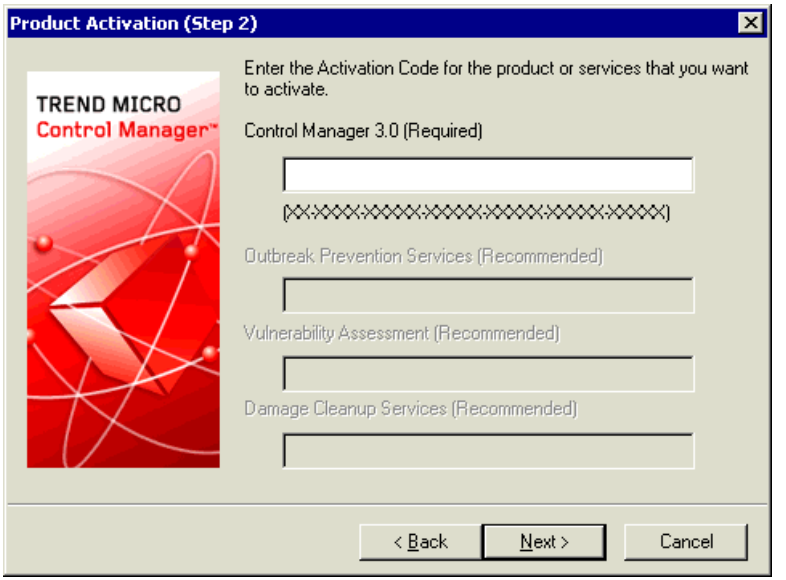


FIGURE 3-5. Enter the Activation Code to activate Control Manager and services

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.

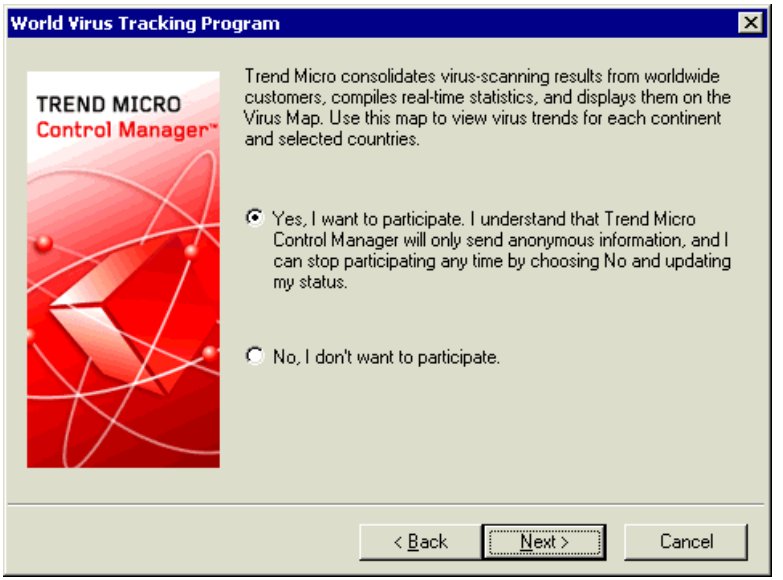


FIGURE 3-6. Participate in the World Virus Tracking Program

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**. 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) in predetermined folders in the Program files folder.

---

2. Click **Next**. The settings on the next screen define communication security and how the Control Manager network identifies your server.

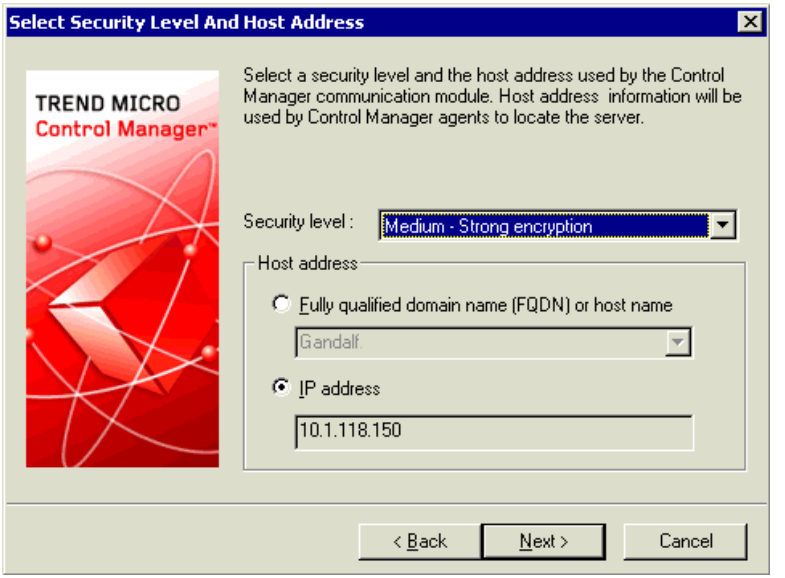


FIGURE 3-7. Select a security level

3. Select a **Security level** for Control Manager server and managed product communication. The options are Low, Medium, and High; the default setting is Medium.
4. Under **Host address**, define 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.

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

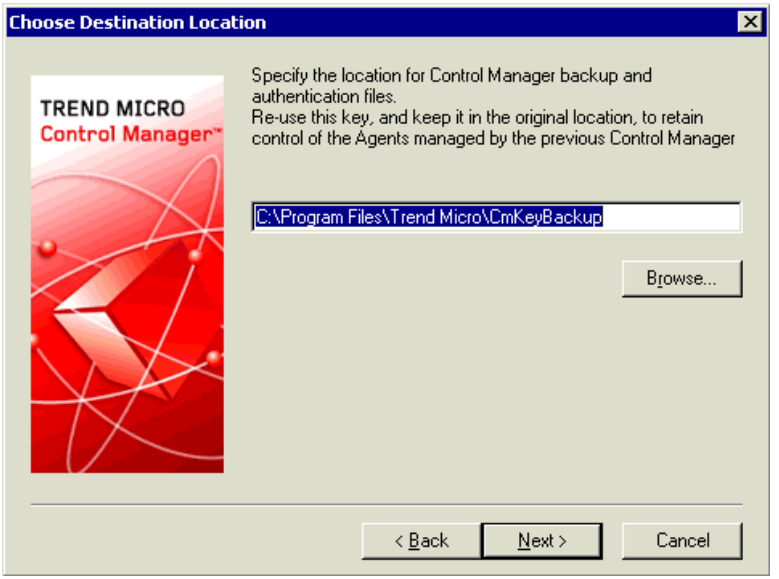


FIGURE 3-8. Specify location of Control Manager backup and authentication files

6. Specify the location of the Control Manager backup and authentication files (for more information see the *Control Manager 2.5 files that should be backed up* on page 4-4). Click **Browse** to specify an alternate location.
7. Click **Next**. The Specify Web Server Information screen appears.

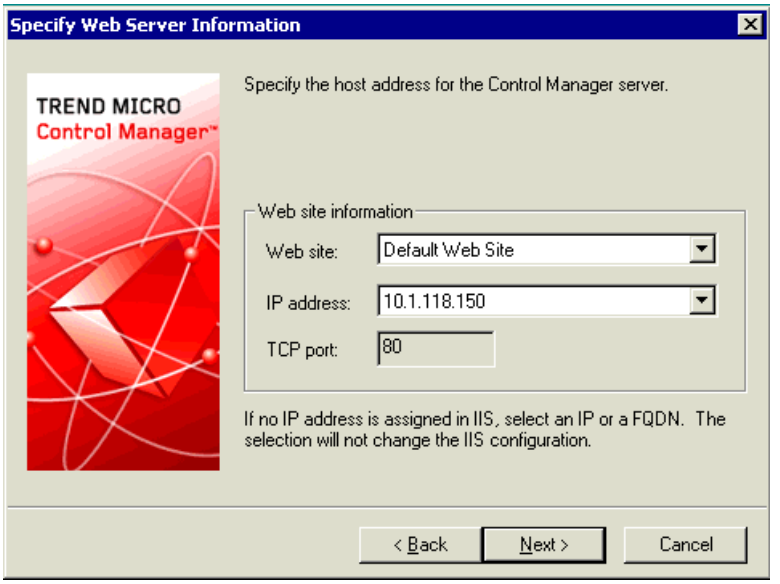


FIGURE 3-9. Specify Control Manager server host address

8. From the IP address list, select the IP address or FQDN/host name you want to use for the Control Manager Management Console.

Step 3: Choose and configure database information

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

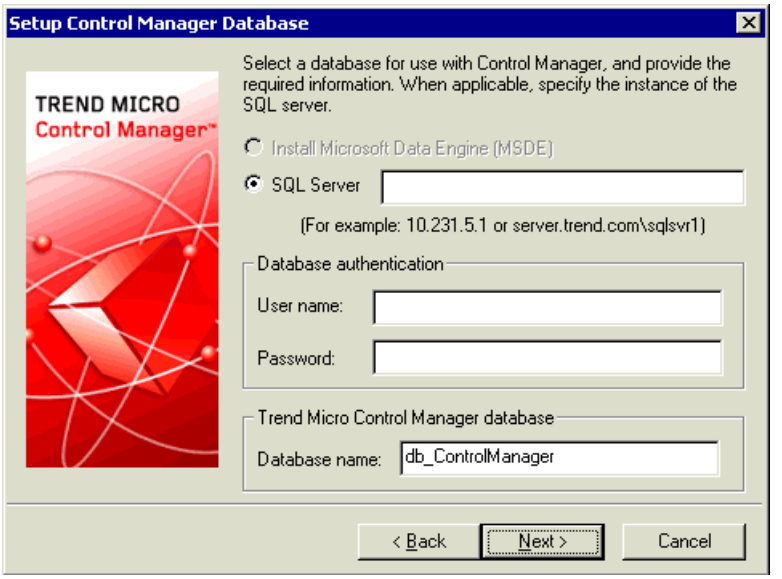


FIGURE 3-10. Choose the Control Manager database

2. Select a database to use with Control Manager.

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

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

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

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

If more than one instance of SQL server exists on a host server (this can be either the same server where you are installing Control Manager, or another server), you must specify the instance. For example: `your_sql_server.com/instance`

- **SQL Server Authentication** - provide credentials to access the SQL server. By default, the User name is "sa".

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

3. Under **Trend Micro Control Manager database**, provide a name for the Control Manager database. The default name is "db_ControlManager".
4. Click **Next** to create the required database. If the setup program detects an existing Control Manager database you have the following options:
   - **Append new records to existing database**- the Control Manager you install retains the same settings, accounts, and Product Directory entities as the previous server. In addition, Control Manager retains the root account of the previous installation - you cannot create a new root account.
   - **Delete existing records, and create a new database**- the existing database is deleted, and another, using the same name, is created
   - **Create a new database with a new name**- you are returned to the previous screen to allow you to change your Control Manager database name

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

Step 4: Set up root account and configure proxy server

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

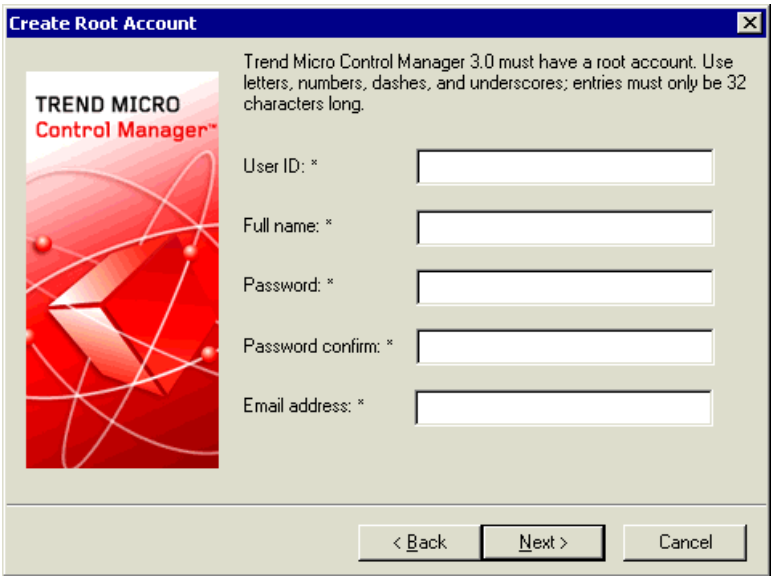


FIGURE 3-11. Enter information for the Control Manager root account

2. Provide the following required account information:
   - User ID
   - Full Name
   - Password
   - Password confirmation
   - Email address
3. Click **Next**. The following screen appears:

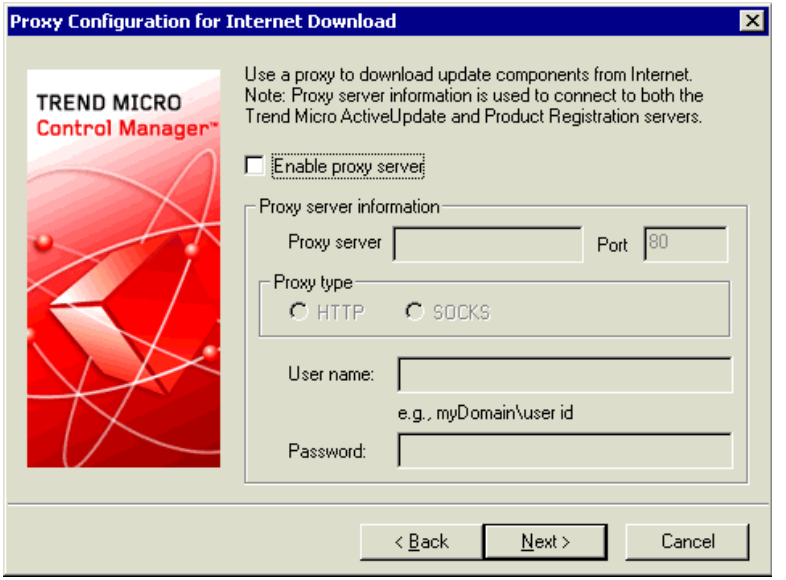


FIGURE 3-12. Enable proxy server

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

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

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

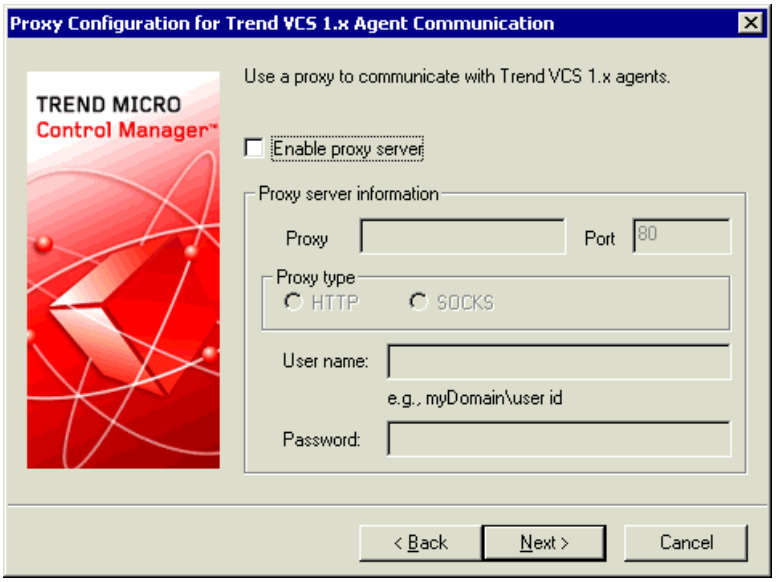


FIGURE 3-13. Enable proxy server to communicate with Trend VCS 1.x agents

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

Step 5: Configure notification settings

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

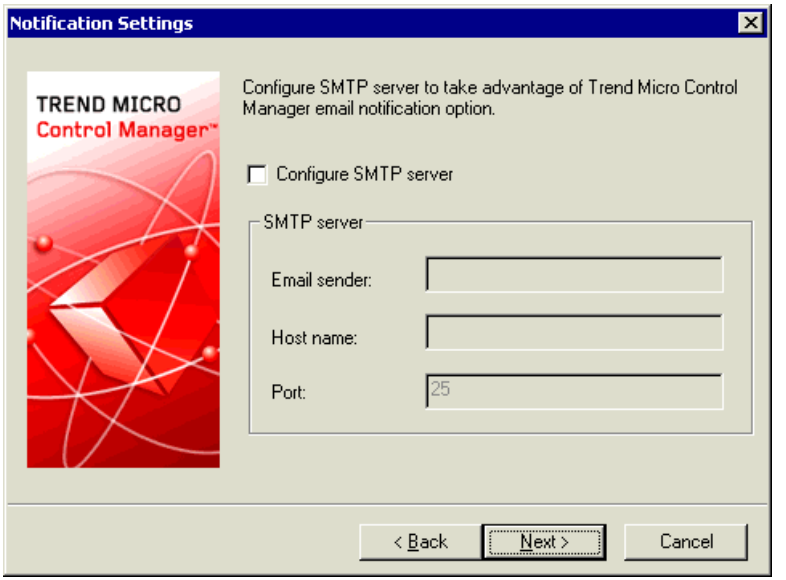


FIGURE 3-14. Configure SMTP options

2. Configure the various settings used for the Control Manager notification functions.
   - SMTP server- this 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.

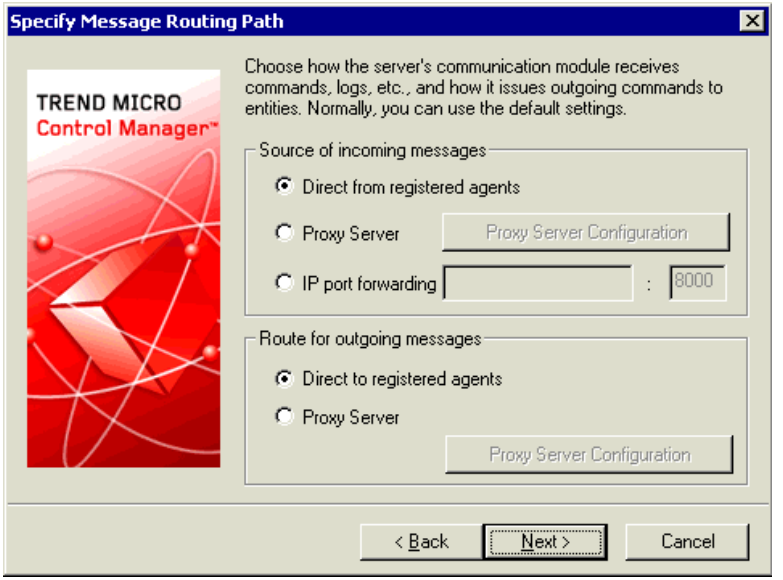


FIGURE 3-15. Define routes for messages or requests

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

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

Source of incoming messages

- **Direct from registered agents**- the agents can directly receive incoming messages.
- **Proxy server**- use a proxy server when receiving messages. For additional details about using and configuring proxies, see *Configure proxy server connection for component download and Trend VCS agents* on page 5-30.

- **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 5-30.

5. Click **Next**. Specify the Start menu program folder that will contain the Control Manager shortcut. The default is 'Trend Micro Control Manager'. Click **Next**. The installation begins.
6. Click **Finish** to complete the installation.

Installing Control Manager agents

Control Manager uses agents to manage products on your network. It can use two 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 agents - Trend Micro built this agent according to the Control Manager architecture. All products will eventually upgrade to this standard.

Trend VCS and Control Manager 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), or a native Control Manager agent.

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

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

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

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

Prepare for Control Manager agent installation

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

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

Note: You need administrator rights for those target servers that you want to 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 who are responsible for managing the product servers

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

- The location of the public encryption key of the Control Manager you want to register the agent with. Only Control Manager agents use this key. See *Public encryption key* on page 3-29 for instructions on how to obtain a Control Manager public encryption key.

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

Refer to the following checklists to collect relevant information:

- For a list of important product-specific information, see *Agent installation checklist* on page A-4
- For a list of important ports, see *Ports checklist* on page A-3

Understanding the Control Manager agent remote installation

The Control Manager 3.0 server can support Trend Virus Control System 1.8x and Control Manager 2.5x agents.

There are two agent remote installation programs:

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

RemoteInstall.exe

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

- To install agents to supported product servers
- To upload agent packages to Control Manager servers

This tool differs from the original `CMAgentSetup.exe` program because it does not actually contain any agents. Instead, it uses agent packages stored on Control Manager servers. The tool merely identifies the target servers, and then the setup programs in the agent packages themselves perform the installation.

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

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

CMAgentSetup.exe

A similar program used in Trend Virus Control System 1.x is the basis of this agent installation program. All the agents required for the corresponding products are contained in this file.

Use the CMAgentSetup.exe to install Trend VCS 1.86 agents for all Trend Micro antivirus products and Control Manager agent for InterScan Messaging Security

Suite 5.1 (InterScan Messaging Security Suite 5.15 or higher uses the RemoteInstall.exe tool).

Performing the installation

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

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

Agent installation is performed in three steps:

- Step One: Obtain required files
- Step Two: Obtain agent packages (Optional)
- Step Three: Install the agents

Step One: Obtain required files

The following are required for agent installation:

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

Agent installation programs

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

To obtain the setup program:

1. Click **Products** on the menu.
2. Click **Add/Remove Product Agents** on the left-hand menu.
3. On the Add/Remove Product Agents screen, click the appropriate **Use this**.

For Control Manager agents, you should use the `RemoteInstall.exe` program. For Trend VCS agents and the Control Manager agent for InterScan Messaging Security Suite 5.1, use the `CMAgentSetup.exe` program

4. At the File Download screen, select **Save** this program to disk, and then click **OK**.
5. At the Save As screen, select a location for the program, and then click **Save**.

Public encryption key

Control Manager agents use the encryption key to identify the Control Manager server that it 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-hand 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.

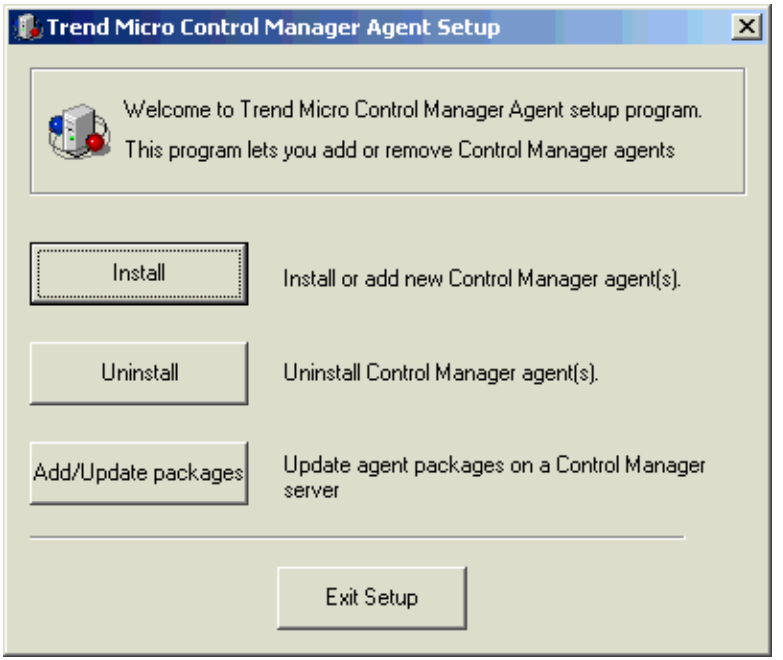


FIGURE 3-16. Control Manager Agent Setup screen

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

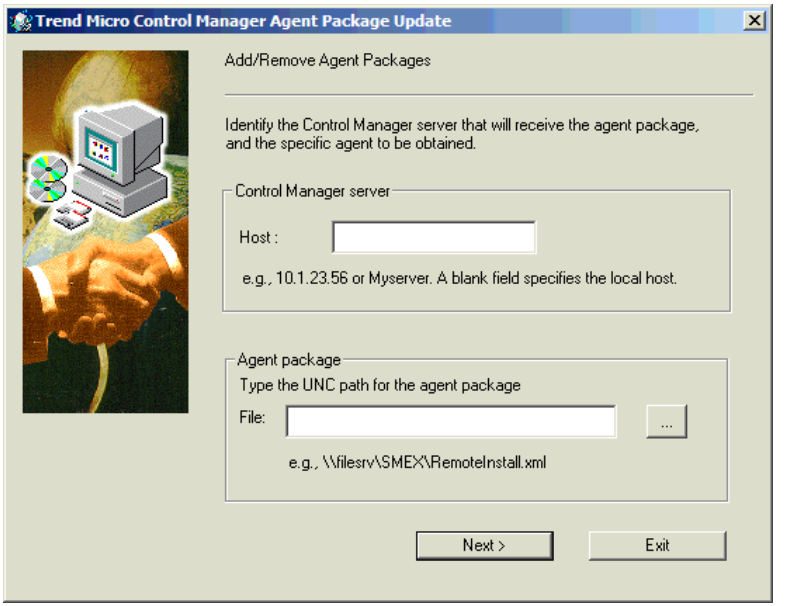


FIGURE 3-17. Identify the Control Manager server and the agent

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.

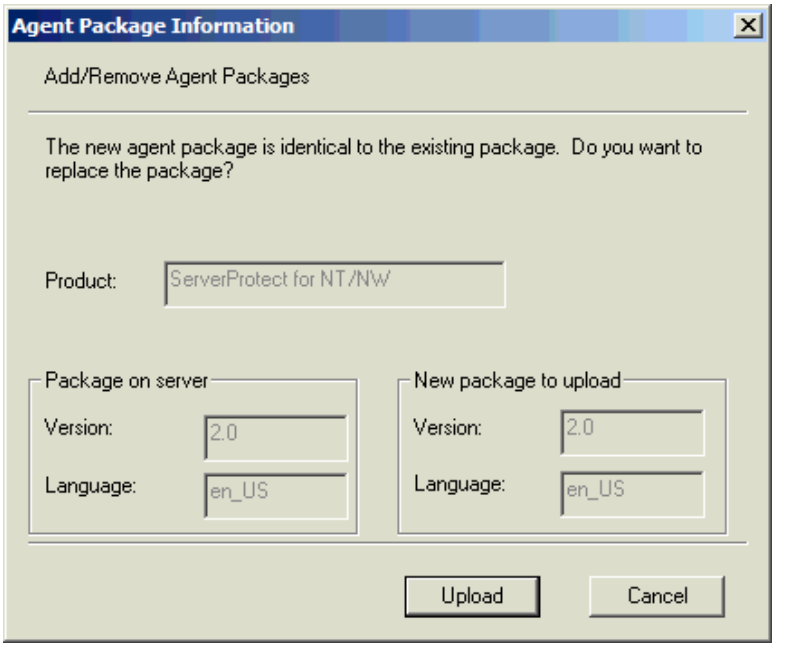


FIGURE 3-18. Agent package information

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 as part of the product installation. However, you can still deploy agents remotely from the Control Manager server; provided you obtain 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.

This section helps with the following:

- Installing Control Manager agents with the Remote Agent Setup tool
- Installing Trend VCS agents
- Installing Control Manager agent for InterScan Messaging Security Suite 5.1 for Windows

Installing Control Manager agents with the Remote Agent Setup tool

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

To install Control Manager agents:

1. Using MS Explorer, go to the location where you saved the Remote agent setup tool.
2. Double-click the `RemoteInstall.exe` file.

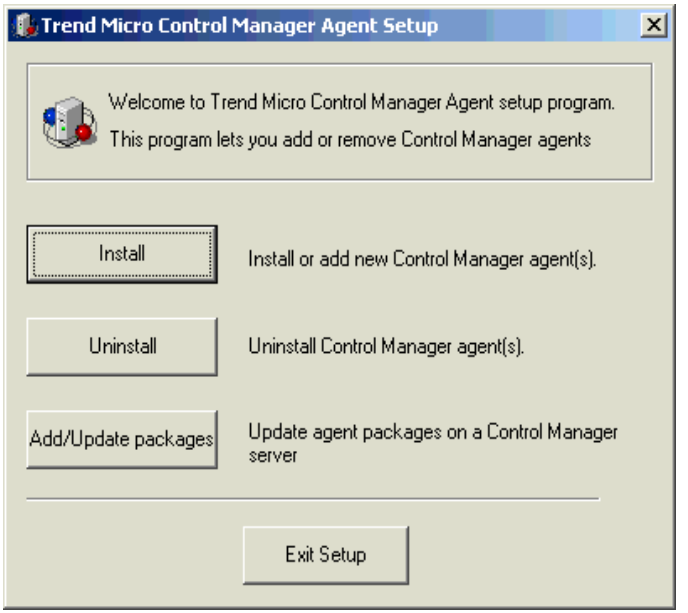


FIGURE 3-19. Control Manager Remote Agent Setup

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 3-20. 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.

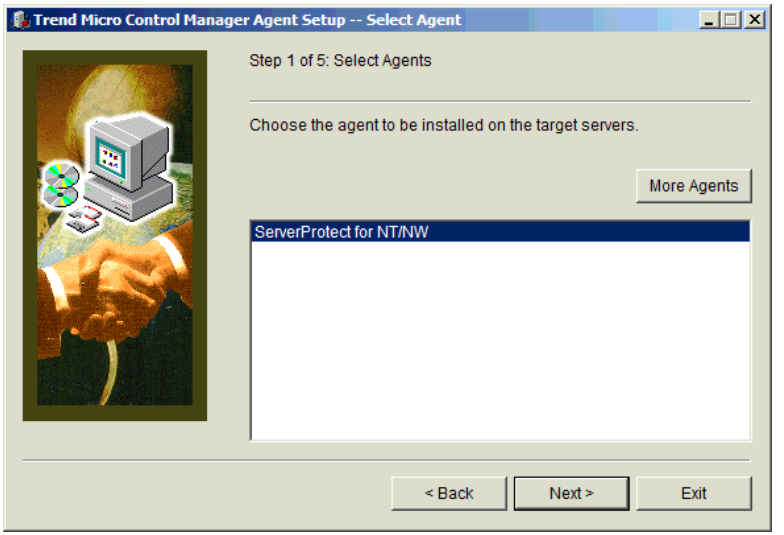


FIGURE 3-21. Choose the agent to install on the target server

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 3-29

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

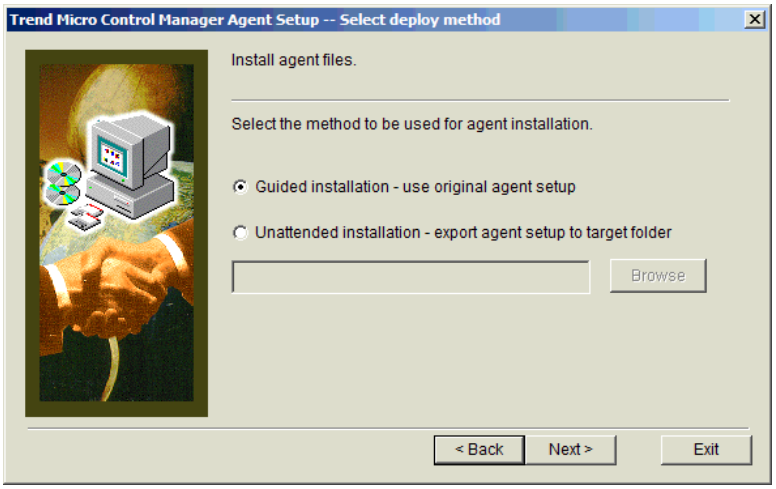


FIGURE 3-22. Select the agent installation method

9. The At the Select Servers to Install screen, select the servers where the agents are to be installed.

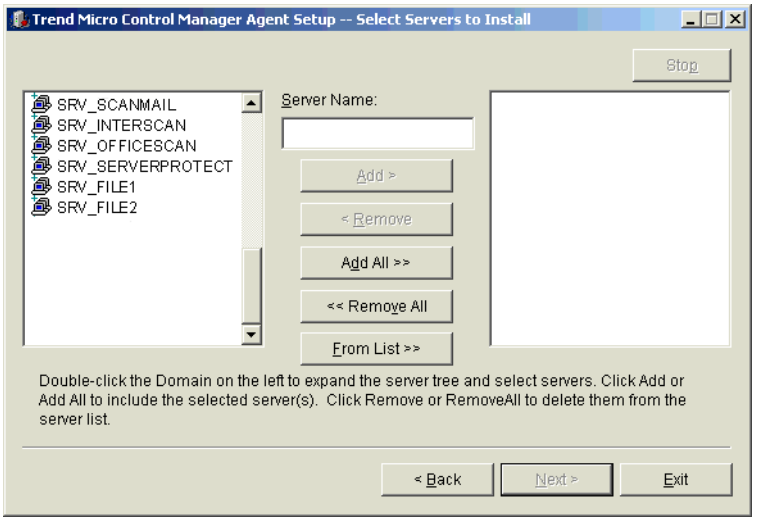


FIGURE 3-23. Select servers to install

There are three 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 install agents on 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 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-hand list.

Note: The migration list is generated by the Trend VCS Migration tool. For additional information about this list, see *Cascading Management Structure Tool (CasTool.exe)* starting on page 8-2.

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 on to 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.

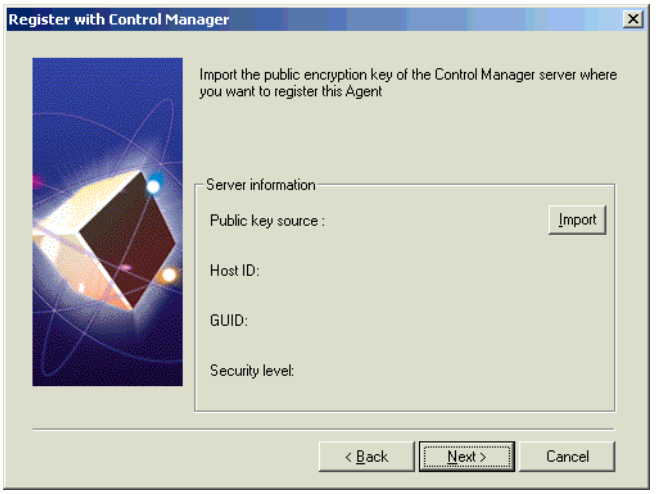


FIGURE 3-24. Encryption key selection screen

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

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

Installing Trend VCS agents

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

To install the Trend VCS agent:

1. Using Windows Explorer, go to the location where you saved the agent setup program.
2. Double-click `CMAgentSetup.exe`.
3. Click **Install** to begin installation. The Software License Agreement appears.

Read the agreement carefully. If you do not agree with the terms of the license, click **No**; the installation will discontinue. Otherwise, click **Yes**.

4. On the agent Installation screen, click **Next**. A list of products appears.
5. Select the products for which you want to install agents. Click **Next** to continue. The Select Servers to Install screen appears.

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

---

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

   To select from the list:

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

   To remove a server from the list, select the server from the right-hand 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.

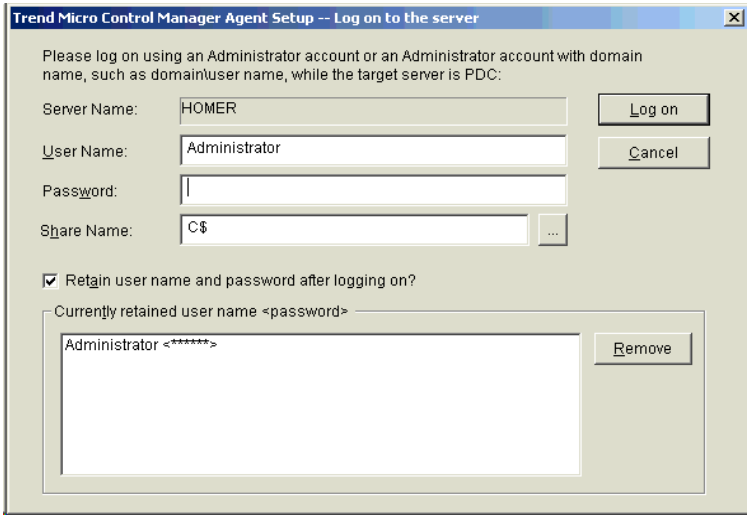


FIGURE 3-25. Logon credentials screen for agent installation

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 actual 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.

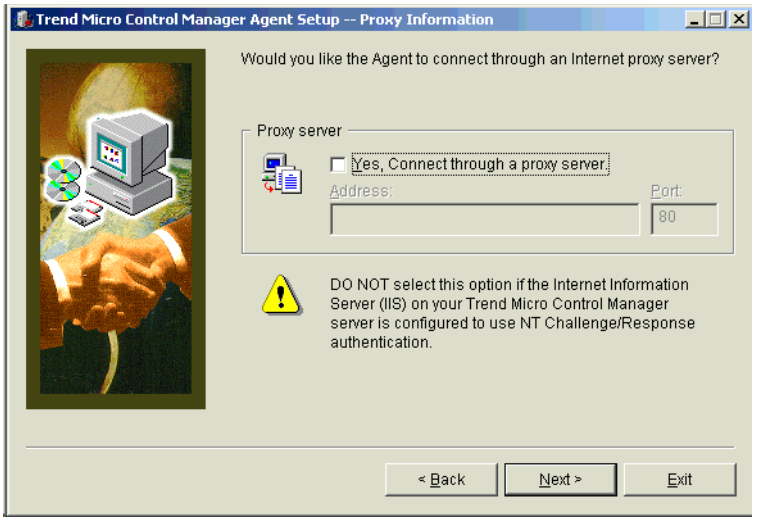


FIGURE 3-26. Trend VCS agent proxy screen

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)* - 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 Server.

13. On the Agent Information screen provide the following:

- *Site* - provide a site name for your agents you are installing. It's helpful to specify a name that reflects the agent's geographical location (for example, New_York, Tokyo, Manila).
- *Relative destination directory* - this is where the Trend VCS agent files will be kept. The directory is relative to the shared path you specified earlier.

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

14. Click **OK**. Click **Exit** to end the setup, or **Next** to install agents for other applications.

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

16. Click **Finish**.

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

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

FIGURE 3-27. Select Antivirus Product screen; note inclusion of IMSS in the selection

To install this agent, see *Installing Trend VCS agents* on page 3-41, and follow the procedure until step 10. Afterwards, see *Installing Control Manager agents with the Remote Agent Setup tool* on page 3-33, and use the procedure outline in step 14 onward.

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

  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:

a. On the NetScreen Policy Manager logon screen, select an **Arbitrator** used for Global PRO communication. Choose an Arbitrator that uses SSL.

b. Click **Edit**.

c. Copy the **16-digit certificate number** at the Cert. Name field.

- Location of the Control Manager server public encryption key (`E2EPublic.dat`)

To install the agent:

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

- A permanent user account on the Control Manager server

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.

Verifying successful installations

Check the following sections to confirm that Control Manager server or agent has successfully installed.

Verify a successful Control Manager server installation

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

The following folder structure appears under the directory `Program Files\Trend Micro`:

- `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)`

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`

Verify a successful agent installation

To verify a successful agent installation, view 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-hand menu select **Managed Products**, and click **Go**. Under product directory the managed product for the agent you installed appears.

If you don't see your managed product, try the following:

1. Refresh the Product Directory. Click the icon on the upper right corner of the left-hand menu.
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.

Post-installation configuration

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

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

Register and activate Control Manager

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

Configure user accounts

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

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

Download the latest components

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

Set notifications

After installation, configure the events that will trigger notifications to monitor significant virus attacks and related security activities. Besides specifying notification recipients, choose notification channels and test them to make sure they work as expected (on the Web console, click Administration > Event Center).

Registering and activating your software

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

If you installed Control Manager for the first time:

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

  Register online and obtain an Activation Code to activate the product

- You are using an evaluation version

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

Activate Control Manager

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

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

To register and activate Control Manager:

1. Click **Administration** on the main menu.
2. On the left-hand 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**.
6. 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 above procedure.

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-hand menu under **Registration**, click **License Information**.
3. On the working area under Control Manager License Information, click **Check Status Online**.

4. Click **OK**.

Log off and then log on to the Management Console for changes to take effect.

To renew maintenance by manually entering an updated Activation Code:

1. Click **Administration** on the main menu.
2. On the left-hand 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

Upgrading Servers or Migrating Agents to Control Manager 3.0

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

This chapter discusses the following topics:

- *Upgrading to Control Manager 3.0* on page 4-2
- *Planning Trend VCS or Control Manager agent migration* on page 4-8
- *Migrate the Control Manager database* on page 4-14

Upgrading to Control Manager 3.0

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

CAPABILITY	STANDARD EDITION	ENTERPRISE EDITION
Upgrade Control Manager 2.x 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 4-1. Considerations when upgrading to Control Manager 3.0

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.

Upgrade Trend VCS 1.8x servers

Consider the following points when upgrading from Trend VCS to Control Manager 3.0 server:

- The Control Manager 3.0 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 8-5).

  Refer to *Planning Trend VCS or Control Manager agent migration* on page 4-8 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 servers

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

- The Control Manager 3.0 installation detects an existing copy of Control Manager 2.5, and gives you the option to upgrade it to the latest Control Manager version

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

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

Control Manager 2.5 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.

TABLE 4-2. Control Manager 2.5 files that should be backed up

Control Manager 2.5 Information	LOCATION
Configuration files	\Program Files\Trend Micro\Control Manager\Settings*.* \Program Files\Trend Micro\Control Manager\DataSource.xml \Program Files\Trend Micro\Control Manager\CascadingLogConfigura-tion.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\ProductUIHan-dler.xml \Program Files\Trend Micro\Control Manager\Settings\SystemConfigura-tion.xml
Serial number infor-mation	Cfg_dm_tms_sn value in \Program files\Trend Micro\COMMON\TMI\TMI.cfg
GUID information	GUID value in \Program files\Trend Micro\COMMON\TMI\TMI.cfg
Hot fix list	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMi-cro\TVCS\hotfix
Managed product information	\Program Files\Trend Micro\com-mon\tmi\mrf_entity.dat \Program Files\Trend Micro\com-mon\tmi\mrf_entity.bak
ActiveUpdate files	\Program Files\Trend Micro\Control Manager\webui\download\Activeupdate

TABLE 4-2. Control Manager 2.5 files that should be backed up

Control Manager 2.5 Information	LOCATION
Control Manager registry	HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TVCS\ . . . HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMI\ . . . HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\CommonCGI HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TMCM HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TMI HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\MSDE HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDE HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMCM HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro_NTP HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro Infrastructure\. . . HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendCCGI HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSSQLServer

TABLE 4-2. Control Manager 2.5 files that should be backed up

Roll back to Trend VCS 1.8x server

In the unlikely event that the upgrade to Control Manager 3.0 is unsuccessful, it is possible to 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. However, if you decide to remove Control Manager later, it will be necessary to 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 server

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

To roll back to Control Manager 2.5:

1. Collect all Control Manager 2.5 backup files (refer to Table 4-2, “Control Manager 2.5 files that should be backed up,” on page 4-4).
2. Remove Control Manager 3.0. Perform one of the following
   - Use the Control Manager uninstallation shortcut
   - Use the Windows Add/Remove Programs feature
3. Install Control Manager 2.5. Refer to Control Manager 2.5 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: When you install Control Manager 2.5, setup generates a new public key. If you set the security level to high, the Control Manager agents registered to the original Control Manager 2.5 server re-import the public key to register to the new Control Manager server. Since, a new public key is available, agents cannot match the original public key to the new one. The agents will not be

able to register to the Control Manager server. To restore the original settings, reinstall all agents to re-register to the new Control Manager 2.5 server.

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

Planning Trend VCS or Control Manager agent migration

There are two ways to migrate Trend VCS and Control manager 2.5x agents to Control Manager 3.0 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 with Control Manager 2.5x agents	Registers Control Manager 2.5x agents to Control Manager 3.0 server; Control Manager agents maintain their original Product Directory structure
Control Manager 2.5 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 3.0 server; Control Manager agents maintain their original Product Directory structure

  Trend Micro recommends rapid upgrade for migrating agents in a laboratory setting or in relatively small networks, preferably during test deployments (see

page 2-16). However, since you cannot stop the migration it started, this method works best for smaller deployments, and the degree of difficulty increases with the size of the network.

- **Phased upgrade**

  Trend Micro recommends a phased upgrade for large, single-server Trend VCS 1.8x or Control Manager 2.5x networks; and is essential for multiple-server networks. It offers a more structured approach to migrating your system, and follows these guidelines:

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

    This will simplify any troubleshooting that may be required.

  Phased upgrade involves the following steps:

  a. Install Control Manager 3.0 on a server that does not have any previous Trend VCS or Control Manager version installed (preferably without any managed products).

  b. Run the AgentMigrateTool.exe tool on the Trend VCS 1.8x or Control Manager 2.5 server.

  You can now consolidate all Trend VCS agents that were originally separated for functional control purposes, as well as Control Manager 2.5 agents, under a single Control Manager 3.0 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

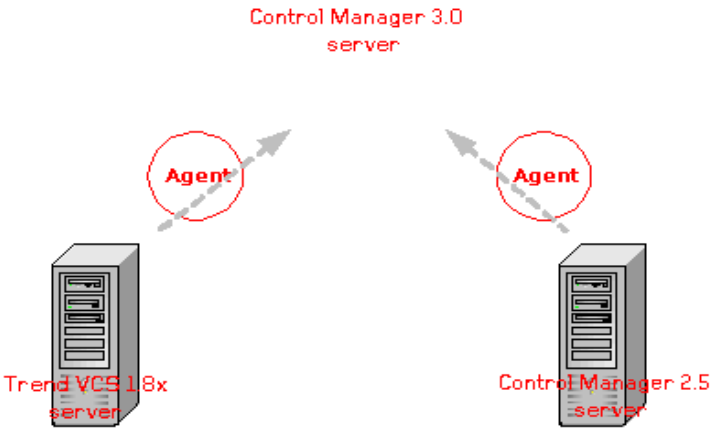


FIGURE 4-1. Migration of agents belonging to a single server

You can use both Rapid and Phased migration in this instance. See *Upgrading to Control Manager 3.0* on page 4-2. Trend Micro recommends using Phased migration for large Trend VCS networks.

- Consolidation of different servers/agents

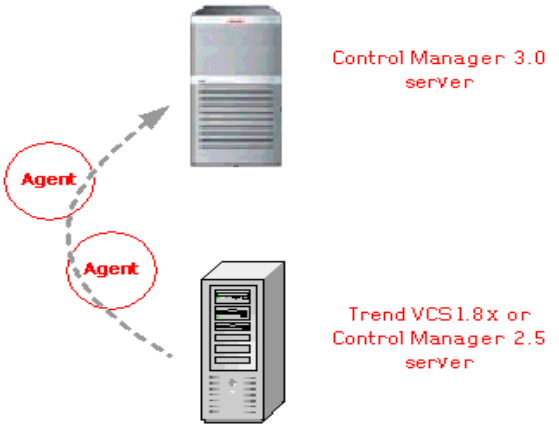


FIGURE 4-2. Migration of agents belonging to multiple servers

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

Trend VCS 1.8x agent migration flow

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

- Upgrades Trend VCS 1.8x agents to version 1.86
- Removes Trend VCS 1.8x server information from the registry and replaces them with Control Manager 3.0 server information
- Unregisters from the Trend VCS server and registers to the Control Manager 3.0 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 3.0 server and re-registers them back to the Trend VCS server.

Control Manager 2.5x agent migration flow

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

- Stops the Trend Micro Infrastructure service
- Obtains the Product Directory information from the Control Manager 2.5 server
- Removes the agent information from the Control Manager 2.5 database and TMI.cfg
- Retains the Control Manager 2.5x agent version (no upgrade takes place)
- Writes the agent information to the Control Manager 3.0 database and TMI.cfg
- Restarts the Trend Micro Infrastructure service

If AgentMigrationTool.exe is unable to complete or finish the Control Manager 2.5x agent migration, it removes the agent information from the Control Manager 3.0 database and TMI.cfg and then writes them back to the Control Manager 2.5 database.

Migrate Trend VCS or Control Manager agents

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

Run `AgentMigrateTool.exe` directly on the *destination server*—a Control Manager 3.0 server where you will migrate the agents.

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

1. Using Windows Explorer, open the Control Manager 3.0 root folder. For example:

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

2. Double-click `AgentMigrateTool.exe`.
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, or Control Manager 3.0 server hosting the agents that will be migrated.

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 3.0 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

   These options are applicable to agents listed in the Destination list.

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 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 3.0 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 or Control Manager 3.02 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 3.0 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

There are two ways to migrate a Control Manager 2.5 database:

- Install Control Manager 3.0 to a Control Manager 2.5 server - this is the recommended method

  The Control Manager 3.0 setup will automatically upgrade the database to version 3.0. Refer to Control Manager 2.5x agent migration on *page 4-12* for more details.
- Manually transfer Control Manager 2.5 database to Control Manager 3.0 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.

   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`. This means keeping the same ID and password combination.

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

   Backup `TMI.cfg` to roll back to the original settings.

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

   `CFG_DM_DB_ID`

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

   If the destination server is not available from the list, type the **server name**.

10. On the next window, select **With SQL Server authentication using a logon ID and password entered by the user** and **Connect to SQL Server to obtain default settings for the additional configuration** options.
11. Type the same **ID** and **password** available in `TMI.cfg` and then click **Next**.
12. Click **Finish** to save the new configuration and close Microsoft SQL Server DSN Configuration.
13. Click **OK** to close ODBC Data Source Administrator.
14. Using Windows Services, restart all Control Manager services.

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

Chapter 5

Getting Started with Control Manager

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

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

- *Use the management console* on page 5-2
- *Configure Control Manager user accounts and groups* on page 5-7
- *Administer managed products* on page 5-16
- *Manage child servers* on page 5-19
- *Download and deploy new components* on page 5-25
- *Monitor the Control Manager environment* on page 5-37

Use the management console

The management console consists of the following elements:

- Header menu - includes links to the following:
  - Control Manager 3.0 help - provides advanced feature descriptions and detailed configuration information
  - Trend Micro Knowledge Base - provides technical product information and procedures provided by the Trend Micro Support team
  - Trend Micro Security Information - provides the latest malware advisories as well as the list of the current top ten malware threats
  - Control Manager 3.0 About page - provides the Control Manager version, build number, and copyright information
- Main menu - includes links to the following Control Manager functions:
  - 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
- 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.

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

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

There are 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 will appear:

The page must be viewed over a secure channel

Access the HTTPS management console

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

```
https://{hostname}:443/ControlManager
```

Where:

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

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

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

Configure Control Manager user accounts and groups

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

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

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

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

Menu Item	Operator	Power User	Root/Administrator
Home			
	●	●	●
Services			
TrendLabs Message Board			●
Outbreak Prevention Services			●
Damage Cleanup Services			●
Vulnerability Assessment			●
Products			
Add/Remove Product Agents	●	●	●

Menu Item	Operator	Power User	Root/Administrator
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	●	●	●

Menu Item	Operator	Power User	Root/Administrator
User Manager > User Accounts			●
User Manager > User Groups			●
System Settings			●
Tools			●
Registration			●

Additional root account privileges

The root account also has the following additional privileges:

- Only the root account can see all user accounts on the server; other accounts can only see their child accounts
- The root account can unlock a locked function by forcibly logging out the user who is using it

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

Understanding the User Manager

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

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

Setting access rights

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

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

- View
- Execute
- Configure
- Edit Directory

View

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

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

Execute

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

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

Configure

This gives the user access to the configuration consoles of the managed products in the assigned folders. Users with this right can see Configuration for <product> and similar product-specific controls (for example, OfficeScan password configuration features) on their menus.

Edit Directory

This permits the user to modify the organization of the assigned folders.

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

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

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

Add a user account

Add user accounts to allow others to log on to the Control Manager management console, appear on the recipient list for notifications, or be added to user groups. When adding a user account you need to provide information to identify the user, assign an account type and folder access rights.

To add a user account:

1. Click **Administration** on the main menu.
2. On the left-hand menu, click **User Accounts**.
3. On the working area, click **Add New User**. The following information is required 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 a "9" and a comma "," [each comma causes a 2 second pause])
- MSN Messenger address

4. Click **Next>>**.
5. 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.

---

6. 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

7. 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-hand menu, click **User Accounts**.
3. On 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-hand 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-hand 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

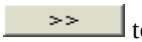
User groups simplify the management of Control Manager users by providing a convenient way to send notifications to a single group rather than to individual users. You can add users to groups according to similar properties including: user types, location, or the type of notifications they should receive. 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-hand menu, under **User Manager**, click **User Groups**.
3. On the working area, click **Add New Group**.
4. Type a descriptive name for the group in Group name.
5. Under **Group Members**, add or remove users to the group list.

   To add a user:

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

   b. Click 

to add the selected user(s) to the Group User List.

   Control Manager sends notifications to users based on the contact information specified during their account setup.

To remove a user:

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

b. Click  to remove the user.

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

- **Email address(es)**
- **Pager number(s)** (precede the pager number with a "9" and a comma "," [each comma causes a 2 second pause])

Separate multiple entries with semicolons.

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

Edit a user group

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

To edit a user group:

1. Click **Administration** on the main menu.
2. On the left-hand 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-hand menu, under **User Manager**, click **User Groups**.
3. On the working area, click **Delete** beside the group to delete.
4. Click **OK** to delete the user group.
5. Click **OK**.

Administer managed products

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

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

Configure managed products using the Product Directory

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

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

Careful planning of this structure is necessary, 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.

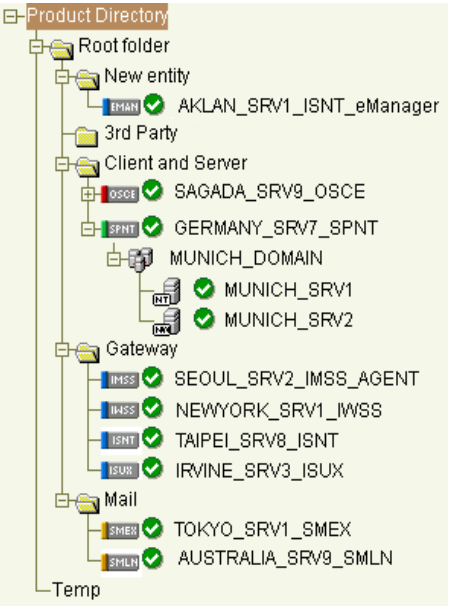
- Deployment planning

  Control Manager deploys 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 will therefore simplify 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

Here's a sample of a Product Directory:



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

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

Arrange the Product Directory using the **Directory Manager**. Use descriptive folder names to group your managed products according to their protection type or the Control Manager network administration model (see *Administration Plan* on page 2-8). For example, grant access rights to mail administrators to configure the Mail folder. Refer to the Control Manager *Understanding Directory Manager* online help topic for details on how to arrange the Product Directory.

Default folder for managed products

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

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

Use the Product Directory tabs

Use the Product Directory tabs to configure and administer managed products. In Control Manager 3.0, the following tabs are available:

- **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.

Group managed products using Directory Manager

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

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

GROUPING TYPE	ADVANTAGE	DISADVANTAGE
Geographical or Administrative	Clear structure	No group configuration for identical products
Product type	Group configuration and status is available	Access rights may not match
Combination of both	Group configuration and access right management	Complex structure, may not be easy to manage

TABLE 5-1. 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
Create global reports	Yes	No

TABLE 5-2. 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 8-3 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.

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 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 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}"`

  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 the unregister command:

   ```
   castool /u
   ```

Note: You can use the **`/d`** command to debug the process while CasTool unregisters a child server.

When user uninstalls Control Manager 3.0 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 structure Cascading Manager:

1. Click **Products** on the main menu.
2. On the left-hand menu, select **Control Managers** from the list and then click **Go**.
3. On the left-hand menu, click **Cascading Manager**.

4. On the working area, right-click the child server to unregister, and then select **Delete** from the menu.

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.

Download and deploy new components

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

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

- Pattern files/Cleanup templates - refer to virus pattern files, damage cleanup templates, Vulnerability Assessment patterns, network outbreak rules, and network virus pattern files
- Anti-spam rules - refer to import and rule files used for anti-spam and content filtering
- Engines - refers to virus scan engine, damage cleanup engine, and VirusWall engine for Linux
- Product 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.

Update the Control Manager managed products components

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

1. Downloading components

   Choose a download **source**:

   - Internet: Trend Micro ActiveUpdate server - by default, Control Manager implements digital signature checking whenever it downloads components from the ActiveUpdate server

     Aside from this, you can enable HTTPS when downloading components from the ActiveUpdate server.

- Other Internet source - specify a Web site (for example, your local Intranet Web site) from where Control Manager can download updates
- UNC -- specify a shared folder in your network from where Control Manager can download updates

Choose a **download method**:

- Manual download - run manual downloads to obtain updates on-demand

  Control Manager only downloads components needed by its managed products.
- Scheduled download - implement scheduled downloads to obtain update components according to the schedule that you set

  The Control Manager server provides four predefined scheduled download settings.

The download options of Control Manager allow you to select which components to download, when, and how often to obtain the updates, and where to get them.

2. Deploying components

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

Manually download components

Use the Manual Download screen to immediately download new components.

To manually download components:

1. Click **Administration** on the main menu.
2. On the left-hand menu under **Update Manager**, click **Manual Download**. The Manual Download screen appears.
3. On the working area, click **Download Now** and then click **OK** to confirm.

   The download response screen opens. The progress bar shows the download status.

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

Enable scheduled component download

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
- **State** - indicates if the schedule for the component is either enabled or disabled
- **Update Source** - displays the URL or path of the update source

To enable scheduled component download:

1. Click **Administration** on the main menu.
2. On the left-hand menu under **Update Manager**, click **Scheduled Download**. The Scheduled Download screen appears.
3. From the {Component} screen, select the **Enable scheduled download** check box to enable scheduled download for the component.
4. Define a **schedule** for a component by clicking its corresponding **Edit** link. This opens the component's configuration screen, which is divided into three groups: **Schedule and Frequency** (see *Configure scheduled download schedule and frequency* on page 5-27), **Download settings** (see *Configure scheduled download settings* on page 5-28), and **Automatic deployment** (see *Configure scheduled download automatic deployment settings* on page 5-29).
5. 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** from the main menu, and then click **Scheduled Download** from the left-hand menu under Update Manager to access the Scheduled Download screen.
2. On the working area, click the **Edit** link of the component whose scheduled download schedule and frequency you want to modify.
3. Under **Schedule and frequency**:

a. Define the download **schedule**. Select a **frequency**, and use the appropriate drop down menu to specify the desired schedule. You may schedule a download every minute, hour, day, or week.

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

4. Click **Save**.

Configure scheduled download settings

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

To configure scheduled download settings:

1. Click **Administration** from the main menu, and then click **Scheduled Download** from the left-hand menu under **Update Manager** to access the Scheduled Download screen.
2. On the working area, click the **Edit** link of the component whose scheduled download settings you want to modify.
3. Under **Download settings**:
   a. Select the **components** to download.
   b. Under **From**, select one of the following update sources:
      - **Internet: Trend Micro update server** - (default setting) Control Manager downloads latest components from the Trend Micro ActiveUpdate server
      - **Other Internet source** - specify the URL of the latest component source, for example, your company's Intranet server
      - **File path** - specify a location on your network of the latest component source, for example, your company's file server (see *Enable UNC download* on page 5-31)
   c. Select **Retry frequency** to instruct Control Manager to retry downloading latest components. Specify the **number of attempts** and the **frequency** of each set of attempts in the appropriate fields.
   d. If 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 (*Configure proxy server connection for component download and Trend VCS agents* on page 5-30) from the System Settings screen.

4. Click **Save**.

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

Configure scheduled download automatic deployment settings

Use the Auto-deploy Setting group to set how Control Manager deploys updates.

To configure scheduled download auto-deploy settings:

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

     It gives you the greatest control over the update, since you can specify which products Control Manager updates, and in what order.
   - **Deploy immediately** - this deploys the updates to all managed products immediately after Control Manager completes the download
4. Click **Save**.

Configure proxy server connection for component download and Trend VCS agents

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

To configure proxy server settings:

1. Click **Administration** on the main menu.
2. On the left-hand menu, click **System Settings**. The System Settings screen appears.
3. On the working area under **Proxy Settings for Component Download** or **Proxy Settings for Trend VCS Agents**, set the proxy server settings:
   a. If you are using a proxy server to connect to the Internet:
      - On the working area under **Proxy Settings for Component Download**, click **Use a proxy server to download update components from the Internet**
      - On the working area under **Proxy Settings for Trend VCS Agents**, click **Use a proxy server to connect to Trend VCS agents**

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

   c. Select the proxy server protocol—**HTTP** or **Socks**.

   d. Type the **user name** and **password** used for proxy authentication.

   e. Click **Save**.

Enable HTTPS download

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

To enable HTTPS download:

1. Click **Administration** on the main menu.
2. On the left-hand menu, click **System Settings**. The System Settings screen appears.

3. On the working area under **ActiveUpdate settings**, select **Enable HTTPS for the default update download source** or specify your organizations component source server in the **Other Internet source field**.
4. Click **Save**.
5. Do one of the following:
   - On the left-hand menu under **Update Manager**, click **Manual Download**
   - On the left-hand menu under **Update Manager**, click **Scheduled Download**

   Define a **schedule** for a component by clicking its corresponding **Edit** link. This opens the component's configuration screen, which is divided into three groups: **Schedule and frequency**, **Download settings**, and **Automatic deployment**.
6. On the working area under **Download settings** > **From** group, select **Internet: Trend Micro update server**.
7. Click **Save**.

Enable UNC download

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

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

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

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

To enable UNC download:

1. Click **Administration** on the main menu.
2. On the left-hand menu, click **System Settings**. The System Settings screen appears.
3. On the working area under ActiveUpdate settings, provide the **local Windows** and **Remote UNC** authentication **user names** and **passwords**.
4. Click **Save**.
5. Do one of the following:

- On the left-hand menu under Update Manager, click **Manual Download**
- On the left-hand menu under Update Manager, click **Scheduled Download**

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

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

Set "Log on as batch job" policy

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

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

To set "Log on as batch job" policy:

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

d. On the left-pane, right-click the **Security Configuration and Analysis** scope item and then select **Configure Computer Now…** from pop-up menu.

e. Provide the error log **file name**, and then click **OK**.

f. On the left-pane, right-click the **Security Configuration and Analysis** scope item and then select **Analyze Computer Now…** from pop-up menu.

g. Provide the error log **file name**, and then click **OK**.

3. Set **Log on as a batch job** policy.

a. On the left-pane, expand the **Security Configuration and Analysis** > **Local Policies** scope item.

b. Click **User Rights Assignment**.

c. On the right-pane, double-click **Log on as a batch job**.

d. On the Analysis Security Policy Setting window, select **Define this policy in the database**.

If the user account used for local Windows authentication is not in the list, click **Add** to assign **Log on as batch job Database Setting** to a user with administrative privilege and then click **OK**.

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

Deploy updated components

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

The Control Manager installation creates two deployment plans:

- Deploy to All Managed Products Now (Default) - default plan used during component updates

- Deploy to All Immediately (Outbreak-Prevention) - default plan for the Outbreak Prevention Services, Prevention Stage

By default, these plans deploy updates to all products in the Product Directory immediately. Select or create plans from the Manual and Scheduled download pages. Customize these plans, or create new ones, as required by your network. For example, create Deployment Plans according to the nature of the outbreak:

- Email-borne virus
- File-sharing virus

Create deployment plans

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

To create a new deployment plan:

1. Click **Administration** on the main menu.
2. On the left-hand 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, provide a deployment plan **name** in the plan name field.
5. Click **Add New Schedule** to provide deployment plan details.
6. On the Add New Schedule screen, choose a deployment time **schedule**. Select one the following:
   - **Delay** - after Control Manager downloads the update components, it delays the deployment according to the interval you specify

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

     Use the drop-down menus to designate the time, in terms of hours and minutes.
7. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.
8. Click **OK**.
9. On the Add New Plan screen, do one of the following:
   - Click **Add New Schedule** to add another schedule

- Click **Save** to apply the new deployment plan

Update all outdated components

Updating and deploying new components to managed products with out-of-date components is a two-step process.

To update all out-of-date components:

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

      Note: Clicking **Add to Temp** only adds the managed products shown on the status screen. 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.

   g. Click **<<Back** to return to the Status Summary page, and then proceed to the next out-of-date component. Repeat the instructions until Control Manager adds all the out-of-date managed products to Temp.
2. On the working area, click the **Tasks** tab.

3. Select **Deploy <component>** from the Select a task list, and then click **Next**.
4. Click **Deploy Now** to start updating all out-of-date components.

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

Monitor the Control Manager environment

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

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

- **System information** - groups all Control Manager server related system information and includes the following:
  - Control Manager server - indicates the host name of the server hosting the Control Manager application
  - Installed version - indicates the version and build number of the Control Manager program
  - Registration - indicates the date you installed the Control Manager program

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

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

Use Command Tracking

The Control Manager server maintains a record of all commands issued to managed products and child servers. Commands refer to instructions given to managed products or child server to perform specific tasks. Command Tracking allows you to monitor the progress of all commands.

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

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

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

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

Query and view commands issued in the past 24 hours

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

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

1. Click **Administration** on the main menu.
2. On the left-hand menu click **Command Tracking.**
3. On the working area, click **Query**.
4. On the Query (Command Tracking), specify **values** for the following parameters:
   - Issued - specify the scope of the query

     Choose among the predetermined ranges, or specify your own range. Set custom ranges according to months, days, and years.
   - Command - select the command that you want to monitor
   - User - leave this field blank to query commands issued by all users
   - Status - select the command status
   - Sort records by - specify how the Query Result screen will display results

     Arrange the query results according to Time, Command, or User.
   - Sort order - specify whether the Query Result screen will display results in ascending or descending order
5. Click **View Commands**. The Query Result screen shows the number of products affected by the command, as well as their results.

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

Use Event Center

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

The Event Center categorizes events according to the following types:

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

- Damage Cleanup Services -- provides information about policy application and update information about damage cleanup services-related events
- Update - provides antivirus and content security components update result (successful or unsuccessful)
- Unusual - provides information about product option or service activation and deactivation

Control Manager can send notifications to individuals or groups of recipients about events that occur in the Control Manager network. Configure Event Center to send notifications through the following methods:

- Email - messages sent to a mailbox belonging to the organization's email system or to a POP3 account (for example, Yahoo!™ or Hotmail™)
- Windows event log - the Windows Event Viewer application log contains events logged by Control Manager
- SNMP - an SNMP (Small Network Management Protocol) trap is a method of sending notifications to network administrators that use management consoles that support this protocol

  Control Manager stores notification in Management Information Bases (MIBs). Use **MIBs browser** to view SNMP trap notification.
- Pager - an electronic device that accepts messages from a special radio signal
- MSN Messenger - an online service provided by Microsoft that establishes real-time communication between two users

  Control Manager sends notifications to an online MSN Messenger account. Otherwise, an off-line MSN Messenger account cannot receive Control Manager notifications.
- Trigger Application - any in-house or industry-standard application used by your organization to send notification

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

Enable or disable notifications

Enable or disable notifications from the Event Center screen.

To enable or disable notifications:

1. Click **Administration** on the main menu.
2. On the left-hand 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-hand menu, click **Event Center**.
3. On the working area under Notification Settings, configure the notification method:
   - **To set an email notification:**
     i. 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.
     ii. 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:**
     i. On the working area under **MSN notification**, specify the **MSN Messenger email address**. This is the user name used in MSN Messenger.

ii. Type the .Net Passport email address **password**.

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

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

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

c. Type the **login name** and **password** used for proxy authentication.

- **To set an SNMP notification:**

i. On the working area under **SNMP trap notification**, specify the **Community name**.

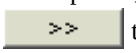
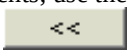
ii. Specify the SNMP trap server **IP address.**

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-hand menu, click **Event Center**.
3. On the working area, click the **Recipients** link of the event you want to configure.
4. On the Edit Recipients under **Email and Pager Recipient List**, specify or remove the email and pager notification recipients:
   - **To add recipients from the list:**
     i. Click the user or group from the **Users and groups** list. To select multiple recipients, use the CTRL key.
     ii. Click  to add the entry to the **Recipients** list.
   - **To remove a recipient from the list:**
     i. Click the user or group from the Recipient list. To select multiple recipients, use the CTRL key.
     ii. Click  to remove the entry from the Recipients list.

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

   Configure the notification method settings via the System Settings screen. Refer to Configure notification method.
6. Provide the **notification message** in the corresponding message fields.
7. Click **Test** to experiment if your system is able to deliver the notifications.
8. Click **Save**.

Configure virus outbreak alert settings

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

To configure virus outbreak alert settings:

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

Configure special virus alert settings

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

To configure special virus alert settings:

1. Click **Administration** on the main menu.
2. On the left-hand 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**.

Use reports

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

Control Manager 3.0 categorizes reports according to the following types:

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

---

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

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

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

  Control Manager cannot send reports in ActiveX format as email attachments.
- RPT - Crystal Report format; use Crystal Smart Viewer to view *.RPT reports

When the Report Server finishes generating the report, it launches the default viewer for the report file format. For RPT reports, you need to have installed the Crystal Smart Viewer.

Create report profiles

Use the local or global Create Report Profile screen to create report profiles.

To create local or global report profile:

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-hand menu under Reports
   - To create a global report profile, click **Global Report Profile** on the left-hand menu under Reports
3. On the left-hand menu under Local Report Profile or Global Report Profile, click **Create Report Profile**.
4. Provide the information required by the following tabs:
   - **Contents**
     - **i.** On the working area under the Contents tab, type a **name** for the report in the Report name field. The name will identify this profile on the Local Reports screen.
     - **ii.** Type a **title** for the report in the Report Title field. This information is optional.
     - **iii.** Type a **description** of the report profile in the Description field. This information is also optional.
     - **iv.** Select the **report template** from the Select report template list.
     - **v.** Select the **report format**.
     - **vi.** Click **Next >** to proceed to the Targets tab.
   - **Targets**
     - **i.** On the working area under the Targets tab, select the **target** of the local or global report profile:
       - Select the **managed products** or **folders**

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

         The profile will only contain information about the child servers selected. Select the parent server to include all child servers' managed products in the profile.
     - **ii.** Click **Next >** to proceed to the Frequency tab.

- **Frequency**

  i. On the working area under the Frequency tab, specify **how often** Control Manager generates this report. The options are:

  - 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

  ii. 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

  iii. For scheduled reports, click **Number of reports to keep** and then specify the **instance** Control Manager will maintain on the server.

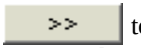
Note: Control Manager automatically enables a scheduled report profile. To temporarily disable generating reports, navigate to the Local or Global Scheduled Reports screen, and then clear the check box adjacent to the scheduled report profile.

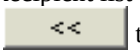
---

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

- **Recipient**

  i. 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

ii. 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.

iii. Click **Next >** to proceed to the Summary tab.

5. On the working area under the Summary tab, review the profile settings and then click **Finish** to save the profile.

Generate on-demand scheduled reports

The Report Server generates scheduled reports based on the date and time you specified. When the date and time has not yet commenced, use **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-hand menu under **Reports**
   - To create a global report profile, click **Global Report Profile** on the left-hand menu under **Reports**
3. On the working area under the **Available Reports** column, click the corresponding **View** link.
4. On the Available Reports for {profile name} under **Generate a Monthly report starting from**, specify the **starting month**, **day**, and **year**.
5. Click **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-hand menu under Reports
   - To create a global report profile, click **Global Report Profile** on the left-hand 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.

Chapter 6

Using Trend Micro Damage Cleanup Services™

Damage Cleanup Services (DCS) is a comprehensive Control Manager service which can remotely assess and clean (*Cleanup*) system damages without installing software on clients. It also removes virus remnants that could re-attack the network.

Damage Cleanup Services offers:

- Removal of unwanted registry entries created by worms or Trojans
- Removal of memory resident worms and Trojans
- Removal of garbage and viral files droppings from worms and Trojans
- Restoration of system configuration files after being altered or infected by malicious code

Damage Cleanup Services supports the following Microsoft platforms:

- Windows NT 4 Server/Workstation with Service Pack 6 or later
- Windows 2000 Professional/Server/Advanced Server with Service Pack 3
- Windows XP Professional
- Windows Server 2003 Standard/Enterprise edition

This chapter contains the following topics:

- *Features and Benefits* on page 6-3
- *Activating Damage Cleanup Services* on page 6-4
- *Accessing Damage Cleanup Services* on page 6-5
- *Downloading Updates* on page 6-6
- *Configuring Damage Cleanup Services* on page 6-7
- *Checking the status of a current task* on page 6-16
- *Using the damage cleanup history (task logs)* on page 6-16

Features and Benefits

Damage Cleanup Services offers the following features and benefits:

- **Centralized damage assessment reporting**: Damage Cleanup Services uses the latest damage cleanup engine (DCE) and damage cleanup template (DCT) to generate in depth damage assessment reports; reports are available by accessing the Control Manager Web console

  Damage assessment reports are essential to ensure optimal system performance, especially after an outbreak occurs. See *Using the damage cleanup history (task logs)* on page 6-16.

- **Regular and scheduled damage cleanup task creation**: use Damage Cleanup Services to create regular and scheduled damage cleanup tasks; regular damage cleanup tasks are performed on demand, whereas scheduled damage cleanup tasks are performed based on a specific schedule

  Damage cleanup tasks are easy to create and require very low maintenance. Once created, damage cleanup tasks can be quickly edited to meet administrator needs.

  The following two centralized management actions are available when performing tasks:

  - *Assessment only*: assessment on machines with possible virus remnants still in the network
  - *Cleanup*: assessment and cleanup including removal of virus remnants that could re-attack a network

  See *Managing Damage Cleanup tasks* on page 6-10 for additional information on how to configure damage cleanup tasks.

- **Remote damage cleanup task deployment**: use the Control Manager Web console to deploy damage assessment and cleanup tasks without installing any software on client machines; this feature helps minimize the amount of work for administrators

- **Seamless integration with other Control Manager services**: Damage Cleanup Services is easy to integrate with other Control Manager services such as Outbreak Prevention Services and Network VirusWall 1200

  In the event of an outbreak, Control Manager can prompt Damage Cleanup Services to assess and cleanup existing managed products (under the Product Directory) with minimal intervention. This reduces the risk of potential damage to your network and saves administrators deployment time.

- **Flexible update methods**: download the latest damage cleanup engine/template updates with or without user intervention; scheduled updates provide both flexibility and peace of mind

  It is important to have the latest updates to obtain the correct assessment and damage cleanup results. See *Downloading Updates* on page 6-6.

- **Real-time task monitoring**: view the status of damage cleanup tasks through the Control Manager Web console whenever there is a need for it

  This feature is quite useful to visually verify that Damage Cleanup Services is working properly. See *Checking the status of a current task* on page 6-16.

- **Hassle free machine selection**: Specify a range of IP addresses or a domain to select the target machines Damage Cleanup Services will deploy to; this effective approach will save you time when deploying Damage Cleanup Services to a large network

  Refer to *Selecting machines* in the online help for additional information.

Activating Damage Cleanup Services

You can activate Damage Cleanup Services during Control Manager Setup. Alternatively, activation can be performed after Setup using the Web console.

To find out how to activate Damage Cleanup Services during Control Manager Setup, see *Installing a Control Manager server* on page 3-6.

To activate Damage Cleanup Services from the Web console, do the following:

1. Login to the Control Manager Web console.
2. Click **Administration** on the main menu.
3. On the left-hand menu under **Registration**, click **License Information**.
4. On the working area under **Damage Cleanup Services License Information**, click the **Activate the product** link.
5. In the **New** box, enter 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.
6. Click **Activate**.
7. Click **OK**.

To renew product maintenance for a full version, do the following:

1. Login to the Control Manager Web console.
2. Click **Administration** on the main menu.
3. On the left-hand menu under **Registration**, click **License Information**.
4. On the working area under **Control Manager License Information**, click **Check Status Online**.
5. Click **OK**.

Accessing Damage Cleanup Services

After activating Damage Cleanup Services, use the Control Manager Web console to access this service.

To access Damage Cleanup Services, do the following:

1. Login to the Control Manager Web console.
2. Click **Services** on the main menu.
3. On the left hand menu, click **Damage Cleanup**. For additional information about the Damage Cleanup Services page, click the context sensitive help.

Downloading Updates

Before configuring Damage Cleanup Services, you should obtain the latest damage cleanup template (DCT) and damage cleanup engine (DCE) updates. This is essential for performing an accurate assessment and an effective damage cleanup.

- **Damage cleanup template**: displays the damage cleanup template in use

  The damage cleanup template includes the database for all malware (worms, Trojans, and backdoors) and works with the damage cleanup engine

- **Damage cleanup engine**: displays the damage cleanup engine in use

  The damage cleanup engine removes unwanted registry entries created by worms or Trojans, and memory resident worms or Trojans. The engine can also repair a system configuration file such as "*system.ini*" after it has been altered or infected by malicious code.

You can download damage cleanup templates manually or if you prefer you can define a schedule for downloads. For scheduled downloads, refer to *Enable scheduled component download* on page 5-27 for additional information.

To manually download the damage cleanup engine and template, do the following:

1. Login to the Control Manager Web console.
2. Click **Services** on the main menu.
3. On the left hand menu, click **Damage Cleanup**.
4. Click **Download Now**. The **Manual Download** screen appears.
5. Select **Pattern files/Cleanup templates** and **Engines** in the **Download Settings** group.
6. Select an update source.
7. Select a retry frequency.
8. Configure proxy settings (if not previously configured). To save your settings, click **Save**, and then **OK**.
9. Click **Download Now**.

Configuring Damage Cleanup Services

This section describes how to configure Damage Cleanup Services with the least amount of effort.

Damage Cleanup Services includes an account management tool which provides maximum protection when entering machine and domain login credentials. This tool is not accessible from the Control Manager Web console.

Note: Before configuring Damage Cleanup Services, please read *Using the Account Management Tool* on page 6-7.

Using the Account Management Tool

Use this tool to view, add, modify, or delete login credentials for the target machines and domains you wish to add in the **Select Machines** page.

This tool is only accessible from the machine hosting the Control Manager Server. When using the account management tool, you cannot input IP addresses.

WARNING! *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.*

To view all existing domains and machines, do the following:

1. Click **Start** > **Programs > 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.

To add a domain or machine, do the following:

1. Click **Start** > **Programs > 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, do the following:
     i. Type the Windows domain name you wish to add next to **Domain name**.
     ii. Type the domain administrator account next to **Domain administrator account**.
     iii. Type the password for the domain administrator account next to **Password**.
     iv. Retype the password entered in step iii next to **Confirm password**.
     v. Type a description for this account next to **Description**. For example, *Company domain 1*.
   - If you selected **Machine** in step 3, do the following:
     i. Type the machine name you wish to add next to **Machine name**.
     ii. Type the machine administrator account next to **Administrator account**.
     iii. Type the password for the machine administrator account next to **Password**.
     iv. Retype the password entered in step 3 next to **Confirm password**.
     v. Type a description for this account next to **Description**.
5. Click **Apply**.
6. Click **OK** to save this setting.
7. Click **OK** again, the domain appears in the list under **Accounts**.
8. Click **Exit** to close the tool.

To delete a domain or machine, do the following:

1. Click **Start** > **Programs > 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, do the following:

   i. Click the domain you wish to delete in the **Accounts** list.
   ii. Click **Delete**.
   iii. Type the password for the domain administrator account.
- If you selected **Machine** in step 2, do the following:
   i. Click the machine you wish to delete in the **Accounts** list.
   ii. Click **Delete**.
   iii. 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.

To modify domain or machine information, do the following:

1. Click **Start Programs > 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, do the following:
      i. Click the domain you wish to modify in the **Accounts** list.
      ii. Click **Modify**.
      iii. Type the updated domain information in **Domain name**, **Administrator account**, and **Description**. To change the password, type the new password in **New password** and **Confirm new password**.
      iv. Type the pre-existing password in **Old Password**.
   - If you selected **Machine** in step 2, do the following:
      i. Click the machine you wish to modify in the **Accounts** list.
      ii. Click **Modify**.
      iii. 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**.
      iv. 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.

Managing Damage Cleanup tasks

This section explains how to create, run, edit, delete, and view all existing regular and scheduled damage cleanup tasks.

Regular damage cleanup tasks are performed on demand, whereas scheduled damage cleanup tasks are performed based on a specific schedule.

Tasks provide central reporting back to the Control Manager server. The following two centralized management actions are available when performing tasks:

- **Assessment only**: assessment on machines with possible virus remnants still in the network
- **Cleanup**: assessment and cleanup including removal of virus remnants that could re-attack a network

You can select target machines by machine name/domain, or IP/IP address range. refer to *Selecting machines* in the online help for additional information.

To create a task, do the following:

1. Login to the Control Manager Web console.
2. Click **Services** on the main menu.
3. On the left hand menu, click **Tasks**.
4. Under **Damage Cleanup Scheduled Tasks,** click **Add a New Task...**. The **Create a Damage Cleanup Task** screen appears.
5. Type the name of the task in **Name**. Valid name strings can be up to 48 characters long. The following characters are not allowed: **\ / : * ? " < > | & ‘** For example, *iT#3-01-03-2004-mP.*
6. In **Step 1 of 3**, click **Select Machines** to select the target machines for this task. A Trend Micro security certificate window will appear. Accept the certificate to proceed with machine selection. You can select machines by machine name or IP address. If you select the **By machine name** option, see *Using the Account Management Tool* on page 6-7.

After machine selection, the target machines will appear under **Selected Machines**. Click the context sensitive help for additional information on how to select machines.

7. In **Step 2 of 3**, do the following:
   a. Select one of the following:
      - **One time on month - day - year**: select this option to specify the exact date when a task should run once

        Select a month, day, and year from each drop down menu.

        For example, when selecting *One time on January 01 2003*, this task will run once on the specified date.
      - **Every day**: select this option to run a task everyday
      - **Every number of weeks on day of week**: select this option to specify how often a task should run once

        Select the number of weeks (1 through 4) and the day of the week (Sunday through Saturday) from each drop down menu.

        For example, when selecting **Every 1 week on Sunday**, this task will run once every week 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 each drop down menu.

        For example, when selecting *Every month on 1st day of the month*, this task will run on the first day of each 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 the **Tasks** section.

   b. Select the starting time for the task from the two drop down menus. The first drop down menu shows the hours (**00 - 23**). The second drop down menu displays the minutes (**00 - 59**).

      For example, for *11:34 P.M.*, select **23** in the hours drop down menu, and **34** in the minutes drop down menu.

8. In **Step 3 of 3**, select the action the task will perform. The two actions tasks can perform are **Assessment only** and **Cleanup**.

Note: To learn how to simultaneously perform a Vulnerability Assessment task, refer to *Creating a Damage Cleanup Task* on the online help.

9. Click **Save** to save this task and return to the **Damage Cleanup Tasks** section. Alternatively, click **Cancel**.

To run a task, do the following:

1. Login to the Control Manager Web console.
2. Click **Services** on the main menu.
3. On the left hand menu, click **Tasks**. The **Damage Cleanup Scheduled Tasks** screen appears**.**
4. Select a task from the table.
5. Click **Run Now**. A confirmation message appears.
6. Click **OK** to go to the **Current task** screen.

   If the task was running before clicking **Run Now**, a page informing the task is currently running will appear. Click **OK** to return to the **Damage Cleanup Scheduled Tasks** screen.

To edit a task, do the following:

1. Login to the Control Manager Web console.
2. Click **Services** on the main menu.
3. On the left hand menu, click **Tasks**. The **Damage Cleanup Scheduled Tasks** screen appears**.**
4. Select a task from the table, and then click **Edit...**.
5. To modify the task name, type a new name in **Name**. Valid name strings can be up to 48 characters long. The following characters are not allowed: **\ / : * ? " < > |& ‘** For example, *iT#3-01-03-2004-mP.*
6. In **Step 1 of 3**, click **Select Machines** to modify the target machines for this task. A Trend Micro security certificate window will appear. Accept the certificate to proceed with machine selection. You can select machines by machine name or IP address. If you select the **By machine name** option, see *Using the Account Management Tool* on page 6-7.

After machine selection, the target machines will appear under **Selected Machines**. Click the context sensitive help for additional information on how to select machines.

7. In **Step 2 of 3**, do the following to modify the schedule settings:
   a. Select one of the following:
      - **One time on month - day - year**: select this option to specify the exact date when a task should run once

        Select a month, day, and year from each drop down menu.

        For example, when selecting *One time on January 01 2003*, this task will run once on the specified date.
      - **Every day**: select this option to run a task everyday
      - **Every number of weeks on day of week**: select this option to specify how often a task should run once

        Select the number of weeks (1 through 4) and the day of the week (Sunday through Saturday) from each drop down menu.

        For example, when selecting **Every 1 week on Sunday**, this task will run once every week 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 each drop down menu.

        For example, when selecting *Every month on 1st day of the month*, this task will run on the first day of each 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 the starting time for the task from the two drop down menus. The first drop down menu shows the hours hh (**00** - **23**). The second drop down menu displays the minutes mm (**00** - **59**).

      For example, for *11:34 P.M.*, select **23** in the hours drop down menu, and **34** in the minutes drop down menu.
8. In **Step 3 of 3**, select the new action the task will perform. The two actions tasks can perform are **Assessment only** and **Cleanup**.

Note: To learn how to simultaneously perform a Vulnerability Assessment task, refer to *Creating a Damage Cleanup Task* on the online help.

9. Click **Save** to save the task modifications and return to the **Damage Cleanup Tasks** screen. Alternatively, click **Cancel**.

To delete a task, do the following:

1. Login to the Control Manager Web console.
2. Click **Services** on the main menu.
3. On the left hand menu, click **Tasks**. The **Damage Cleanup Scheduled Tasks** screen appears**.**
4. Select a task from the table.
5. Click **Delete**. A confirmation message appears.
6. Click **OK** to proceed. The **Delete a Task** screen appears, click **OK** to delete the task and return to **Damage Cleanup Scheduled Tasks**.

Note: Running tasks cannot be deleted.

To view all existing tasks, do the following:

1. Login to the Control Manager Web console.
2. Click **Services** on the main menu.
3. Do one of the following:
   - On the left hand menu, click **Tasks**. The **Damage Cleanup Scheduled Tasks** screen appears displaying all existing tasks.
   - On the left hand menu, click **Damage Cleanup**, and then click **view all the scheduled tasks** under **Damage Cleanup Services**. The **Damage Cleanup Scheduled Tasks** screen appears displaying all existing tasks.

Using the manual Damage Cleanup tool

Trend Micro provides a Manual Damage Cleanup tool for the following Microsoft Windows based machines:

- Windows 95
- Windows 98
- Windows ME
- Windows XP Home 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 XP Professional
- Windows Server 2003 Standard/Enterprise Edition

The system administrator can make this tool available to users when Damage Cleanup Services is unable to deploy a pre-configured *Cleanup* task (when a machine is not accessible or if it appears as **Unsupported**). Users can then manually assess and Cleanup their machine(s).

Note: The Damage Cleanup Services system administrator should provide users with the URL listed below.

To use the manual Damage Cleanup tool, do the following:

1. From the client machine you wish to Cleanup, go to the following URL:

   `http://CM Server/ControlManager/cgi-bin/dcs/CGIDcsx.exe`

   Where "CM Server" is the name of the Control Manager Server where Damage Cleanup Services is installed. The **TREND MICRO Manual Damage Cleanup Tool** ActiveX page appears.

2. Click **Start Damage Cleanup** to run a *Cleanup* task on the local machine. The **Cleanup progress** status bar appears displaying the name of the target machine and the status of the *Cleanup* task. Click **Stop** if you wish to interrupt the task.

   When the *Cleanup* task is complete, you can view the result under **Damage Cleanup Result**. If Damage Cleanup Services finds any damage, it will also display the type of malware.

For example, **Result**: *Damage Cleaned* **Virus Name**: *WORM_KLEZ.H*

Checking the status of a current task

This page describes how to check the status of a current damage cleanup task.

To see the status of the current damage cleanup task, do the following:

1. Login to the Control Manager Web console.
2. Click **Services** on the main menu.
3. On the left hand menu, click **Current Task.**
4. Click **Refresh,** to see the most updated status of a current damage cleanup task.

Note: This page is refreshed automatically every 2 minutes.

For additional information, click on the context sensitive help button in the **Current Task** section.

Using the damage cleanup history (task logs)

Use the **History** page to generate and save reports (logs) for damage cleanup task results based on customized queries. Damage Cleanup Services allows you to do the following:

- Create log queries based on task results
- Create log queries for specific tasks
- Create customized log queries

To view the History section, do the following:

1. Login to the Control Manager Web console.
2. Click **Services** on the main menu.
3. On the left hand menu, click **History.** The **Damage Cleanup History** page appears.

Note: To find out additional information about creating and saving log queries, click the context sensitive help button in the **Damage Cleanup History** section.

Chapter 7

Introducing Trend Micro Vulnerability Assessment™

Trend Micro Vulnerability Assessment™ is an integrated component of Control Manager that is accessed and controlled through the Control Manager console.

This chapter contains the following topics:

- *What is Vulnerability Assessment?* on page 7-2
- *What Are the Benefits and Capabilities of Vulnerability Assessment?* on page 7-3
- *Activating Vulnerability Assessment* on page 7-4
- *Accessing Vulnerability Assessment* on page 7-5
- *Downloading Updates* on page 7-5
- *Configuring Vulnerability Assessment* on page 7-6
- *Using Vulnerability Assessment* on page 7-6

What is Vulnerability Assessment?

Vulnerability Assessment provides system administrators or other network security personnel with the ability to assesses 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.

Vulnerability Assessment supports the following Microsoft platforms:

Servers:

- Windows NT 4 Server with Service Pack 6 or later
- Windows 2000 Server/Advanced Server with Service Pack 3
- Windows Server 2003 Standard/Enterprise edition

Clients:

- Windows NT 4 Server/Workstation with SP 6 or later
- Windows 2000 Professional/Server/Advanced Server with SP3 or later
- Windows XP Professional
- Windows Server 2003 Standard/Enterprise edition
- (Only supports remote deploy ActiveX control agent)
- Windows 9x / ME
- Windows XP Home

What Are the Benefits and Capabilities of Vulnerability Assessment?

Vulnerability Assessment offers the following features and benefits:

Centralized assessment reporting: Vulnerability Assessment uses the latest Vulnerability Assessment Engine (VAE) and Vulnerability Assessment pattern file (VAP) to generate in depth assessment reports; reports are available by accessing the Control Manager Web console.

Regular and scheduled assessment task creation: use Vulnerability Assessment to create regular and scheduled assessment tasks; regular assessment tasks are performed on demand, whereas scheduled assessment tasks are performed based on a specific schedule.

Assessment Tasks are easy to create and require very low maintenance. Once created, tasks can be quickly edited to meet administrator needs.

Remote assessment task deployment: use the Control Manager Web console to deploy assessment and enforcement tasks without installing any software on client machines; this feature helps minimize the amount of work for administrators.

Seamless integration with other Control Manager services: Vulnerability Assessment is easy to integrate with other Control Manager products and services such as Outbreak Prevention Services, Damage Cleanup Services and Network VirusWall 1200.

Flexible update methods: download the latest component updates; scheduled updates provide both flexibility and peace of mind.

Hassle free machine selection: Specify a range of IP addresses or a domain to select the target machines Vulnerability Assessment will deploy to; this effective approach will save you time when deploying Vulnerability Assessment to a large network.

Refer to Selecting machines in the online help for additional information.

Activating Vulnerability Assessment

You can activate Vulnerability Assessment during Control Manager Setup. Alternatively, activation can be performed after Setup using the Web console.

To find out how to activate Vulnerability Assessment during Control Manager Setup, see *Installing a Control Manager server* on page 3-6.

To activate Vulnerability Assessment from the Web console, do the following:

1. Login to the Control Manager Web console.
2. Click **Administration** on the main menu.
3. On the left-hand menu under **Registration**, click **License Information**.
4. On the working area under **Vulnerability Assessment License Information**, click the **Activate the product** link.
5. In the **New** box, enter 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.
6. Click **Activate**.
7. Click **OK**.

To renew product maintenance for a full version, do the following:

1. Login to the Control Manager Web console.
2. Click **Administration** on the main menu.
3. On the left-hand menu under **Registration**, click **License Information**.
4. On the working area under **Control Manager License Information**, click **Check Status Online**.
5. Click **OK**.

Accessing Vulnerability Assessment

After activating Vulnerability Assessment, use the Control Manager Web console to access this product.

To access Vulnerability Assessment, do the following:

1. Login to the Control Manager Web console.
2. Click **Services** on the main menu.
3. Click **Vulnerability Assessment** on the left-hand menu or in the main window.

Note: For additional information about the Vulnerability Assessment page, click Learn More for context sensitive help.

Downloading Updates

Before configuring Vulnerability Assessment, you should obtain the latest Vulnerability Assessment pattern file (VAP) and Vulnerability Assessment Engine (VAE) updates. This is essential for performing an accurate vulnerability assessment.

- The Vulnerability Assessment pattern file includes the database for all vulnerabilities. It provides the instructions for the VAE to scan for known vulnerabilities.
- The Vulnerability Assessment Engine is the component that performs the scan of the computers attached to your network to identify vulnerabilities.

Your current VAE and VAP are displayed in the **Vulnerability Assessment** screen. Available updates are displayed in the **Services Summary** screen of the Control Manager console under **TrendLab Message Board**.

You can download patterns manually or if you prefer you can define a schedule for downloads. For scheduled downloads, refer to *Enable scheduled component download* on page 5-27 for additional information.

To manually download the Vulnerability Assessment engine and pattern, do the following:

1. Login to the Control Manager Web console.
2. Click **Services** on the main menu.
3. On the left hand menu, click **Vulnerability Assessment**.
4. Click **Download Now**. The **Download Now** screen appears.
5. Select Pattern files and Engines in the Download Settings group.
6. Select an update source.
7. Select a retry frequency.
8. Configure proxy settings (if not previously configured). To save your settings, click Save, and then OK.
9. Click **Download Now**.

Configuring Vulnerability Assessment

This section describes how to configure Vulnerability Assessment with the least amount of effort.

Vulnerability Assessment includes an account management tool which provides maximum protection when entering machine and domain login credentials. This tool is not accessible from the Control Manager Web console.

Note: Before configuring Vulnerability Assessment, please read *Using the Account Management Tool* on page 6-7.

Using Vulnerability Assessment

System Administrators or other network security personnel can use Vulnerability Assessment to quickly assess the security risks to their networks. Once all unacceptable security vulnerabilities are resolved, they can continue to use Vulnerability Assessment to monitor and report on their network to avoid further security risks being introduced.

Creating and Running Tasks

The process of assessing the vulnerabilities is centered on the assessment task. Tasks provide central reporting back to the Control Manager server.

System Administrators or other network security personnel use assessment tasks to assess security risks as follows:

1. They use the Account Manager Tool to identify all the computers to include in the tasks.
2. They create the 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.
3. The assessment tasks log the results and store them on the Control Manager server. Administrators can view these results immediately or 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.

Understanding Assessment Results

After performing an assessment task, Vulnerability Assessment displays 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 and severity of the vulnerability on each computer. Vulnerability Assessment includes the number of machines for which the deploy failed in the results total.

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.

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 the vulnerabilities that are located on the machine determines the overall security risk level. The assessment status terms are defined as follow:

Note: All vulnerabilities that are known to be exploited by malicious code are automatically promoted to critical risk level.

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.

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 *Using the Account Management Tool* on page 6-7 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.

Understanding Enforcement

Not only can Vulnerability Assessment provide an assessment of security risks, but it can also request blocking of clients that present an unacceptable level of risk to the network. This feature is set using **Auto Enforcement** in the **Global Settings** screen.

Note: Vulnerability Assessment cannot enable enforcement without Network VirusWall. To purchase Network VirusWall, find a reseller through the Trend Micro Web site at http://www.trendmicro.com.

What is Enforcement?

Enforcement means a machine is quarantined from the network, or blocked. Blocked machines can access a secure Web site where they receive a manual assessment. 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).

Note: For more information about blocking, refer to Network VirusWall 1200 User's Guide and Online Help.

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, deploy failed or unassessed machines. Global exceptions, also set through the **Global Settings** screen, override any enforcement setting.

Note: Unassessed machines are not excluded from enforcement

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?

	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.

Managing Vulnerability Assessment tasks

Tasks provide central reporting back to the Control Manager server. The following two centralized management actions are available when performing tasks:

- Assessment only: Scan any or all of the clients attached to your network to identify vulnerabilities that present a security risk.
- Assessment with Enforcement: Vulnerability Assessment will instruct Network VirusWall to enforce blocking on those clients which present an unacceptable level of risk as defined by the user.

  Example: enable enforcement for all clients that present a critical risk or enable enforcement for all clients that have the MS03-039 vulnerability.

Note: Vulnerability Assessment cannot enable enforcement without Network VirusWall. You must install Network VirusWall to block a client. To obtain Network VirusWall, find a reseller through the Trend Micro Web site at http://www.trendmicro.com.

To create a task, do the following:

1. Login to the Control Manager Web console.
2. Click **Services** on the main menu.
3. Click **add a new task** in the main Vulnerability Assessment window and the **Create a Vulnerability Assessment** screen appears.

   Or, first open the **Tasks** window by clicking **Tasks** on the left-hand menu and then click **Add a New Task...** in this window to open the **Create a Vulnerability Assessment Task** screen.
4. Type the name of the task in Name. Valid name strings can be up to 48 characters long. The following characters are not allowed: \ / : * ? " < > | & ‘ For example, iT#3-01-03-2004-mP.
5. In **Step 1 of 3**, click **Select Machines** to select the target machines for this task. A Trend Micro security certificate window will appear. Accept the certificate to proceed with machine selection. Select target machines by machine name/domain, or IP/IP address range. Refer to *Using the Account Management Tool* on page 6-7 for more information.

After machine selection, the target machines will appear under **Selected Machines**. Click the context sensitive help for additional information on how to select machines.

Tip: Vulnerability Assessment only scans clients included in the list you made using the Account Management Tool. If you do not know the domain or computer name of all the clients who attach to the network, ensure that Vulnerability Assessment scans all the clients by setting up a Task that scans according to IP range. For example, if a new laptop attaches to the network. Vulnerability Assessment runs an assessment task, but it cannot recognize the laptop (there is no name for that laptop on the list). However, if you make a task that scans by IP range, and the laptop IP address falls within this range, then it is included in the assessment task.

6. In **Step 2 of 3**, do the following:
   a. Select one of the following:
      - **One time on month - day - year**: select this option to specify the exact date when a task should run once

        Select a month, day, and year from each drop down menu.

        For example, when selecting **One time on January 01 2003**, this task will run once on the specified date.
      - **Every day**: select this option to run a task every day
      - **Every number of weeks on day of week**: select this option to specify how often a task should run once

        Select the number of weeks (1 through 4) and the day of the week (Sunday through Saturday) from each drop down menu.
      - **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 each drop down menu.

        For example, when selecting **Every month on 1st day of the month**, this task will run on the first day of each 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 the **Tasks** section.

b. Select the starting time for the task from the two drop down menus. The first drop down menu shows the hours hh (00 - 23). The second drop down menu displays the minutes mm (00 - 59).

For example, for 11:34p.m., select **23** in the hours drop down menu, and **34** in the minutes drop down menu.

7. In **Step 3 of 3**, select one of the following:

a. Assess 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:

`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.

Note: Vulnerability Assessment cannot enable enforcement without Network VirusWall. You must install Network VirusWall 1200 to block a client. To purchase Network VirusWall, find a reseller through the Trend Micro Web site at http://www.trendmicro.com

---

b. 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.

8. 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 an 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.

   Refer to Using Trend Micro Damage Cleanup Services™ on page 6-1 for more information.

9. Click **Save** to save this task and return to the Vulnerability Assessment Tasks section. Click **Cancel** to return to the Vulnerability Assessment Tasks section without saving the task.

To run a task, do the following:

1. Login to the Control Manager Web console.
2. Click **Services** on the main menu.
3. On the left hand menu, under **Vulnerability Assessment**, click **Tasks**. The **Vulnerability Assessment Scheduled Tasks** screen appears**.**
4. Select a task from the table.
5. Click **Run Now**. A confirmation message appears.
6. Click **OK** to go to the **Current Task** screen.

   If the task was running before clicking **Run Now**, a page informing the task is currently running will appear. Click **OK** to return to the Vulnerability **Assessment Scheduled Tasks** screen.

To edit a task, do the following:

1. Login to the Control Manager Web console.
2. Click **Services** on the main menu.
3. On the left hand menu under **Vulnerability Assessment**, click **Tasks**. The **Vulnerability Assessment Tasks** screen appears**.**
4. Select a task from the table and click **Edit...**. The **Create a Vulnerability Assessment Task** screen appears.
5. To modify the task name, type a new name in **Name**. Valid name strings can be up to 48 characters long. The following characters are not allowed: **\ / : * ? " < > |& ‘** For example, iT#3-01-03-2004-mP.
6. In **Step 1 of 3**, click **Select Machines** to modify the target machines for this task.

   A Trend Micro security certificate window will appear. Accept the certificate to proceed with machine selection. You can select machines by machine name or IP address. Refer to *Using the Account Management Tool* on page 6-7 for more information.

   After machine selection, the target machines will appear under **Selected Machines**. Click the context sensitive help for additional information on how to select machines.
7. In **Step 2 of 3**, do the following to modify the schedule settings:
   a. Select one of the following:
      - **One time on month - day - year**: select this option to specify the exact date when a task should run once

        Select a month, day, and year from each drop down menu.

        For example, when selecting **One time on January 01 2003**, this task will run once on the specified date.
      - **Every day**: select this option to run a task every day
      - **Every number of weeks on day of week**: select this option to specify how often a task should run once

        Select the number of weeks (1 through 4) and the day of the week (Sunday through Saturday) from each drop down menu.

        For example, when selecting **Every 1 week on Sunday**, this task will run once every week 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 each drop down menu.

  For example, when selecting **Every month on 1st day of the month**, this task will run on the first day of each 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 the starting time for the task from the two drop down menus. The first drop down menu shows the hours hh (00 - 23). The second drop down menu displays the minutes mm (00 - 59).

For example, for 11:34p.m., select **23** in the hours drop down menu, and **34** in the minutes drop down menu.

8. In **Step 3 of 3**, select one of the following:

a. Assess 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: `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.

Note: Vulnerability Assessment cannot enable enforcement without Network VirusWall. You must install Network VirusWall to block a client. To purchase Network VirusWall, find a reseller through the Trend Micro Web site at http://www.trendmicro.com

---

b. 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.

9. 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.

Refer to Using Trend Micro Damage Cleanup Services™ on page 6-1 for more information.

10. Click **Save** to save the task modifications and return to the **Vulnerability Assessment Tasks** screen. Click **Cancel** to return to the Vulnerability Assessment Tasks section without saving the task.

To delete a task, do the following:

1. Login to the Control Manager Web console.
2. Click **Services** on the main menu.
3. On the left hand menu under **Vulnerability Assessment**, click **Tasks**. The **Vulnerability Assessment Tasks** screen appears**.**
4. Select a task from the table.
5. Click **Delete**. A confirmation message appears.
6. Click **OK** to proceed. The **Delete a Task** screen appears, click **OK** to delete the task and return to **Vulnerability Assessment Scheduled Tasks**.

Note: Running tasks cannot be deleted.

To view all existing tasks, do the following:

1. Login to the Control Manager Web console.
2. Click **Services** on the main menu.
3. Do one of the following:
   - On the left hand menu, under Vulnerability Assessment, click **Tasks**. The **Tasks** screen appears, displaying all existing tasks.
   - On the left hand menu, click Vulnerability Assessment, and then click **view all the scheduled tasks** under Vulnerability Assessment. The **Tasks** screen appears, displaying all existing tasks.

Using 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.

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.

To see the status of the current Vulnerability Assessment task, do the following:

1. Login to the Control Manager Web console.
2. Click **Services** on the main menu.
3. On the left hand menu, under **Vulnerability Assessment,** click **Current Task.**
4. Click **Refresh,** to see the most updated status of a current assessment task.

Note: This page is refreshed automatically every 2 minutes.

For additional information, click the context sensitive help button in the **Current Task** section.

Generating Reports

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.

Vulnerability Assessment History allows you to do the following:

- 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 reports to compare in a single report. The query result displays comparative information based on logs and individual machines. You can export the query result to a comma-separated values file format.

To view the History section, do the following:

1. Login to the Control Manager Web console.
2. Click **Services** on the main menu.
3. On the left hand menu, under **Vulnerability Assessment,** click **History.** The **Vulnerability Assessment History** page appears.

To find out additional information about creating and saving log queries, click the context sensitive help button in the **Vulnerability Assessment History** section.

Setting Global Enforcement 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**, **Deploy failed** or when Vulnerability Assessment cannot assess them (**Unassessed**). 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.

To configure actions for machines that use the Manual Vulnerability Assessment Tool:

- **Assess 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:
  `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.

Chapter 8

Using Tools

Control Manager 3.0 provides a number of tools to help you with specific configuration tasks.

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

- *Agent Migration Tool (AgentMigrateTool.exe)* on page 8-2
- *Cascading Management Structure Tool (CasTool.exe)* on page 8-2
- *IIS Restoration Tool (SetupPatch.exe)* on page 8-5
- *Web Server and Port Configuration Tool (CMWebCfg.bat)* on page 8-6

Agent Migration Tool (AgentMigrateTool.exe)

The Agent Migration tool provided in Control Manager 3.0 Standard or Enterprise edition performs two essential functions:

- Generate a migration list (see page 4-13), that identifies all agents used by managed products administered by a Control Manager 2.5 or Control Manager 3.0 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 3.0 servers.

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

- Migrate agents administered by a Trend VCS 1.8x, Control Manager 2.5x, or Control Manager 3.0 server (see *Migrate Trend VCS or Control Manager agents* on page 4-12)

  Run `AgentMigrateTool.exe` directly on the destination server.

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 10-2).

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`:

TABLE 8-1. `CasTool.exe` commands

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 8-1. `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 8-1. `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.

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:

- Attempted to upgrade from Trend VCS to Control Manager, but the installation procedure was unsuccessful

  Run this tool to revive Trend VCS functions.

- Completed a migration 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.

Run SetupPatch.exe on the server where Trend VCS 1.8x or Control Manager 2.5x functions are to be restored.

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

Chapter 9

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 9-2
- *Remove a Windows-based Control Manager agent* on page 9-2
- *Manually removing Control Manager* on page 9-6

Remove a Control Manager server

There are two ways to automatically remove Control Manager (the following instructions are based on 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 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.

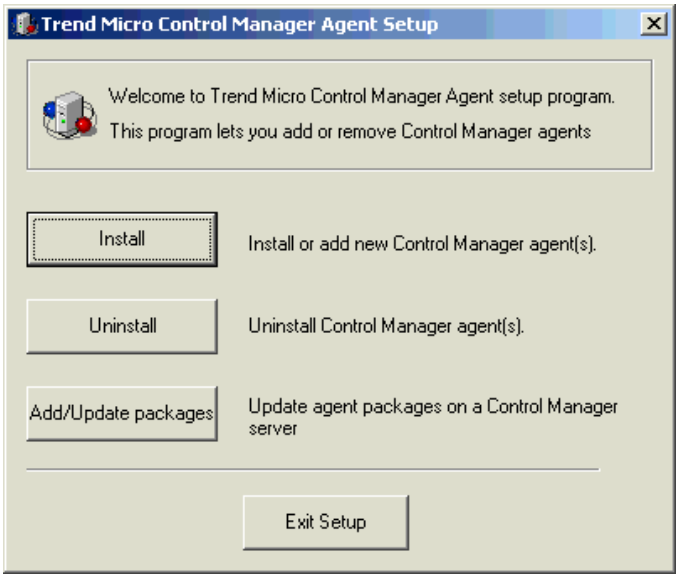


FIGURE 9-1. Trend Micro Agent setup program

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

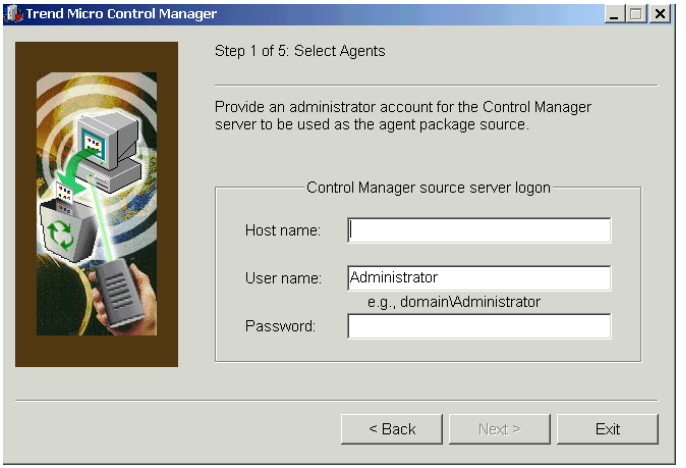


FIGURE 9-2. Control Manager source server logon

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 where the agents are to be removed. There are two ways to do this:
    - **To select from the list:**
      i. 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.
      ii. 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 chosen domain.

    Alternatively, you can double-click on a server to add it to the left-hand list.
    - **To specify a server name directly:**
      i. Enter the server's FQDN or IP address in the **Server name** field.

ii. 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, 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.

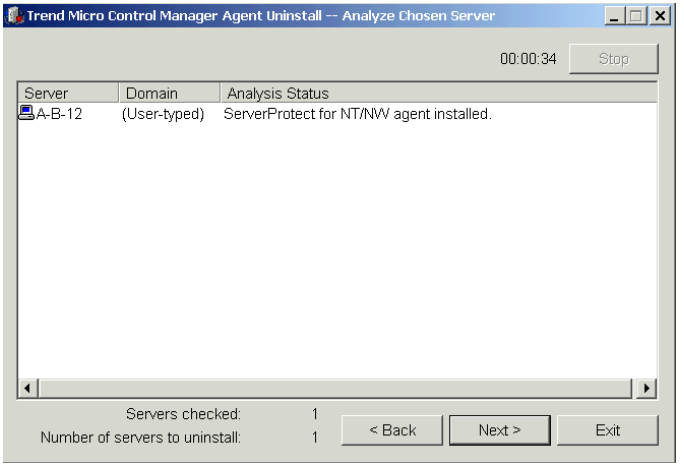


FIGURE 9-3. Analyze chosen Control Manager

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

There are two ways to do this, either from the Services screen, or from 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 9-4. 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-hand 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

Using MS Explorer, delete all files under the Control Manager folder. By default the folder is located at:

```
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

The Trend Micro Management Infrastructure (TMI) -- the communication backbone of the Control Manager system -- can be removed manually in three steps:

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

Stop the TMI service

There are two ways to do this, either from the Services screen, or from 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

There are two ways to do this, either from the Services screen, or from 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

There are two ways to do this, either from the Services screen, or from 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 10

Getting Support

Trend Micro is committed to providing service and support that exceeds our user's 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 10-2
- *Contacting Technical Support* on page 10-2
- *TrendLabs™* on page 10-3
- *Other Useful Resources* on page 10-3

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://kb.trendmicro.com/solutions/solutionSearch.asp`

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://kb.trendmicro.com/solutions/solutionSearch.asp`

- 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 that provide continuous 24 x 7 coverage to Trend Micro customers around the world.

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

System Checklists

Use the checklists in this appendix to record relevant system information. They will be needed from time to time.

Server address checklist

The following server address information is required during installation, and for configuring the Control Manager server to work with your network. Record them here for easy reference.

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
Control Manager server information		
IP address	10.1.104.255	
Fully Qualified Domain Name (FQDN)	server.company.com	
NetBIOS (host) name	yourserver	
Web server information		
IP address	10.1.104.225	
Fully Qualified Domain Name (FQDN)	server.company.com	
NetBIOS (host) name	yourserver	

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
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)		
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	

Control Manager requires 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:\MyDocu-ments\E2EPulic.dat	

You can use any User ID in lieu of the Root account User ID. However, Trend Micro recommends using the Root account because if you delete the User ID specified during agent installation, you will have difficulty managing the agent.

PRODUCT NAME	ADMINISTRATOR-LEVEL ACCOUNT	IP ADDRESS	HOSTNAME
Sample	Admin	10.225.225.225	PH-antivirus

Appendix B

Trend Virus Control System and Trend Micro Control Manager Feature Comparison

The following table presents a comparison of Trend Virus Control System (TVCS) and Trend Micro Control Manager (TMCM) features.

FEATURE	TVCS	TMCM				
	1.84	2.0	2.1	2.5	3.0 Enterprise	3.0 Standard
Agent interfaces with the Products	●	●	●	●	●	●
Automatic component (for example, patterns/rules) update	●	●	●	●	●	●
Cascading management structure					●	
Central database for all virus log and system events	●	●	●	●	●	●
Centralized, web-based, virus management solution for the enterprise	●	●	●	●	●	●
Child server monitoring					●	

FEATURE	TVCS	TMCM				
	1.84	2.0	2.1	2.5	3.0 Enterprise	3.0 Standard
Child server reporting					●	
Child server task issuance					●	
Command Tracking		●	●	●	●	●
Communicator Heartbeat		●	●	●	●	●
Communicator Scheduler		●	●	●	●	●
Configuration by Group				●	●	●
Consistent managed product and Control Manager UI				●	●	●
Damage Cleanup Services					●	●
Deployment Plans		●	●	●	●	●
Directory Manager			●	●	●	●
Enhanced Security Communication	●	●	●	●	●	●
Event Center		●	●	●	●	●
Control Manager MIB File (previously, HP™ OpenView™ SNMP Tool)		●	●	●	●	●
Improved Navigation			●	●	●	●
Improved User Interface			●	●	●	●
InterScan Web Security Service integration					●	●
LDAP for storing Product Tree objects and attributes	●					

FEATURE	TVCS	TMCM				
	1.84	2.0	2.1	2.5	3.0 Enterprise	3.0 Standard
Manage antivirus and content security products	●	●	●	●	●	●
Manage services					●	●
Managed product reporting	●			●	●	
MDSE or Microsoft SQL 7/2000 database		●	●	●	●	●
MSN Messenger notification					●	●
Notification and Outbreak Alert	●	●	●	●	●	●
Outbreak Commander / OPS - Automatic Download and Deployment of OPP				●	●	●
Outbreak Commander / OPS - Manual Download and Deployment of OPP			●	●	●	●
Outbreak Commander / Outbreak Prevention Services (OPS)			●	●	●	●
Passive Support for 3rd Party Product	●			●	●	●
Remote and Local Agent Installation	●	●	●	●	●	●
Remote management	●	●	●	●	●	●
Secure communication between Server and Agents		●	●	●	●	●
SSL support for ActiveUpdate					●	●
SSL support for management console					●	●

FEATURE	TVCS	TMCM				
	1.84	2.0	2.1	2.5	3.0 Enterprise	3.0 Standard
Trend Micro Network VirusWall 1200 integration					●	●
Trend Micro Product Registration server integration					●	●
TrendLabs Message Board					●	●
Supports Trend VCS agents	●	●	●	●	●	●
Support Control Manager agents		●	●	●	●	●
User Manager			●	●	●	●
Vulnerability Assessment					●	●
Work-hour control		●	●	●	●	●

Index

Symbols

"Log on as batch job" policy 5-32

A

access rights
  Configure 5-11
  Edit Directory 5-11
  Execute 5-10
  setting 5-10
  View 5-10
Accessing Damage Cleanup Services 6-5
Account Management Tool 7-6
activating
  Control Manager 3-11, 3-50
  Damage Cleanup Services 3-11–3-12
  Outbreak Prevention Services 3-11–3-12
  services 3-11
  Vulnerability Assessment 3-11–3-12
activating Control Manager 3-51
Activating Damage Cleanup Services 6-4
activating Vulnerability Assessment 7-4
Activation Code 1-5, 3-51
Activation Codes 3-11
adding
  user accounts 5-11
  user groups 5-14
address, checklist A-1
Administration Plan 2-8
  centralized management 2-8
  decentralized management 2-8
agent 3-27
  Control Manager
    installation 3-33
    setup program *See RemoteInstall.exe*
  installation 3-28
    checklist A-4
    programs 3-28
  InterScan Messaging Security Suite 3-29
  package *See RemoteInstall.xml*
  Trend VCS
    installation 3-41
    setup program. *See CMAgentsetup.exe*
Agent Migration Tool 8-2
  migrating agents 8-2
  migration list 8-2
AgentMigrateTool.exe. See Agent Migration Tool
agents
  installation tool 3-27
  installing Control Manager 3-25
  NetScreen Firewall 3-46
  obtaining packages 3-29
  obtaining required files 3-28
  preparing for installation 3-25
  remote installation 3-27
  removing Windows-based 9-2
  verifying successful installation 3-49
audience 1-ii

B

back up. See backing up Control Manager 2.5 information

C

calling CasTool.exe 8-2
cascading management console 1-4
cascading management structure
  child servers 5-19
  feature comparison 5-20
  parent server 5-19
Cascading Management Structure Tool 8-2
  commands 8-2
    /c 8-4
    /d 8-5
    /f 8-4
    /n 8-3
    /p 8-3
    /s 8-5
cascading structure tree tabs 5-21
CasTool.exe commands 8-3
CasTool.exe. See Cascading Management Structure Tool
CCGI *See Common CGI*
Checking the status of a current task 6-16
checklist
  agent installation A-4
  ports A-3
  server address A-1

child servers
configuring 5-20
managing 5-19
registering 5-22
tab 5-21
unregistering 5-23
CMAgentSetup.exe 3-27, 3-41
CMWebCfg.bat 8-6
CMWebCfg.bat. See Web Server and Port Configuration Tool
command prompt
Common CGI, stopping service from 9-11
Control Manager, stopping service from 9-7
Trend Micro Management Infrastructure, stopping service from 9-9
Command Tracking 5-38
query and view commands 5-39
Common CGI
command prompt, stopping service from 9-11
location, files 9-11
registry key 9-11
remove 9-10
comparison
cascading management structure 5-20
Enterprise edition and Standard edition 1-7
components
downloading 5-25
updating out-of-date items 5-35
configuring
child servers 5-20
proxy server connection for component download and Trend VCS agents 5-30
scheduled download automatic deployment settings 5-29
scheduled download settings 5-28
user accounts 5-7
Configuring Damage Cleanup Services 6-7
configuring Vulnerability Assessment 7-6
Control Manager 1-1
accounts 5-7
activating 3-11, 3-50–3-51
agent 1-9
installation 3-33
antivirus and content security components 5-25
architecture 1-8
basic features 1-2
command prompt, stopping service from 9-7
configuring accounts 5-7
deployment. See deployment architecture and strategy
how many 2-3
installation steps 3-7
installing 3-1, 3-7
installing agents 3-25
mail server 1-8
managed product 5-16
manually removing 9-6
migrating database 4-14
new features in version 3.0 1-3
notifications 5-40
preparing for agent installation 3-25
registering 3-11, 3-50
remove manually 9-6
removing overview 9-1
removing server 9-2
removing Windows-based agent 9-2
report server 1-8
report types 5-44
reports 5-44
security levels 3-14
server 1-8
SQL database 1-8
system requirements 3-2
test deployment. See test deployment
Trend Micro Infrastructure 1-9
understanding remote installation 3-27
updating 5-25
verifying agent installation 3-49
verifying installation 3-48
Web server 1-8
Web-based management console 1-9
where to install 2-14
Control Manager 2.5x agent migration flow 4-12
Control Manager agent for NetScreen Firewall 3-46
Certificate Name 3-47
determine Certificate Name 3-47
installing the agent 3-47
Control Manager agents 3-25
convention
document 1-ii

creating
deployment plans 5-34
user groups 5-14
users 5-11
Creating a damage cleanup task 6-10

D

Damage cleanup engine (DCE) 6-3
Damage Cleanup Services 1-4
activating 3-11–3-12
Damage cleanup template (DCT) 6-3
database recommendations 2-7
deleting
user accounts 5-14
user groups 5-15
Deleting a damage cleanup task 6-14
deploy failed, Vulnerability Assessment 7-8
deploying 5-33
deployment plans 5-33
sample 5-34
deployment architecture and strategy 2-10
multiple-site deployment 2-12
multi-site deployment 2-12
single-server deployment 2-10
single-site deployment 2-10
deployment plan
creating 5-34
default plans 5-34
Directory Manager 5-19
grouping managed products 5-19
disable notifications 5-40
disabling
user accounts 5-13
downloading
enable HTTPS 5-30
enable UNC 5-31
set proxy server settings 5-30
downloading and deploying components 5-25
downloading components
manually 5-26
scheduled download 5-27
Downloading the damage cleanup engine and template manually 6-6
Downloading updates for Damage Cleanup Services 6-6

E

E2EPublic.dat *See encryption key*
editing
user accounts 5-12
user groups 5-15
Editing a damage cleanup task 6-12
email 5-40
enable notifications 5-40
Enabling Vulnerability Assessment Services with Damage Cleanup tasks 6-14
encryption key
agent, installation 3-40
obtaining 3-29
obtaining the 3-29
purpose 3-29
enforcement, Vulnerability Assessment, defined 7-9
enterprise
multiple site 2-3
single-site 2-3
Enterprise edition
features 1-7
Event Center 5-39
Alert 5-39
Damage Cleanup Services 5-40
new notifications 1-6
Outbreak Prevention Services 5-39
Unusual 5-40
Update 5-40

F

Features and Benefits 6-3
flow
migrating Control Manager 2.5x agent 4-12
migrating Trend VCS 1.8x agent 4-11

G

generating on-demand scheduled reports 5-47
global reports 5-44
global settings, Vulnerability Assessment 7-22
grouping managed products or child servers 2-12

H

how many
Control Manager servers 2-3
HTTPS 1-5

enable HTTPS download 5-30

I

IIS Restoration Tool 8-5
using SetupPatch.exe 8-6
initializing CasTool.exe. See calling CasTool.exe
installation
agent
Control Manager 3-33
InterScan Messaging Security Suite 5.1 3-45
Trend VCS agent 3-41
installing
Control Manager 3-1, 3-7
Control Manager agents 3-25
steps 3-7
verifying Control Manager server 3-48

L

local reports 5-44
location
Common CGI files 9-11
Microsoft Data Engine files 9-12
Trend Micro Management Infrastructure files 9-10

M

managed products 5-16
configuring 5-16
default folder 5-18
tabs 5-18
using the Product Directory 5-16
management console
access HTTPS 5-6
Managing Tasks 6-10
manual
remove
Common CGI 9-10
MSDE 9-11
Trend Management Infrastructure 9-9
Manual Damage Cleanup tool
using the 6-15
manually
remove Control Manager 9-6
manually uninstalling 9-6
MIBs browser 5-40
Microsoft
Data Engine
location, files 9-12
migrating 4-8
Control Manager 2.5x agent migration flow 4-12
Control Manager SQL 2000 4-14
database 4-14
different servers/agents 4-11
generate a migration list 4-13
phased upgrade 4-9
rapid upgrade 4-8
scenarios 4-9
single-server migration 4-10
steps 4-12
strategy 4-8
Trend VCS 1.8x agent migration flow 4-11
migration list 4-13
minimum system requirements 3-2
monitoring
security level 5-38
system information 5-37
monitoring the Control Manager environment 5-37
MSDE 2000 1-5

N

NetScreen Firewall 3-46
network traffic
plan 2-3
source
log traffic 2-4
logs 2-3
Product registration traffic 2-5
Trend Micro Management Infrastructure policies 2-4
sources 2-3
traffic frequency 2-6
new report templates 1-6
notifications 5-40
configure recipients 5-42
configuring 5-41
enabling or disabling 5-40
special virus alert settings 5-43
test notification delivery 5-42
virus outbreak alert settings 5-43

O

obtaining

agent packages 3-29
encryption key 3-29
ODBC
drivers 2-7
settings, Control Manager 9-11
off-hour period 2-5
OfficeScan
Trend VCS agent for 3-42
on-demand scheduled reports 5-47
Online Registration system 1-5
Outbreak Prevention Services 1-4
activating 3-11–3-12

P

pager 5-40
parent and child server feature comparison 5-20
parent server 5-19
performance, penalty 2-3
phased upgrade 4-9
plan
administration 2-8
data storage 2-7
network traffic 2-3
server distribution 2-2
port
checklist A-3
preface 1-i
preparing
Control Manager agent installation 3-25
Product Directory tabs 5-18
profiles. See report profiles
proxy server
communicating with Trend VCS agents 3-21
connecting to the Internet 3-20
proxy settings 5-30
public encryption key 3-29

Q

queries, creating, Vulnerability Assessment 7-21
querying commands 5-39

R

rapid upgrade 4-8
recommended system requirements 3-3
register online 3-11
registering
Control Manager 3-11, 3-50
registering a child server 5-22
Registration Key 1-5, 3-12, 3-52
registry key
Common CGI 9-11
Microsoft Data Engine 9-12
Trend Micro Management Infrastructure 9-10
Remote Agent Setup tool 3-33
RemoteInstall.exe 3-27, 3-33
RemoteInstall.xml 3-31
remove
manual
Control Manager 9-6
Microsoft Data Engine 9-11
Trend Management Infrastructure 9-9
removing
Control Manager manually 9-6
Control Manager server 9-2
Control Manager Windows-based agent 9-2
renew product maintenance 3-52
Renewing product maintenance for a full version of Damage Cleanup Services 6-5
reports 5-44
global 5-44
local 5-44
on-demand scheduled 5-47
report profiles 5-44
ActiveX 5-44
Contents 5-45
creating 5-44
Frequency 5-46
PDF 5-44
Recipient 5-46
RPT 5-44
RTF 5-44
Targets 5-45
viewing generated reports 5-47
reports, generating, Vulnerability Assessment 7-21
rolling back
to Control Manager 2.5 server 4-7
to Trend VCS 1.8x server 4-7
root account 5-9
root-level share 3-43
Running a damage cleanup task 6-12
running SetupPatch.exe. See using SetupPatch.exe

S

scheduled component download 5-27
scheduled reports 5-47
security levels 3-14
security risks, Vulnerability Assessment 7-8
server
  address, checklist A-1
server distribution plan 2-2
setting
  access rights 5-10
setting "Log on as batch job" policy 5-32
setting global enforcement, Vulnerability Assessment 7-22
setting global exceptions, Vulnerability Assessment 7-22
SetupPatch.exe. See IIS Restoration Tool
sizing recommendations 3-4
Small Network Management Protocol. See SNMP
SNMP 5-40
SQL
  Service Manager 9-12
Standard edition
  features 1-7
support operating systems 2-2
  Control Manager agents 2-2
  Control Manager server 2-2
supported operating systems 2-2
system requirements 3-2
  minimum 3-2
  recommendations 3-4
  recommended 3-3

T

tabs
  cascading structure tree 5-21
  Product Directory 5-18
tasks, creating, Vulnerability Assessment 7-12
tasks, deleting, Vulnerability Assessment 7-19
tasks, editing, Vulnerability Assessment 7-16
tasks, running, Vulnerability Assessment 7-15
tasks, viewing, Vulnerability Assessment 7-19
tasks, Vulnerability Assessment, overview 7-7
test deployment 2-16
  tasks 2-16
TMI 2-5
TMI *See Trend Micro Management Infrastructure*
tool
  AgentMigrateTool.exe 8-2
  CasTool.exe 8-2
  CMWebCfg.bat 8-6
  SetupPatch.exe 8-5
traffic plan
  network 2-3
  network sources 2-3
traffic, network 2-3
Trend Micro Management Infrastructure 2-6
  command prompt, stopping service from 9-9
  location, files 9-10
  registry key 9-10
  remove 9-9
Trend VCS
  agent
    installation 3-41
Trend VCS 1.8x agent migration flow 4-11
Trend VCS agents 3-25
Trigger Application 5-40

U

UNC 5-31
understanding
  Control Manager remote installation 3-27
unregistering a child server 5-23
Update Manager 1-5, 5-25
updating components 5-25, 5-35
upgrading 4-2
  backing up Control Manager 2.5 information 4-4
  considerations 4-2
  Control Manager 2.5 servers 4-3
  Trend VCS 1.8x servers 4-2
user accounts
  adding 5-11
  deleting 5-14
  disabling 5-13
  editing 5-12
user groups
  adding 5-14
  deleting 5-15
  editing 5-15
User Manager 5-9
users

adding accounts 5-11
adding groups 5-14
deleting accounts 5-14
deleting groups 5-15
disabling accounts 5-13
editing accounts 5-12
editing groups 5-15
Using the Account Management Tool 6-7
Using the damage cleanup history (task logs) 6-16
Using Trend Micro Damage Cleanup Services (DCS) 6-1

V

verifying
agent installation 3-49
Control Manager server installation 3-48
version
agent package 3-32
Viewing all existing tasks 6-14
viewing commands 5-39
viewing generated reports 5-47
Vulnerability Assessment
activating 3-11–3-12
Vulnerability Assessment, activating 7-4
Vulnerability Assessment, benefits 7-3
Vulnerability Assessment, configuring 7-6
Vulnerability Assessment, downloading updates 7-5
Vulnerability Assessment, introduction 7-1
Vulnerability Assessment, supported platforms 7-2
Vulnerability Assessment, uses 7-2
vulnerability, defined 7-7

W

who should read this document
audience 1-ii
Windows event log 5-40
work-hour policy 2-5
World Virus Tracking 3-12–3-13