TREND MICRO™

TREND MICRO™ Control Manager 6.0

Centralized Security Management for the Enterprise

Installation Guide

Document Part No.: CMEM65332/120203

Release Date: February 2013

Protected by U.S. Patent No. 5,623,600; 5,889,943; 5,951,698; 6,119,165

The user documentation for Trend Micro Control Manager introduces the main features of the software and installation instructions for your production environment. Read through it before installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the online Knowledge Base at Trend Micro's website.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Please evaluate this documentation on the following site:

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

Table of Contents

Preface

Chapter 1: Introducing Trend Micro Control Manager

Chapter 2: Planning and Implementing the Control Manager Deployment

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

Chapter 4: Upgrading Servers or Migrating Agents to Control Manager

Chapter 5: Removing Trend Micro Control Manager

Chapter 6: Getting Support

Appendix A: Control Manager System Checklists

Index

Preface

Preface

This Installation Guide introduces Trend Micro™ Control Manager™ 6.0 and guides you through planning the installation and installing Control Manager.

This preface contains the following topics:

What's New in This Version

Trend Micro Control Manager 6.0 represents a significant advance in management capability by introducing policy management to deploy product settings directly to endpoints from a single console.

Control Manager 6.0 Features and Enhancements

The following new features and enhancements are available in version 6.0.

Feature	Description
Policy management	• Deploy product settings to managed products using policies • Flexible policy types • Role-based administration • Easy policy template updates from the web console
Policy status dashboard widget	• Up-to-date deployment status of product settings • Monitor the numbers of deployed and pending targets • Check the detailed status of the pending targets
Policy template updates	When new or updated templates become available, administrators can easily perform the update from the web console.

Feature	Description
Data Loss Prevention (DLP) integration	DLP is a feature of the Data Protection module that monitors the transmission of digital assets. The DLP feature can minimize the risk of information loss and improve visibility of data usage patterns and risky business processes. Control Manager has integrated the following DLP features: • Manageable DLP templates and data identifiers • Deploy DLP settings to managed products using policy management, DLP templates, and data identifiers • Collect DLP logs for reports and event notifications • 22 pre-defined DLP report templates • Five DLP event notifications • Four dashboard widgets • Product support: OfficeScan, IMSVA, and ScanMail for Microsoft Exchange
Favorites	Administrators can add menu shortcuts to the Favorites menu for quick access.

Control Manager Documentation

This documentation assumes a basic knowledge of security systems. There are references to previous versions of Control Manager to help system administrators and personnel who are familiar with earlier versions of the product. If you have not used earlier versions of Control Manager, the references may help reinforce your understanding of the Control Manager concepts.

TABLE 1. Control Manager Documentation

DOCUMENT	DESCRIPTION
Online Help	Web-based documentation that is accessible from the Control Manager web console. The online help contains explanations of Control Manager components and features, as well as procedures needed to configure Control Manager.
Trend Micro Online Help Center (http://docs.trendmicro.com)	The Trend Micro Online Help Center provides the latest product documentation.
Readme file	The Readme file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.
Installation Guide	PDF documentation is accessible from the Trend Micro Enterprise DVD or downloadable from the Trend Micro website. The Installation Guide contains detailed instructions of how to install Control Manager and configure basic settings to get you "up and running".
Administrator's Guide	PDF documentation that is accessible from the Trend Micro Solutions DVD for Control Manager or downloadable from the Trend Micro website. The Administrator's Guide contains detailed instructions of how to configure and manage Control Manager and managed products, and explanations on Control Manager concepts and features.

Document	Description
Tutorial	PDF documentation that is accessible from the Trend Micro Solutions DVD for Control Manager or downloadable from the Trend Micro website. The Tutorial contains hands-on instructions of how to deploy, install, configure, and manage Control Manager and managed products registered to Control Manager.

Document Conventions

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

Convention/Term	Description
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard.
Bold	Menus and menu commands, command buttons, tabs, options, and tasks.
Italics	References to other documents.
`Monospace`	Sample command lines, program code, Web URLs, file names, and program output.
 **Note**	Configuration notes.
 **Tip**	Recommendations or suggestions.

CONVENTION/TERM	DESCRIPTION
 **WARNING!**	Critical actions and configuration options.
Navigation > **Path**	The navigation path to reach a particular screen. For example, **Scans** > **Manual Scans**, means, click **Scans**, and then click **Manual Scans** on the interface.

Chapter 1

Introducing Trend Micro™ Control Manager™

Trend Micro Control Manager is a central management console that manages Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. Administrators can use the policy management feature to configure and deploy product settings to managed products and endpoints. The Control Manager web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network.

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

This chapter contains the following topics:

- *Trend Micro™ Smart Protection Network™ on page 1-11*

Control Manager Standard and Advanced

Control Manager is available in two versions: Standard and Advanced. Control Manager Advanced includes features that Control Manager Standard does not. For example, Control Manager Advanced supports a cascading management structure. This means the Control Manager network can be managed by a parent Control Manager Advanced server with several child Control Manager Advanced servers reporting to the parent Control Manager Advanced server. The parent server acts as a hub for the entire network.

Note

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

- Control Manager 6.0 Advanced
- Control Manager 5.5 Advanced
- Control Manager 5.0 Advanced

Control Manager 5.0/5.5/6.0 Standard servers cannot be child servers.

For a complete list of all features Standard and Advanced Control Manager servers support see *Control Manager Product Version Comparison on page A-9*

Introducing Control Manager Features

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

TABLE 1-1. Control Manager Features

FEATURE	DESCRIPTION
Policy management	System administrators can use policies to configure and deploy product settings to managed products and endpoints from a single management console.

Feature	Description
Centralized configuration	Using the Product Directory and cascading management structure, these functions allow you to coordinate virus-response and content security efforts from a single management console. These features help ensure consistent enforcement of your organization's virus/malware and content security policies.
Proactive outbreak prevention	With Outbreak Prevention Services (OPS), take proactive steps to secure your network against an emerging virus/malware outbreak.
Secure communication infrastructure	Control Manager uses a communications infrastructure built on the Secure Socket Layer (SSL) protocol. Depending on the security settings used, Control Manager can encrypt messages or encrypt them with authentication.
Secure configuration and component download	These features allow you to configure secure web console access and component download.
Task delegation	System administrators can give personalized accounts with customized privileges to Control Manager web console users. User accounts define what the user can see and do on a Control Manager network. Track account usage through user logs.
Command Tracking	This feature allows you to monitor all commands executed using the Control Manager web console. Command Tracking is useful for determining whether Control Manager has successfully performed long-duration commands, like virus pattern update and deployment.
On-demand product control	Control managed products in real time. Control Manager immediately sends configuration modifications made on the web console to the managed products. System administrators can run manual scans from the web console. This command system is indispensable during a virus/malware outbreak.

FEATURE	DESCRIPTION
Centralized update control	Update virus patterns, antispam rules, scan engines, and other antivirus or content security components to help ensure that all managed products are up to date.
Centralized reporting	Get an overview of the antivirus and content security product performance using comprehensive logs and reports. Control Manager collects logs from all its managed products; you no longer need to check the logs of each individual product.

Understanding Trend Micro Management Communication Protocol

Trend Micro Management Communication Protocol (MCP) agent is the next generation agent for Trend Micro managed products. MCP replaces Trend Micro Management Infrastructure (TMI) as the way Control Manager communicates with managed products. MCP has several features:

- Reduced network loading and package size
- NAT and firewall traversal support
- HTTPS support
- One-way and two-way communication support
- Single sign-on (SSO) support

Reduced Network Loading and Package Size

TMI uses an application protocol based on XML. Even though XML provides a degree of extensibility and flexibility in the protocol design, the drawbacks of applying XML as the data format standard for the communication protocol consist of the following:

- XML parsing requires more system resources compared to other data formats such as CGI name-value pair and binary structure (the program leaves a large footprint on your server or device).
- The agent footprint required to transfer information is much larger in XML compared with other data formats.
- Data processing performance is slower due to the larger data footprint.
- Packet transmissions take longer and the transmission rate is less than other data formats.

MCP's data format is designed to resolve these issues. MCP's data format is a BLOB (binary) stream with each item composed of name ID, type, length, and value. This BLOB format has the following advantages:

- **Smaller data transfer size compared to XML:** Each data type requires only a limited number of bytes to store the information. These data types are integer, unsigned integer, Boolean, and floating point.
- **Faster parsing speed:** With a fixed binary format, each data item can be easily parsed one by one. Compared to XML, the performance is several times faster.
- **Improved design flexibility:** Design flexibility has also been considered since each item is composed of name ID, type, length, and value. There will be no strict item order and compliment items can be present in the communication protocol only if needed.

In addition to applying binary stream format for data transmission, more than one type of data can be packed in a connection, with or without compression. With this type of data transfer strategy, network bandwidth can be preserved and improved scalability is also created.

NAT and Firewall Traversal Support

With limited addressable IP addresses on the IPv4 network, NAT (Network Address Translation) devices have become widely used to allow more end-point computers to connect to the Internet. NAT devices achieve this by forming a private virtual network to the computers attached to the NAT device. Each computer that connects to the NAT device will have one dedicated private virtual IP address. The NAT device will

translate this private IP address into a real world IP address before sending a request to the Internet. This introduces some problems since each connecting computer uses a virtual IP and many network applications are not aware of this behavior. This usually results in unexpected program malfunctions and network connectivity issues.

For products that work with Control Manager 2.5/3.0 agents, one pre-condition is assumed. The server relies on the fact that the agent can be reached by initiating a connection from server to the agent. This is a so-called two-way communication product, since both sides can initiate network connection with each other. This assumption breaks when the agent sits behinds a NAT device (or the Control Manager server sits behind a NAT device) since the connection can only route to the NAT device, not the product behind the NAT device (or the Control Manager server sitting behind a NAT device). One common work-around is that a specific mapping relationship is established on the NAT device to direct it to automatically route the in-bound request to the respective agent. However, this solution needs user involvement and it does not work well when large-scale product deployment is needed.

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

HTTPS Support

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

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

Using MCP, Control Manager has three security levels:

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

One-Way Communication

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

Two-Way Communication

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

Single Sign-on (SSO) Support

Through MCP, Control Manager supports single sign-on (SSO) functionality for Trend Micro products. This feature allows users to sign in to Control Manager and access the resources of other Trend Micro products without having to sign in to those products as well.

Control Manager Architecture

Trend Micro Control Manager provides a means to control Trend Micro products and services from a central location. This application simplifies the administration of a corporate virus/malware and content security policy. The following table provides a list of components Control Manager uses.

TABLE 1-2. Control Manager Components

COMPONENT	DESCRIPTION
Control Manager server	Acts as a repository for all data collected from the agents. It can be a Standard or Advanced Edition server. A Control Manager server includes the following features: • An SQL database that stores managed product configurations and logs Control Manager uses the Microsoft SQL Server database (`db_ControlManager.mdf`) to store data included in logs, Communicator schedule, managed product and child server information, user account, network environment, and notification settings. • A web server that hosts the Control Manager web console • A mail server that delivers event notifications through email messages Control Manager can send notifications to individuals or groups of recipients about events that occur on the Control Manager network. Configure Event Center to send notifications through email messages, Windows event log, MSN Messenger, SNMP, Syslog, pager, or any in-house/industry standard application used by your organization to send notification. • A report server, present only in the Advanced Edition, that generates antivirus and content security product reports A Control Manager report is an online collection of figures about security threat and content security events that occur on the Control Manager network.

COMPONENT	DESCRIPTION
Trend Micro Management Communication Protocol	MCP handles the Control Manager server interaction with managed products that support the next generation agent. MCP is the new backbone for the Control Manager system. MCP agents install with managed products and use one/two way communication to communicate with Control Manager. MCP agents poll Control Manager for instructions and updates.
Trend Micro Management Infrastructure	Handles the Control Manager server interaction with older managed products. The Communicator, or the Message Routing Framework, is the communication backbone of the older Control Manager system. It is a component of the Trend Micro Management Infrastructure (TMI). Communicators handle all communication between the Control Manager server and older managed products. They interact with Control Manager 2.x agents to communicate with older managed products.
Control Manager 2.x Agents	Receives commands from the Control Manager server and sends status information and logs to the Control Manager server The Control Manager agent is an application installed on a managed product server that allows Control Manager to manage the product. Agents interact with the managed product and Communicator. An agent serves as the bridge between managed product and communicator. Therefore, install agents on the same computer as managed products.
Web-based management console	Allows an administrator to manage Control Manager from virtually any computer with an Internet connection and Windows™ Internet Explorer™ The Control Manager management console is a web-based console published on the Internet through the Microsoft Internet Information Server (IIS) and hosted by the Control Manager server. It lets you administer the Control Manager network from any computer using a compatible web browser.

COMPONENT	DESCRIPTION
Widget Framework	Allows an administrator to create a customized dashboard to monitor the Control Manager network.

Trend Micro™ Smart Protection Network™

The Trend Micro™ Smart Protection Network™ is a next-generation cloud-client content security infrastructure designed to protect customers from security risks and web threats. It powers both on-premise and Trend Micro hosted solutions to protect users whether they are on the network, at home, or on the go. Smart Protection Network uses lighter-weight clients to access its unique in-the-cloud correlation of email, web, and file reputation technologies, as well as threat databases. Customers' protection is automatically updated and strengthened as more products, services and users access the network, creating a real-time neighborhood watch protection service for its users.

Email Reputation

Trend Micro's email reputation technology validates IP addresses by checking them against a reputation database of known spam sources and by using a dynamic service that can assess email sender reputation in real time. Reputation ratings are refined through continuous analysis of the IP addresses' "behavior," scope of activity and prior history. Email reputation blocks malicious email messages in the cloud based on the sender's IP address, preventing threats from reaching the network or the user's PC.

File Reputation Services

File Reputation Services checks the reputation of each file against an extensive in-the-cloud database. Since the malware information is stored in the cloud, it is available instantly to all users. High performance content delivery networks and local caching servers ensure minimum latency during the checking process. The cloud-client architecture offers more immediate protection and eliminates the burden of pattern deployment besides significantly reducing the overall client footprint.

Web Reputation Services

With one of the largest domain-reputation databases in the world, Trend Micro web reputation technology tracks the credibility of web domains by assigning a reputation score based on factors such as a website's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis. Web reputation then continues to scan sites and block users from accessing infected ones. Web reputation features help ensure that the pages that users access are safe and free from web threats, such as malware, spyware, and phishing scams that are designed to trick users into providing personal information. To increase accuracy and reduce false positives, Trend Micro web reputation technology assigns reputation scores to specific pages or links within sites instead of classifying or blocking entire sites, since often, only portions of legitimate sites are hacked and reputations can change dynamically over time.

Smart Feedback

Trend Micro Smart Feedback provides continuous communication between Trend Micro products and its 24/7 threat research centers and technologies. Each new threat identified through every single customer's routine reputation check automatically updates all Trend Micro threat databases, blocking any subsequent customer encounters of a given threat.

By continuously processing the threat intelligence gathered through its extensive global network of customers and partners, Trend Micro delivers automatic, real-time protection against the latest threats and provides "better together" security, much like an automated neighborhood watch that involves the community in the protection of others. Because the gathered threat information is based on the reputation of the communication source, not on the content of the specific communication, the privacy of a customer's personal or business information is always protected.

Chapter 2

Planning and Implementing the Control Manager Deployment

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

This chapter contains the following topics:

- *Web Server Plan on page 2-24*

Identifying Deployment Architecture and Strategy

Deployment is the process of strategically distributing Control Manager servers in 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 network requires careful planning and assessment.

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

- **Single-site deployment**: Refers to distributing and managing child servers, managed products, and endpoints 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 network connections between sites, single-site deployment still applies to your environment.
- **Multiple-site deployment**: Refers to distributing and managing Control Manager servers in an organization that has main offices in different geographical locations.

Tip

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

Understanding Single-Site Deployment

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

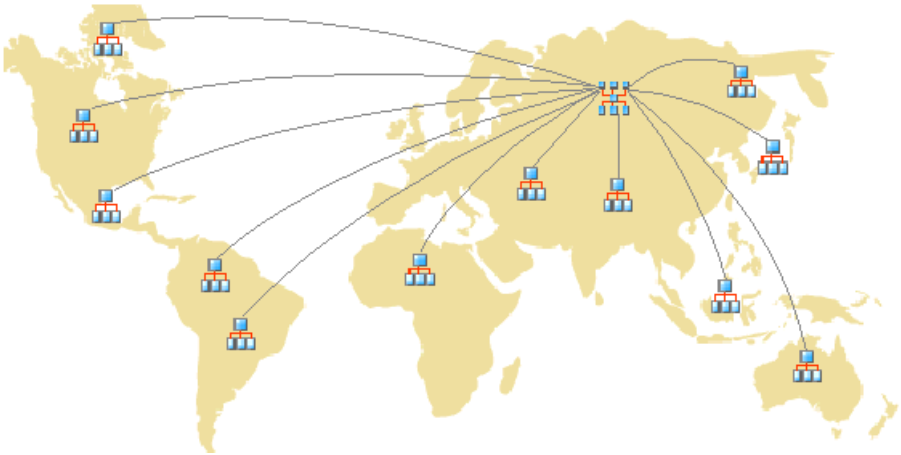


FIGURE 2-1. A single-server deployment using Control Manager Advanced parent server and mixed child servers

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

1. Determine the number of managed products, endpoints, and cascading structures
2. Plan for the optimal ratios of the following:
   - Server-managed products to cascading structures
   - Server-endpoints to cascading structures
3. Designate the Control Manager Standard server or Control Manager Advanced server

Note

Control Manager 6.0 Advanced supports the following as child Control Manager servers:

- Control Manager 6.0 Advanced
- Control Manager 5.5 Advanced
- Control Manager 5.0 Advanced

Control Manager 5.0/5.5/6.0 Standard servers cannot be child servers.

Determining the Number of Managed Products, Endpoints, and Cascading Structures

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

Planning for the Optimal Ratios of Server-Managed Products/Server-Endpoints to Cascading Structures

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

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

Designating Control Manager Servers

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

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

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

- The 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.

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

Understanding Multiple-Site Deployment

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

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

Deploy Control Manager servers in a number of different locations, including the demilitarized zone (DMZ) or the private network. Position the Control Manager server in the DMZ on the public network to administer managed products, endpoints, or child

servers and access the Control Manager web console using Internet Explorer over the Internet.

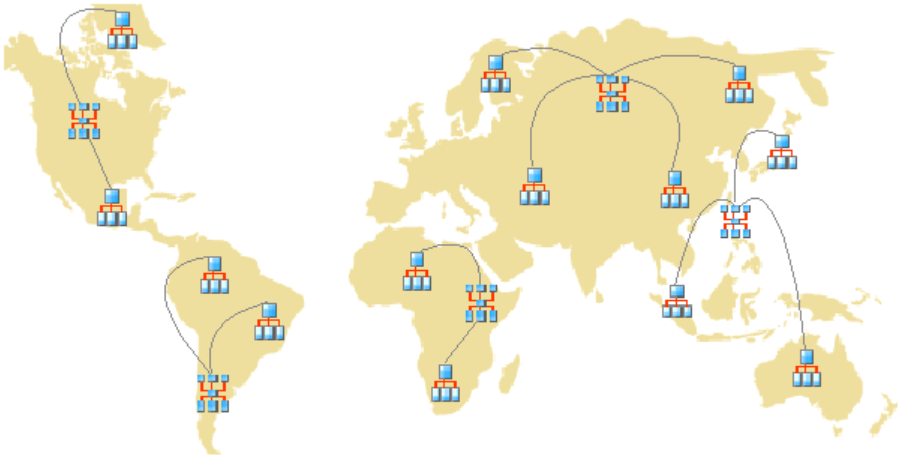


FIGURE 2-2. A multi-site deployment using multiple Control Manager Advanced parent servers and mixed child servers

Consider the following for multi-site deployment:

- Group managed products, endpoints, or child servers
- Determine the number of sites
- Determine the number of managed products, endpoints, and child servers
- Plan for network traffic
- Plan for the optimal ratios of the following:
  - Server-managed products to cascading structures
  - Server-endpoints to cascading structures
- Decide where to install the Control Manager server

Grouping Managed Products, Endpoints, or Child Servers

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

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

CONSIDERATION	DESCRIPTION
Company network and security policies	If different access and sharing rights apply to the company network, group managed products, endpoints, and child servers according to company network and security policies.
Organization and function	Group managed products, endpoints, 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, endpoints, and child servers affects the communication between the Control Manager server and its managed products, endpoints, or child servers.
Administrative responsibility	Group managed products, endpoints, and child servers according to system or security personnel assigned to them. This allows group configuration.

Determining the Number of Sites

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

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

Determining the Number of Managed Products, Endpoints, and Child Servers

You also need to know the total number of managed products, endpoints, and child servers Control Manager server will manage. Trend Micro recommends gathering managed product, endpoint, 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 to install.

Planning for the Optimal Ratio of Server-Managed Products/ Server-Endpoints to Cascading Structure

When deploying Control Manager across the WAN, the Control Manager server in the main office administers managed products, endpoints, and child servers in the remote office. If you will have managed products, endpoints, or child servers in the remote office reporting to the server in the main office over the WAN, you need to consider the diversity of the network bandwidth in your WAN environment. Having different network bandwidth in your WAN environment can be beneficial to Control Manager. If you have managed products, endpoints, 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, endpoints, or child servers on the LAN.

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

Designating Control Manager Servers

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

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

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

- The CPU load
- Other functions the server performs

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

Deciding Where to Install the Control Manager Server

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

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

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

  Tip

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

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

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

Planning for Network Traffic

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

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

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

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

  For brand-new Trend Micro products that have not had a product profile, Trend Micro delivers updates to enable Control Manager to identify these products.
- Child server registration to Control Manager parent server
- Downloading and deploying updates
- Policy deployment

Control Manager Setup Flow

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

1. Planning the Control Manager system installation (server distribution, network traffic, data storage, and web server considerations).
2. Installing the Control Manager server.

Note

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

Testing Control Manager at One Location

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

Tip

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

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

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

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

A Control Manager test deployment consists of the following tasks:

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

Preparing for the Test Deployment

Complete the following activities during the preparation stage.

Procedure

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

Selecting a Test Site

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

Creating a Rollback Plan

Create a disaster recovery or rollback plan (for example, how to roll back to Control Manager 5.0/5.5) in case there are some difficulties with the installation or upgrade. This process should take into account local corporate policies, as well as IT resources.

Beginning the Test Deployment

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

Evaluating the Test Deployment

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

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

Server Distribution Plan

Consider the following when planning for server distribution:

- Administration models
- Control Manager server distribution
- Single-server topology
- Multiple-server topology

Understanding Administration Models

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

Follow one of these administration models:

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

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

- **Decentralized management**: This is appropriate for large networks where system administrators have clearly defined and established areas of responsibility. For

example, the mail server administrator may also be responsible for email protection; regional offices may be independently responsible for their local areas.

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

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

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

Understanding Control Manager Server Distribution

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

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

Single-Server Topology

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

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

Multiple-Server Topology

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

For information on the traffic that a Control Manager network generates, see *Understanding Control Manager Network Traffic on page 2-16*.

Network Traffic Plan

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

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

Understanding Control Manager Network Traffic

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

Sources of Network Traffic

The following Control Manager sources generate network traffic:

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

Traffic Frequency

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

- Logs generated by managed products
- MCP polling and commands
- Trend Micro Management Infrastructure policies

Logs

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

Managed Product Agent Heartbeat

By default, managed product agents send heartbeat messages every 60 minutes. Administrators can adjust this value from 5 to 480 minutes (8 hours). When choosing a heartbeat setting, choose a balance between the need to display the latest Communicator status information and the need to manage system resources.

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

- **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 the interval.

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

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

Note

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

Network Protocols

Control Manager uses the UDP and TCP protocols for communication.

Source of Network Traffic

Log Traffic

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

TABLE 2-2. Control Manager Log Traffic

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

LOG	CONTAINS INFORMATION ABOUT
Performance Metric	Used for previous product versions.
URL Usage	Violations reported by web security products.
Security Violation	Violations reported by Network VirusWall products.
Security Compliance	Endpoint compliances reported by Network VirusWall products.
Security Statistic	The difference between security compliances and security violations calculated and reported by Network VirusWall products.
Endpoint	Violations reported by Web security products.

Trend Micro Management Communication Protocol Policies

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

- **MCP Heartbeat**: The MCP heartbeats to Control Manager ensure that Control Manager displays the latest information and that the connection between the managed product and the Control Manager server is functional.
- **MCP Command Polling**: When an MCP agent initiates a command poll to Control Manager, Control Manager notifies the agent to send managed product logs or issues a command to the managed product. Control Manager also interprets a command poll as a passive heartbeat verifying the connection between Control Manager and the managed product.

Trend Micro Management Infrastructure Policies

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

- **Communicator Heartbeat**: The Communicator, the message routing framework of TMI, polls the Control Manager server at regular intervals. This ensures that the Control Manager console displays the latest information, and that the connection between the managed product and the Control Manager server is functional.
- **Work-Hour Policy**: The work-hour policy defines when a Communicator sends information to the Control Manager server. Use the Communication Scheduler to define this policy; a user can set three periods of inactivity – also called "off-hour" periods. There are two types of information, however, that do not follow the Communicator Scheduler:
  - Emergency messages
  - Prohibited messages

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

Product Registration Traffic

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

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

- Category (for example, antivirus)
- Product name
- Product version

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

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

Policy Deployment

Control Manager generates network traffic when deploying policy settings to managed products and endpoints. The traffic originates from the following sources:

- Periodic policy enforcement

  Control Manager enforces the policy settings on managed products and endpoints every 60 minutes.

- Deployed information

  A policy contains the Globally Unique Identifier (GUID) information for each endpoint and the setting information. A policy containing 50,000 targets and a full set of settings can generate up to 1.8MB of network traffic.

Deploying Updates

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

1. Obtain the latest update components from Trend Micro.

   Control Manager can download components either directly from the Trend Micro update server, or from an alternative location.

2. Deploy these components to the managed products.

Control Manager deploys update components to managed products, including:

- Pattern files/Cleanup templates
- Engines (scan engines, damage cleanup engines)
- Antispam rules
- OfficeScan Plug-in Manager Plug-in Programs
- Product programs (depending on the product)

Tip

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

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

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

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

Data Storage Plan

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

Note

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

Database Recommendations

This section provides recommendations for administrators when installing Control Manager and its SQL server on the same computer.

Important

You must manually install .NET Framework 3.5 SP1 before installing Control Manager.

- Production environment
  - Use a computer with more than 4GB of memory

    Note

    The minimum memory requirement to install Control Manager is 2GB, and the recommended requirement is 4GB. For a computer with less than 4GB of memory, Trend Micro does not recommend installing Control Manager and its SQL server on the same computer.

  - Configure the maximum amount of memory used by the SQL server

    Leave at least 4GB of memory for Control Manager and system usage.

    For example, if a computer has 8GB of memory, set the maximum memory usage of the SQL server to 4GB. In this case, 4GB of memory is available for Control Manager and system usage.

    Note

    See http://msdn.microsoft.com/en-us/library/ms191144(v=sql.105).aspx for details on how to configure memory usage for the SQL server.

- Test environment

  Leave at least 2GB of memory for Control Manager and system usage.

Note

See http://msdn.microsoft.com/en-us/library/ms191144(v=sql.105).aspx for details on how to configure memory usage for the SQL server.

Tip

- For Control Manager managing more than 1,000 products (including OfficeScan clients and ServerProtect Normal servers), Trend Micro recommends using a dedicated SQL server.
- If Control Manager and the SQL server are installed on different computers, set the same time zone on both computers.
- Trend Micro highly recommends using Microsoft SQL Server Standard or Enterprise Edition. SQL Express is suitable for testing purposes but not for production environments.

ODBC Drivers

Control Manager uses an ODBC driver to communicate with the SQL server. For most instances, ODBC version 3.7 is sufficient.

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

Authentication

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

Web Server Plan

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 settings 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 website
- **Component**: This depends on the updated component. For example, when the virus pattern file is updated, the value added here is:

  `Pattern/vsapi.zip`

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

Chapter 3

Installing Trend Micro Control Manager for the First Time

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

This chapter contains the following topics:

System Requirements

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.

For a complete list of fresh installation requirements, visit the following link:

http://docs.trendmicro.com/en-us/enterprise/control-manager.aspx

Note

Control Manager 6.0 Advanced supports the following as child Control Manager servers:

- Control Manager 6.0 Advanced
- Control Manager 5.5 Advanced
- Control Manager 5.0 Advanced

Control Manager 5.0/5.5/6.0 Standard servers cannot be child servers.

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

Installing Prerequisite Components

The following table lists the components required before starting the installation program for Control Manager. Without these components the installation process cannot proceed.

TABLE 3-1. Prerequisite Components

PLATFORM	COMPONENTS
Windows 2003 Server	• .Net Framework 3.5 SP1 • Microsoft Message Queuing • Windows Installer 4.5
Windows 2008 Server/Windows 2012 Server	• IIS 6 Management Compatibility components • IIS Windows authentication module • IIS ASP.NET • .Net Framework 3.5 SP1 • Microsoft Message Queuing

About Installing a Control Manager Server

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

You need the following information for the installation:

- Relevant target server address and port information
- Control Manager Registration Key
- Security Level to use for Server-Agent communication

Note

Creation of 8.3 file names is required for the installation. Enable this function to successfully install Control Manager. For more information, go to http://esupport.trendmicro.com/solution/en-us/1056505.aspx.

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

Important

You must manually install .NET Framework 3.5 SP1 before installing Control Manager.

- Prepare the following information about the SQL database for Control Manager:
  - User name for the database
  - Password

Note

Control Manager uses both Windows authentication and SQL 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 the server, Control Manager installs SQL Server 2008 Express, which can only handle a limited number of connections

Control Manager Installation Flow

Installing Control Manager requires performing the following steps:

1. Install all required components
2. Specify the installation location
3. Register and activate the product and services
4. Specify Control Manager security and web server settings
5. Specify the backup settings
6. Configure notification settings
7. Configure database information
8. Set up the root account

Tip

Trend Micro recommends upgrading to version 6.0 instead of doing a fresh installation.

Installing All Required Components

Important

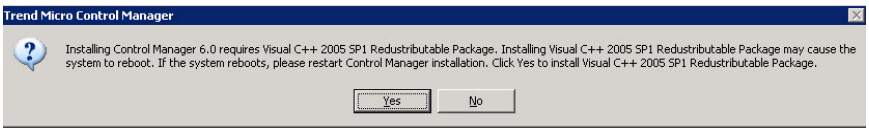
You must manually install .NET Framework 3.5 SP1 before installing Control Manager.

Procedure

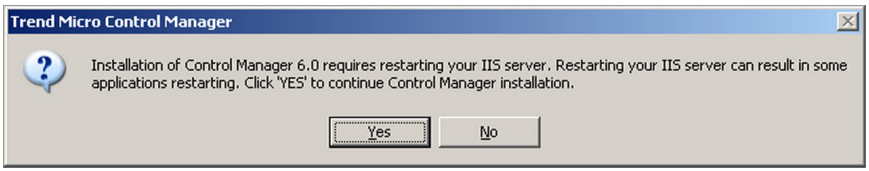
1. On the Windows taskbar, click **Start** > **Run**, and then locate the Control Manager installation program (`Setup.exe`). If installing from the Trend Micro Enterprise DVD, go to the Control Manager folder on the DVD. If you downloaded the software from the Trend Micro website, navigate to the relevant folder on your computer. The installation program checks your system for required components. If the installation program does not detect the following components on the server, dialog boxes appear prompting you to install the missing component:

   - **Visual C++ 2005 SP1 Redistributable Package**: This component is included in the Control Manager installation package
   - **PHP 5.3.5**: If the server uses an older PHP, remove it before starting the installation. Control Manager then installs PHP 5.3.5 during the installation.

2. Install all missing components. A confirmation dialog box appears.



3. Click **Yes** to continue the installation. Another confirmation dialog box appears.



4. Click **Yes** to continue the installation.

   The **Welcome** screen appears.

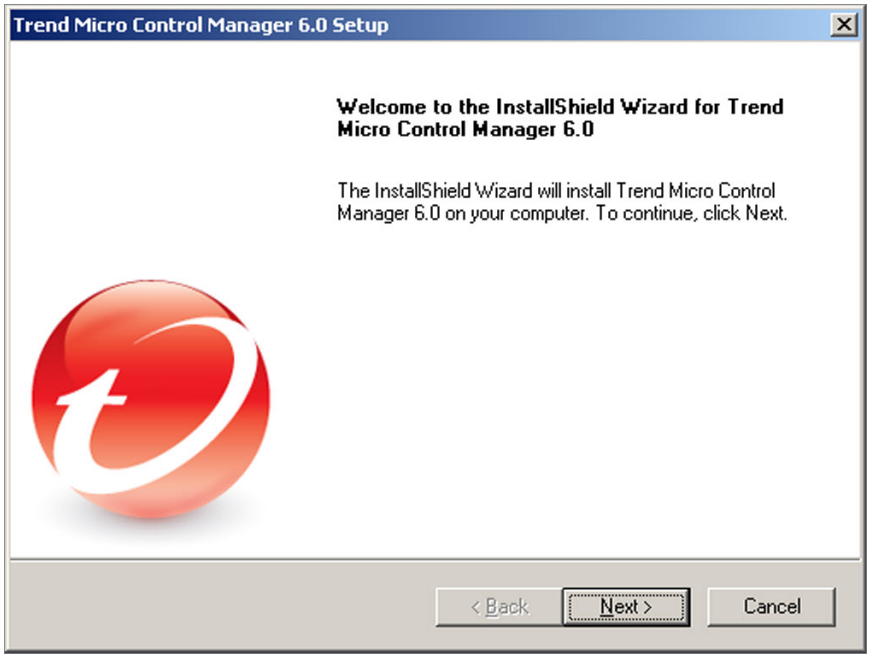


FIGURE 3-1. The Welcome screen

The installation program checks your system for existing components. Before proceeding with the installation, close all instances of the Microsoft Management Console. For more information about migration, see *Migration Scenarios for Control Manager 2.x Agents on page 4-12*.

5. Click **Next**.

The **Software License Agreement** screen appears.

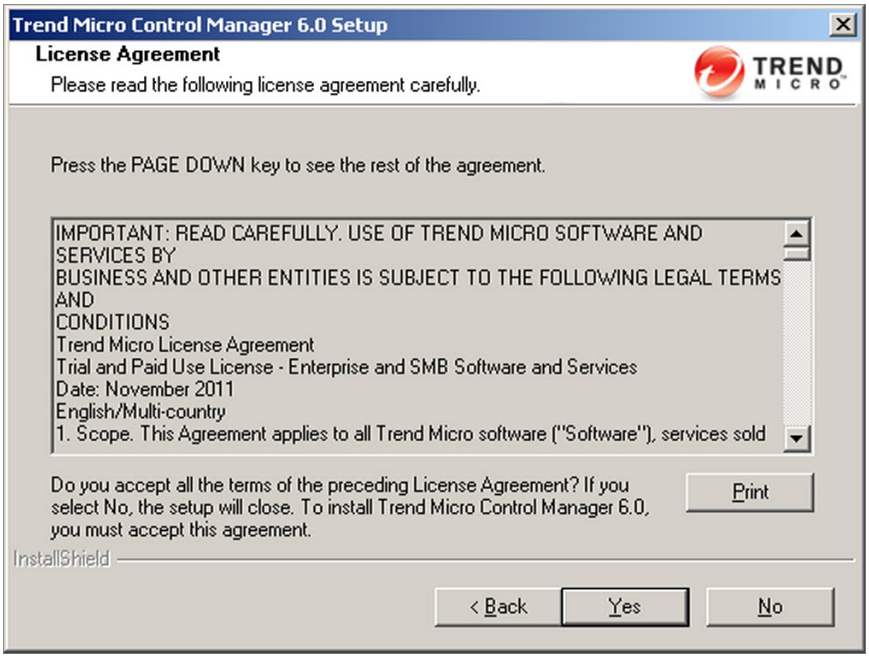


FIGURE 3-2. Agree with the License Agreement

6. If you do not agree with the terms of the license, click **No**; the installation stops. Otherwise, click **Yes**.

7. (For Windows 2003, 64-bit installation only) A confirmation dialog box appears. Click **Yes** to switch the Microsoft IIS to 32-bit mode. Click **No** to stop the installation.

8. A summary of detected components appears.

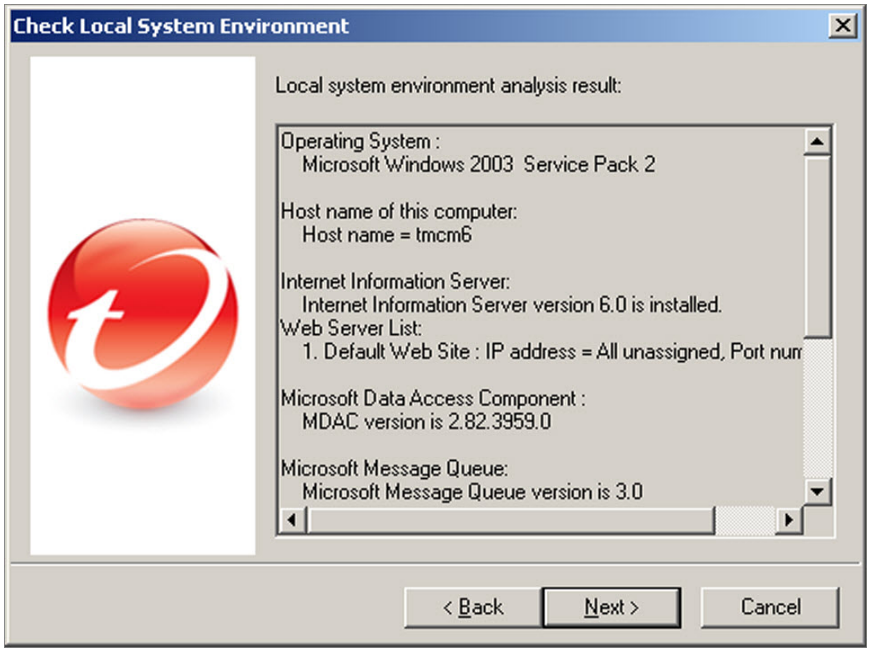


FIGURE 3-3. Displays local system environment information

Specifying the Installation Location

Note

Creation of 8.3 file names is required for the installation. Enable this function to successfully install Control Manager. For more information, go to http://esupport.trendmicro.com/solution/en-us/1056505.aspx.

Procedure

1. Click **Next**.

The **Select Destination Folder** screen appears.

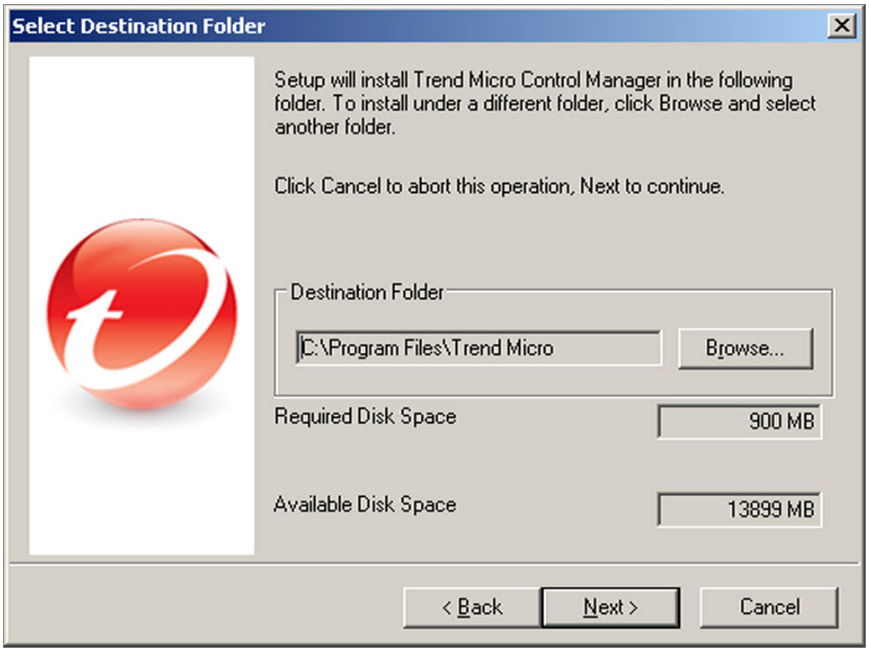


FIGURE 3-4. Select a destination folder

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

Note

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

Registering and Activating the Product and Services

Procedure

1. Click **Next**.

   The **Product Activation** screen appears.

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

2. Type the Activation Code for Control Manager and any other additional purchased services (you can also activate optional services from the Control Manager console). To use the full functionality of Control Manager and other services (Outbreak Prevention Services), you need to obtain Activation Codes and activate the software or services. Included with the software is a Registration Key that you use to register your software online on the Trend Micro Online Registration website and obtain an Activation Code.

3. Click **Next**.

   The **Trend Micro Smart Feedback** screen appears.

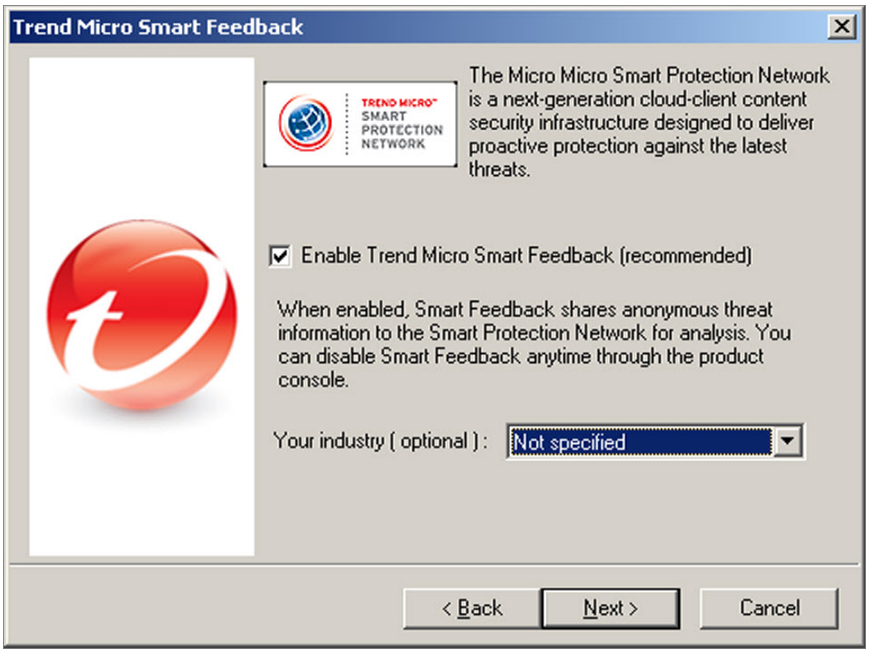


FIGURE 3-6. Smart Protection Network settings

4. Select **Enable Trend Micro Smart Feedback** to participate in the Smart Protection Network program. When you choose to participate, Control Manager sends anonymous threat information to the Trend Micro Smart Protection Network servers. This allows proactive protection of your network. You can stop participating any time through the Control Manager web console.

Specifying Control Manager Security and Web Server Settings

Procedure

1. Click **Next**.

   The **Select Security Level and Host Address** screen appears.

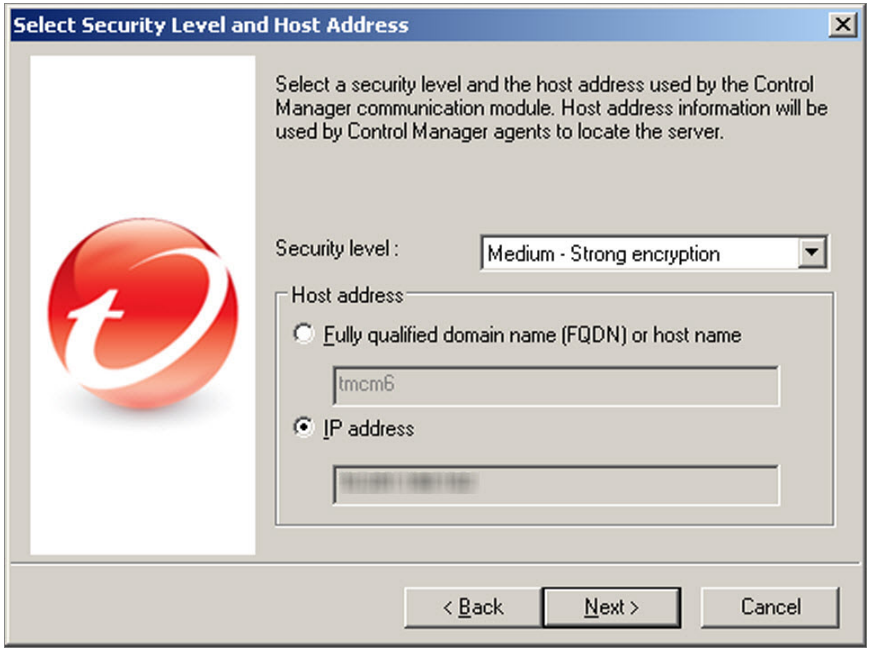


FIGURE 3-7. Select a security level

2. From the Security level list, select the security level for Control Manager communication with agents. The options are as follows:

   - **High**: All communication between Control Manager and managed products use 128-bit encryption with authentication. This ensures the most secure communication between Control Manager and managed products.

- **Medium**: If supported, all communication between Control Manager and managed products use 128-bit encryption. This is the default setting when installing Control Manager.
- **Low**: All communication between Control Manager and managed products use 40-bit encryption. This is the least secure communication method between Control Manager and other products.

3. Select a host address for agents to communicate with Control Manager:
   - FQDN/host name
     a. Select **Fully qualified domain name (FQDN) or host name**.
     b. Select or type an FQDN or host name in the accompanying field.
   - IP address
     a. Select **IP address**.

        By default the IP address field displays an IPv4 address. When users install Control Manager on a pure IPv6 server, the IP address field displays the local IPv4 address (127.0.0.1).
4. Click **Next**.

   The **Specify Web Server Information** screen appears.

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

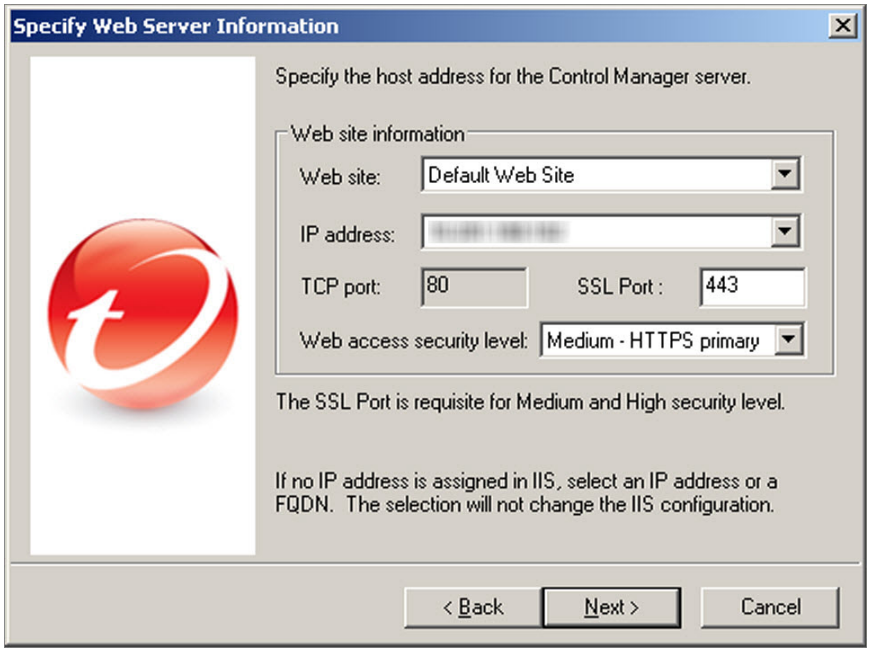


FIGURE 3-8. Specify web server information

5. From the **Web site** list, select the website to access Control Manager.

6. From the IP address list, select the FQDN/host name, IPv4, or IPv6 address you want to use for the Control Manager Management Console. This setting defines how the Control Manager communication system identifies your Control Manager server. The setup program attempts to detect both the server's fully qualified domain name (FQDN) and IP address and displays them in the appropriate field.

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

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

7. From the Web access security level list, select the security level for Control Manager communication. The options are as follows:

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

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

Specifying Backup Settings

Procedure

1. Click **Next**.

The **Choose Destination Location** screen appears.

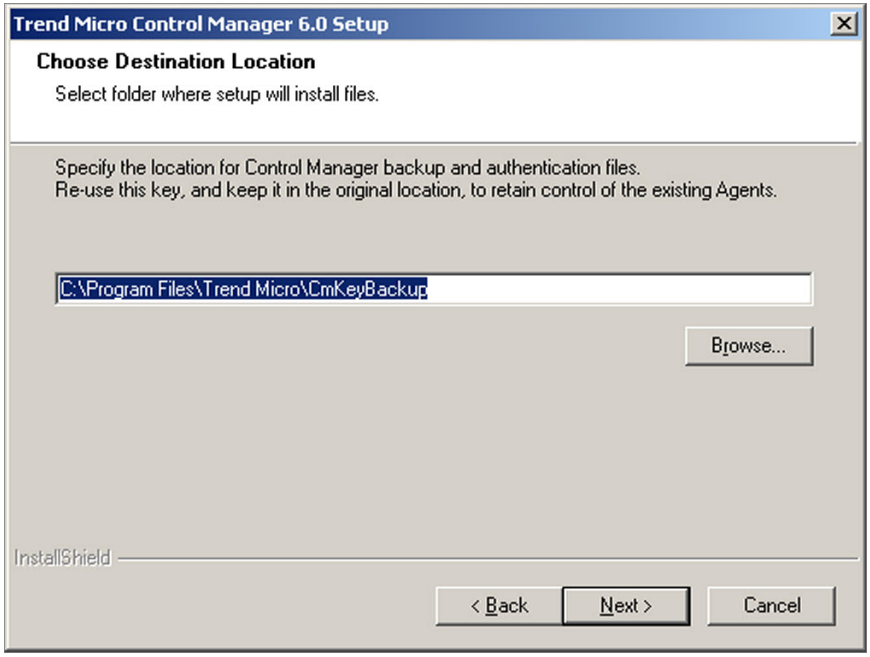


FIGURE 3-9. Choose a destination location for backup and authentication files

2. Specify the location of the Control Manager backup and authentication files (for more information see *Chapter 4, Table 4-2: Control Manager files that should be backed up on page 4-6*). Click **Browse** to specify an alternate location.

Configuring Notification Settings

Procedure

1. Click **Next**.

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

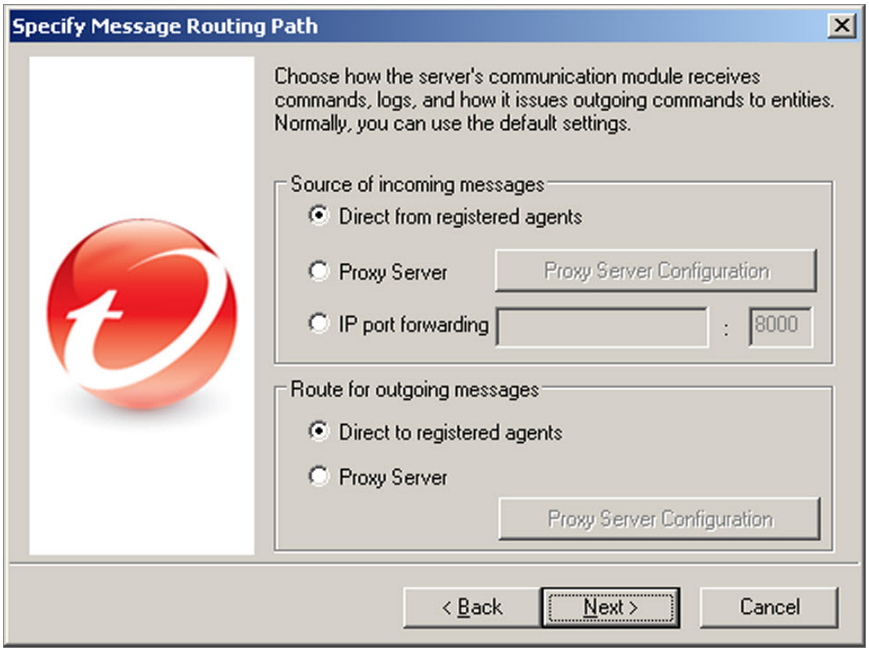


FIGURE 3-10. Define routes for messages or requests

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

Note

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

- Source of incoming messages

- **Direct from registered agents**: The agents can directly receive incoming messages.
- **Proxy server**: Uses a proxy server when receiving messages.
- **IP port forwarding**: This feature configures Control Manager to work with the IP port forwarding function of your company's firewall. Provide the firewall server's FQDN, IP address, or NetBIOS name, and then type the port number that Control Manager opened for communication.

- Route for outgoing messages
  - **Direct to registered agents**: Control Manager sends outgoing messages directly to the agents.
  - **Proxy server**: Control Manager sends outgoing messages through a proxy server.

Configuring Database Information

Important

You must manually install .NET Framework 3.5 SP1 before installing Control Manager.

Procedure

1. Click **Next**.

The **Setup Control Manager Database** screen appears.

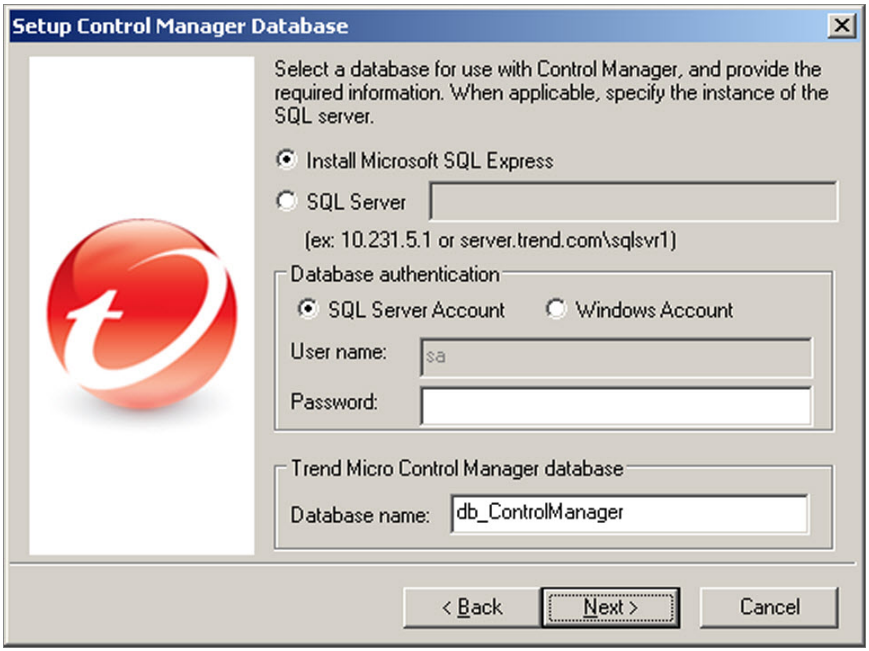


FIGURE 3-11. Choose the Control Manager database

2. Select a database to use with Control Manager.

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

     Tip

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

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

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

  To specify an alternative server, identify it using its FQDN, IPv4 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`

  Note

  If users choose to use a remote SQL server, do not specify an IPv6 address in the SQL Server field. Control Manager cannot identify the remote database by its IPv6 address.

3. Provide credentials to access the SQL server in **Database authentication**.

   - **SQL Server Account**

     By default, the user name is **sa**.

   - **Windows Account**

     Type the user name in this format: **domain name\user name**. The account should meet the following requirements:

     - Belongs to the **Administrators Group**
     - Contains the **Log on as a service** and **Log on as a batch job** user rights
     - Contains the **dbcreator** and **db_owner** database roles

   WARNING!

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

4. Under **Trend Micro Control Manager database**, provide a name for the Control Manager database. The default name is db_ControlManager.

5. Click **Next** to create the required database. If the setup program detects an existing Control Manager database, you have the following options:

   - **Append new records to existing database**: The Control Manager you install retains the same settings, accounts, and Product Directory entities as the previous server. In addition, Control Manager retains the root account of the previous installation. You cannot create a new root account.

     Note

     When installing Control Manager 6.0, you cannot select Append new records to existing database for previous Control Manager database versions.

   - **Delete existing records, and create a new database**: The existing database is deleted, and another is created using the same name.

   - **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.

Setting Up Root Account

Procedure

1. Click **Next**.

The **Create Root Account** screen appears.

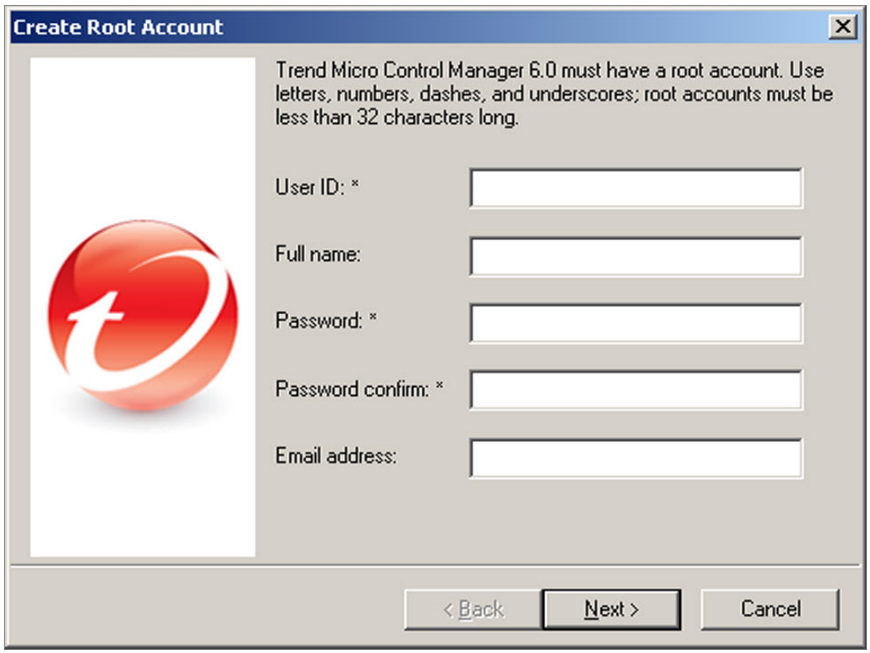


FIGURE 3-12. Provide information for the Control Manager root account

2. Provide the following required account information:
   - User ID
   - Full name
   - Password
   - Password confirmation
   - Email address
3. Click **Next**.
4. Click **Finish** to complete the installation.

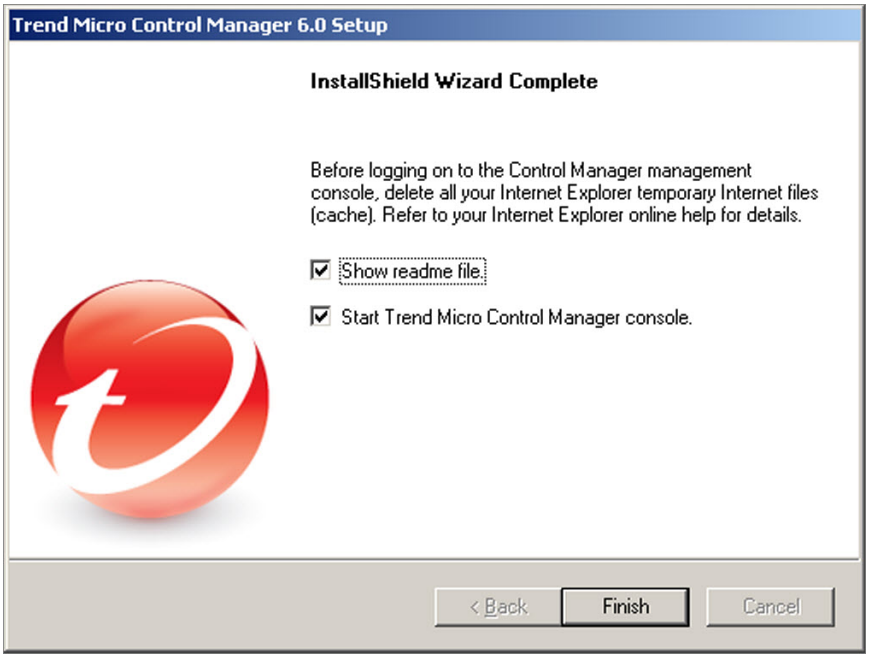


FIGURE 3-13. Setup complete

Verifying a Successful Control Manager Server Installation

To confirm a successful Control Manager server installation, check the items in the following table.

ITEM	DESCRIPTION
Control Panel > **Add/Remove Programs** dialog	The following programs appear in Add/Remove Programs: • Trend Micro Common CGI • Trend Micro Control Manager • Trend Micro Management Infrastructure • Microsoft Visual C++ 2005 Redistributable (latest version) • .NET Framework 3.5 SP1 • PHP 5.3.5 • Crystal Report 2008 Runtime SP4 • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2008 R2 Native Client • Microsoft SQL Server 2008 R2 Setup • Microsoft SQL Server 2008 Setup Support Files • Microsoft SQL Server Browser • Microsoft SQL Server VSS Writer • FastCGI (only appears in Windows Server 2003)

ITEM	DESCRIPTION
`C:\Program Files`	The following folders appear under the directory: • `Trend Micro\Common\TMI` • `Trend Micro\Common\CCGI` • `Trend Micro\Control Manager` • `PHP` **Note** The PHP folder should be created by the Control Manager installation.
Control Manager Database files	• db_ControlManager.mdf • db_ControlManager_Log.LDF
The setup program creates the following services and processes	
Control Manager Services	• Trend Micro Control Manager • Trend Micro Common CGI • Trend Micro Management Infrastructure • Trend Micro Network Time Protocol
CCGI processes	• Jk_nt_service.exe • Java.exe
IIS process	Inetinfo.exe (Internet Information Services)
ISAPI filters	• CCGIRedirect • ReverseProxy • TmcmRedirect

ITEM	DESCRIPTION
TMI processes	• CM.exe (TMI-CM) • MRF.exe (Message Routing Framework Module) • DMServer.exe (TMI-DM full-function)
Control Manager processes	• ProcessManager.exe • LogReceiver.exe • MsgReceiver.exe • LogRetriever.exe • CmdProcessor.exe • UIProcessor.exe • ReportServer.exe • NTPD.exe (appears when users chose to turn on the Trend Micro NTP server during the installation) • DCSProcessor.exe • CasProcessor.exe • sCloudProcessor.NET.exe
Message Queue process	LogProcessor.exe

Post-installation Configuration

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

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

4. Set notifications

Registering and Activating Control Manager

After successfully installing Control Manager, please check the license status and expiration date in the web console, by selecting **Administration** > **License Management** > **Control Manager**. If the status is not *Activated* or is expired, obtain an Activation Code and activate your software (in the web console, select **Administration** > **License Management** > **Control Manager** > **Specify a new Activation Code**). If you experience issues with your Activation Code, please contact technical support. For more information, see *Registering and Activating Your Software on page 3-28*.

Configuring User Accounts

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

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

Downloading the Latest Components

After the 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 Trend Micro server and the Internet, configure the proxy server settings (in the web console, select **Administration** > **Settings** > **Proxy Settings**).

Setting Notifications

After the installation, configure the events that will trigger notifications to monitor significant virus/malware attacks and related security activities. Besides specifying

notification recipients, choose notification channels and test them to make sure they work as expected (in the web console, select **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 install Control Manager for the first time:

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

  Register online and obtain an Activation Code to activate the product.

- You install an evaluation version

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

About Activating Control Manager

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

Note

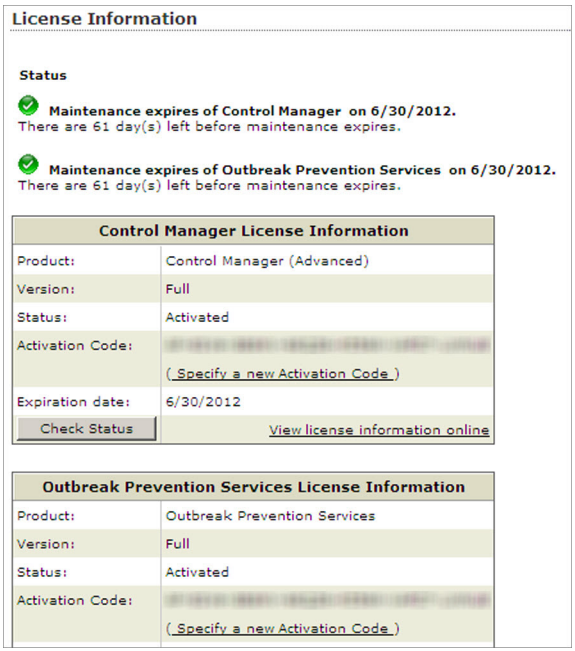
After activating Control Manager, log off and then log on to the Control Manager web console for changes to take effect.

Activating Control Manager

Procedure

1. Navigate to **Administration** > **License Management** > **Control Manager**.

   The **License Information** screen appears.



2. Click the **Specify a new Activation Code** link.

3. In the **New** box, type your Activation Code. If you do not have an Activation Code, click the **Register online** link and follow the instructions on the Online Registration website to obtain one.

4. Click **Activate**, and then click **OK**.

Converting to the Full Version

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

Procedure

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

Renewing Your Product Maintenance

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

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

Renewing Product Maintenance Using Check Status Online

Procedure

1. Navigate to **Administration** > **License Management** > **Control Manager**.

   The **License Information** screen appears.

2. On the working area under **Control Manager License Information**, click **Check Status Online**, and then click **OK**.

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

Renewing Maintenance by Manually Entering an Updated Activation Code

Procedure

1. Navigate to **Administration** > **License Management** > **Control Manager**.

   The **License Information** screen appears.

2. On the working area under **Control Manager License Information**, click the **Activate the product** link.

3. Click the **Specify a new Activation Code** link and follow the instructions on the Online Registration website.

4. In the **New** box, type your Activation Code.

5. Click **Activate**.

6. Click **OK**.

Chapter 4

Upgrading Servers or Migrating Agents to Control Manager

Upgrading existing Control Manager 5.0/5.5 servers to Control Manager 6.0 requires careful consideration and detailed planning. Likewise, the same is true when migrating MCP and older Control Manager agents to a Control Manager 6.0 server.

This chapter contains the following topics:

Upgrading to Control Manager 6.0

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

TABLE 4-1. Considerations for Upgrading to Control Manager 6.0

CAPABILITY	STANDARD EDITION	ADVANCED EDITION
Retain the reporting functions	No	Yes
Upgrade a Standard Edition to Advanced Edition To upgrade from a Standard Edition to an Advanced Edition, obtain an Advanced Edition Activation Code (AC), and then change the AC from the **License Management** screen.	Yes	N/A
Convert an Enterprise/ Advanced Edition to Standard Edition	N/A	Yes

Upgrading Control Manager 5.0/5.5 Servers

Trend Micro recommends installing Control Manager 6.0 over the previous installations of Control Manager. By doing so all your previous settings, logs, reports, and Product Directory remain the same. However, before upgrading, verify that the server where Control Manager installs has sufficient system resources.

Supported Versions for Upgrade

Control Manager supports upgrading from the following versions installed on the IIS default website:

- Control Manager 5.5 SP1

- Control Manager 5.5
- Control Manager 5.0

WARNING!

Always back up the existing server before performing the upgrade.

Upgrading and Migrating Scenarios

Control Manager supports three scenarios for upgrade and migration:

- *Scenario 1: Upgrading a Control Manager 5.0/5.5 Server to Control Manager 6.0 on page 4-3*
- *Scenario 2: Migrating to a Fresh Control Manager 6.0 Installation Using the Agent Migration Tool on page 4-5*
- *Scenario 3: Upgrading or Migrating a Cascading Environment on page 4-5*

Scenario 1: Upgrading a Control Manager 5.0/5.5 Server to Control Manager 6.0

When upgrading Control Manager 5.0/5.5 directly to Control Manager 6.0, administrators can choose to back up Control Manager or back up the entire operating system of the server on which Control Manager installs. Backing up the operating system is more labor intensive but provides better security to prevent data loss.

Upgrading by Backing Up the Previous Control Manager Server and Database

Procedure

1. Back up the existing Control Manager 5.0/5.5 database.
2. Back up all the files under `\Trend Micro\CmKeyBackup\*.*`.
3. Back up all folders of the current Control Manager 5.0/5.5 server.

4. Back up the registries of the current Control Manager 5.0/5.5 server.

Note

See *Table 4-2: Control Manager files that should be backed up on page 4-6* for step 2 through 4.

5. Install Control Manager 6.0 over Control Manager 5.0/5.5.

Upgrading by Backing Up the Entire Operating System of the Server and the Control Manager Database

Procedure

1. Back up the operating system of existing Control Manager 5.0/5.5 server.
2. Back up the existing Control Manager 5.0/5.5 database.
3. Install Control Manager 6.0 over Control Manager 5.0/5.5.

Upgrade Flow

To upgrade Control Manager 5.0/5.5 to Control Manager 6.0, run the installation program (`Setup.exe`) as described in step 1 of *Installing All Required Components on page 3-5*. Follow the steps to upgrade Control Manager.

Important

You must manually install .NET Framework 3.5 SP1 before upgrading Control Manager.

The upgrade process is very similar to fresh installation except the following:

- The installation program upgrades the Visual C++ 2005 SP1 Redistribution Package
- (For upgrading from Control Manager 5.5 only) The installation program upgrades the existing PHP from the server

- The installation program migrates the existing database to Control Manager 6.0.

Scenario 2: Migrating to a Fresh Control Manager 6.0 Installation Using the Agent Migration Tool

This scenario involves installing Control Manager 6.0 on a separate server from the existing Control Manager server. This method allows you to slowly decommission the previous server. See *Planning Control Manager Agent Migration on page 4-10* for more information about migrating agents.

Migrating a Control Manager 5.0/5.5 Server to a Fresh Installation of Control Manager 6.0

Procedure

1. Back up the existing Control Manager 5.0/5.5 database.
2. Perform a fresh installation of Control Manager 6.0 on a different computer.
3. Use the Agent Migration Tool to migrate entities from the Control Manager 5.0/5.5 server to the Control Manager 6.0 server.

Note

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

Scenario 3: Upgrading or Migrating a Cascading Environment

Control Manager supports upgrading a cascading environment. To upgrade a cascading environment, unregister and then re-register the child Control Manager servers.

Procedure

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

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

CONTROL MANAGER 5.0/5.5/6.0 INFORMATION	LOCATION
Database	Use the SQL Enterprise Manager or osql to back up the Control Manager database. Refer to the Control Manager backup db_ControlManager using SQL Enterprise Manager / osql online help topics for detailed steps.
Authentication information (Ensures that managed products reporting to the Control Manager server will report to the same server if Control Manager is restored)	`\Program Files\Trend Micro \CmKeyBackup\*.*`
GUID information	GUID value in `\Program files\Trend Micro\COMMON\TMI\TMI.cfg`

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

CONTROL MANAGER 5.0/5.5/6.0 INFORMATION	LOCATION
ActiveUpdate files	`\Program Files\Trend Micro \Control Manager\webui\download \Activeupdate`

Control Manager registry	**For 32-bit operating systems**:
	`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\MSSQLServer`
	`HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services\TMCM`

CONTROL MANAGER 5.0/5.5/6.0 INFORMATION	LOCATION
Control Manager registry	**For 64-bit operating systems**: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\TVCS HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\TMI\ HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\CommonCGI HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\TMCM HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\TMI HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMCM
Control Manager registry	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\MSSQL$SQLEXPRESS

Rolling Back to Control Manager 5.0/5.5 Servers

If upgrading to Control Manager 6.0 is unsuccessful, perform the following steps to roll back to your Control Manager 5.0/5.5 system.

Scenario 1: Rolling Back a Control Manager 6.0 Server to Control Manager 5.0/5.5

Use one of the following methods to roll back the Control Manager 5.0/5.5 system:

- Roll back from a Control Manager server and database backup
- Roll back from an entire operating system of the server and the Control Manager database backup

Rolling Back from a Control Manager Server and Database Backup

Procedure

1. Remove the Control Manager 6.0 server.
2. Install the Control Manager 5.0/5.5 server.
3. Apply the required Control Manager 5.0/5.5 service packs and hot fixes.

   WARNING!

   Apply only the service packs and hot fixes that the original Control Manager 5.0/5.5 server had installed.

4. Restore the Control Manager 5.0/5.5 database with the backup database.
5. Restore all the Control Manager 5.0/5.5 folders with the backed up folders.
6. Restore Control Manager 5.0/5.5 registries with the backed up registries.

7. Restore all the files under `\Trend Micro\CmKeyBackup\*.*`.
8. Import the old certificate.

Rolling Back from an Entire Operating System of the Server and the Control Manager Database Backup

Procedure

1. Restore the Control Manager 5.0/5.5 database with the backup database.
2. Restore the operating system of the server with the backed up operating system.

Scenario 2: Rolling Back a Cascading Environment

Procedure

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

Planning Control Manager Agent Migration

There are two ways to migrate agents to a Control Manager 6.0 server:

- Rapid upgrade
- Phased upgrade

Rapid Upgrade

Rapid upgrade works using the approach presented in the table below.

TABLE 4-3. Rapid Upgrade

ORIGINAL SERVER/AGENT	ACTION
Control Manager 5.0/5.5 with MCP agents	Register MCP agents to the Control Manager 6.0 server and then re-organize the Product Directory structure
Control Manager 5.0/5.5 with mixed agents	Register MCP agents to the Control Manager 6.0 server and then re-organize Product Directory structure

Trend Micro recommends rapid upgrade for migrating agents in a laboratory setting or in relatively small networks, preferably during test deployments (see *Testing Control Manager at One Location on page 2-12*). However, since you cannot stop the migration once it starts, this method works best for smaller deployments. The degree of difficulty increases with the size of the network.

Phased Upgrade

Trend Micro recommends a phased upgrade for large, single-server Control Manager 5.0/5.5 networks. This is essential for multiple-server networks. This method offers a more structured approach to migrating your system, and follows these guidelines:

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

  This will simplify any troubleshooting that may be required.

Phased upgrade involves the following steps:

1. Install Control Manager 6.0 on a server that does not have any previous Control Manager version installed (preferably without any managed products).
2. Run the `AgentMigrateTool.exe` tool on the Control Manager 6.0 server.

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

Migration Scenarios for Control Manager 2.x Agents

The following agent migration scenarios are possible:

- Single-server migration
- Consolidations of different servers/agents

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 and Migrating Scenarios on page 4-3*.

Consolidation of Different Servers/Agents

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

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

Control Manager 2.5x Agent Migration Flow

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

1. Stops the Trend Micro Management Infrastructure service
2. Obtains the Product Directory information from the Control Manager 5.0/5.5 server
3. Removes the agent information from the Control Manager 5.0/5.5 database and `TMI.cfg`

4. Retains the Control Manager 2.5x agent version (no upgrade takes place)
5. Writes the agent information to the Control Manager 6.0 database and `TMI.cfg`
6. Restarts the Trend Micro Management Infrastructure service

If `AgentMigrationTool.exe` cannot complete or finish the Control Manager 2.5x agent migration, it removes the agent information from the Control Manager 6.0 database and `TMI.cfg` and then writes the information back to the Control Manager 5.0/5.5 database.

MCP Agent Migration Flow

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

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

Migrating Control Manager 2.5x and MCP Agents

Use `AgentMigrateTool.exe` to migrate Windows-based agents originally administered by Control Manager 5.0/5.5 servers. When migrating agents, 2.5x agents migrate first, then MCP agents migrate.

If an agent migration is unsuccessful, the following occurs:

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

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

Note

Run `AgentMigrateTool.exe` directly on the destination server — a Control Manager 6.0 server to which you migrate the agents.

Procedure

1. Using Windows Explorer, open the Control Manager 6.0 root folder. For example: `<root>\Program Files\Trend Micro\Control Manager\`
2. Double-click `AgentMigrateTool.exe`.

   Note

   Remember to start the Remote Registry service on the destination Control Manager server or agent migration will not be successful.

3. Click **Configure Source Server Settings** on the main menu.
4. On the Configurations screen under **Source server**, type the **IP address** of the source server hosting the agents that will migrate.
5. Under **System Administrator Account**, specify the administrator **user name** and **password** used to access the source server, and then click **Connect**.
6. On the main window, click **Add >** or **Add All >>** to migrate agents from the **Source** to the **Destination** list.
7. Select all or one of the following options:
   - **Retain tree structure**: `AgentMigrateTool.exe` instructs the destination server (a Control Manager 6.0 server) to retain the original Product Directory structure of the selected managed products

- **Migrate logs**: `AgentMigrateTool.exe` copies the logs of the selected managed products from the source to the destination server
- **Enable HTTPS**: `AgentMigrateTool.exe` notifies migrating agents to use HTTPS to register to Control Manager. If you do not select this option, agents use HTTP to register to Control Manager

  These options apply to agents listed in the Destination list.

Note

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

8. Click **Migrate**. `AgentMigrateTool.exe` migrates the agent(s) listed in the Destination list.

Migrating the Control Manager Database

To migrate a Control Manager 5.0/5.5 database, install Control Manager 6.0 on a Control Manager 5.0/5.5 server. This is the recommended method.

The Control Manager 6.0 setup program automatically upgrades the database to version 6.0.

Migrating a Control Manager SQL Database to Another SQL Server

To move a Control Manager database from an SQL Server to another SQL Server, use the DBConfig tool to perform the migration.

Using the DBConfig Tool

The DBConfig tool allows users to change the user account, password, and the database name for the Control Manager database.

The tool offers the following options:

- **DBName:** Database name
- **DBAccount:** Database account
- **DBPassword:** Database password
- **Mode:** Database's authentication mode (SQL or Windows authentication)

Note

The default mode is SQL authentication mode, however Windows authentication mode is necessary when configuring for Windows authentication.

Procedure

1. From the Control Manager server, click **Start** > **Run**.
2. Type `cmd`, and then click **OK**.

   The command prompt screen appears.
3. Change the directory to the Control Manager root directory (for example, `<root>\Program Files\Trend Micro\Control Manager\DBConfig`).
4. Type `dbconfig`.

   The DBConfig tool interface appears.
5. Specify which settings you want to modify:
   - **Example 1:** `DBConfig -DBName="db_your_database>" -DBAccount="sqlAct" -DBPassword="sqlPwd" -Mode="SQL"`
   - **Example 2:** `DBConfig -DBName="db_your_database>" -DBAccount="winAct" -DBPassword="winPwd" -Mode="WA"`
   - **Example 3**: `DBConfig -DBName="db_your_database>" -DBPassword="sqlPwd"`

Chapter 5

Removing Trend Micro Control Manager

This chapter contains information about how to remove Control Manager components from your network, including the Control Manager server, Control Manager agents, and other related files.

This chapter contains the following sections:

Removing a Control Manager Server

You have two ways to remove Control Manager automatically (the following instructions apply to a Windows 2003 environment; details may vary slightly, depending on your Microsoft Windows platform):

Procedure

- From the Start menu, click **Start** > **Programs** > **Trend Micro Control Manager** > **Uninstalling Trend Micro Control Manager**.
- Using Add/Remove Programs:

  a. Click **Start** > **Settings** > **Control Panel** > **Add/Remove Programs**.

  b. Select **Trend Micro Control Manager**, and then click **Remove**. This action automatically removes other related services, such as the Trend Micro Management Infrastructure and Common CGI services, as well as the Control Manager database.

  c. Click **Yes** to keep the database, or **No** to remove the database.

  Note

  Keeping the database allows you to reinstall Control Manager on the server and retain all system information, such as agent registration, and user account data.

  If you reinstalled the Control Manager server, and deleted the original database, but did not remove the agents that originally reported to the previous installation, then the agents will re-register with the server when:

  - Managed product servers restart the agent services
  - Control Manager agents verify their connection after an 8-hour period

Manually Removing Control Manager

This section describes how to remove Control Manager manually. Use the procedures below only if the Windows Add/Remove function or the Control Manager uninstall program is unsuccessful.

Note

Windows-specific instructions may vary between operating system versions. The following procedures are written for **Windows Server 2003**.

Removing Control Manager actually involves removing distinct components. These components may be removed in any order; they may even be removed together. However, for purposes of clarity, the uninstallation for each module is discussed individually, in separate sections. The components are:

- Control Manager application
- Trend Micro Management Infrastructure
- Common CGI Modules
- Control Manager Database (optional)
- PHP
- FastCGI

Other Trend Micro products also use the Trend Micro Management Infrastructure and Common CGI modules, so if you have other Trend Micro products installed on the same computer, Trend Micro recommends not removing these two components.

Note

After removing all components, you must restart your server. You only have to do this once — after completing the removal.

Removing the Control Manager Application

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

Stopping Control Manager Services

Use the Windows Services screen to stop all of the following Control Manager services:

- Trend Micro Management Infrastructure
- Trend Micro Common CGI
- Trend Micro Control Manager
- Trend Micro NTP

Note

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

Stopping Control Manager Services from the Windows Services Screen

Procedure

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

Stopping IIS and Control Manager Services from the Command Prompt

Procedure

- Run the following commands at the command prompt:

  ```
  net stop w3svc
  ```

  ```
  net stop tmcm
  ```

Removing Control Manager IIS Settings

Remove the Internet Information Services settings after stopping the Control Manager services.

Procedure

1. From the Control Manager server, click **Start** > **Run**.

   The **Run** dialog box appears.

2. Type the following in the **Open** field:

   ```
   %SystemRoot%\System32\Inetsrv\iis.msc
   ```

3. On the left-hand menu, double-click the server name to expand the console tree.

4. Double-click **Default Web Site**.

5. Delete the following virtual directories:

   - ControlManager
   - TVCSDownload
   - crystalreportviewers12
   - TVCS
   - Jakarta

- WebApp

6. On IIS 6 only:

   a. Right-click the IIS website you set during the installation.

   b. Click **Properties**.

7. Select the **ISAPI Filters** tab.

8. Delete the following ISAPI filters:

   - TmcmRedirect
   - CCGIRedirect
   - ReverseProxy

9. On IIS 6 only, delete the following web service extensions:

   - Trend Micro Common CGI Redirect Filter (If removing CCGI)
   - Trend Micro Control Manager CGI Extensions

Removing Crystal Reports, PHP, FastCGI, TMI, and CCGI

Removal of PHP, FastCGI, TMI and CCGI is optional. Use Add/Remove Programs to uninstall Crystal Reports, PHP, and FastCGI.

Removing Crystal Reports

Procedure

1. On the Control Manager server, click **Start** > **Settings** > **Control Panel** > **Add/ Remove Programs**.

2. Scroll down to Crystal Reports Runtime Files, and then click **Remove** to remove the Crystal Reports related files automatically.

Removing PHP and FastCGI

Procedure

1. On the Control Manager server, click **Start** > **Settings** > **Control Panel** > **Add/ Remove Programs**.
2. Scroll down to PHP, and then click **Remove** to remove PHP related files automatically.
3. Scroll down to FastCGI, and then click **Remove** to remove FastCGI related files automatically.

Removing TMI and CCGI

Procedure

1. Run the Microsoft service tool `Sc.exe`.
2. Type the following commands:

```
sc delete "TrendCGI"
```

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

Deleting Control Manager Files/Directories and Registry Keys

Procedure

1. Delete the following directories:
   - `.Trend Micro\Control Manager`
   - `.Trend Micro\COMMON\ccgi`
   - `.Trend Micro\COMMON\TMI`

- .PHP
- C:\Documents and Settings\All Users\Start Menu\Programs \PHP 5
- C:\Documents and Settings\All Users\Start Menu\Programs \Trend Micro Control Manager

2. Delete the following Control Manager registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\CommonCGI
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro \DamageCleanupService
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\MCPAgent
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OPPTrustPort
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TMI
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TVCS
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro \VulnerabilityAssessmentServices
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Uninstall\TMCM
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Uninstall\TMI
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \TMCM
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \TrendCCGI
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \TrendMicro Infrastructure
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \TrendMicro_NTP

Removing the Database Components

This section describes how to remove the following database components from the Control Manager server:

- Removing Control Manager ODBC Settings
- Removing the Control Manager SQL Server 2008 Express Database

Removing Control Manager ODBC Settings

Procedure

1. On the Control Manager server, click **Start** > **Run**.

   The **Run** dialog box appears.

2. Type the following in the Open field:

   `odbcad32.exe`

3. On the **ODBC Data Source Administrator** screen, click the **System DSN** tab.
4. Under **Name**, select **ControlManager_Database**.
5. Click **Remove**, and then click **Yes** to confirm.

Removing the Control Manager SQL Server 2008 R2 Express Database

Procedure

1. On the Control Manager server, click **Start** > **Control Panel** > **Add/Remove Programs**.
2. Scroll down to **SQL Server 2008 R2** and then click **Remove** to remove the related files automatically.

Tip

Trend Micro recommends visiting the Microsoft website for instructions on removing SQL Server 2008 R2 Express if you have any issues with the uninstallation:

http://support.microsoft.com/kb/955499

Removing Control Manager and NTP Services

Procedure

1. Run the Microsoft service tool `Sc.exe`.
2. Type the following commands:

```
sc delete "TMCM"

sc delete "TrendMicro_NTP"
```

Removing a Windows-Based Control Manager 2.x Agent

To remove one or more agents, you must run the uninstallation component of the Control Manager Agent setup program.

Uninstall agents remotely, either by running the program from the Control Manager server, or another server, or locally, by running the setup program on the agent computer.

Procedure

1. Navigate to **Administration** > **Settings** > **Product Agent Settings**.

   The **Product Agent Settings** screen appears.

2. Click the **RemoteInstall.exe** link to download the application.

3. Using Microsoft Explorer, go to the location where you saved the agent setup program.

4. Double-click the `RemoteInstall.exe` file.

   The **Trend Micro Control Manager Agent Setup** screen appears.

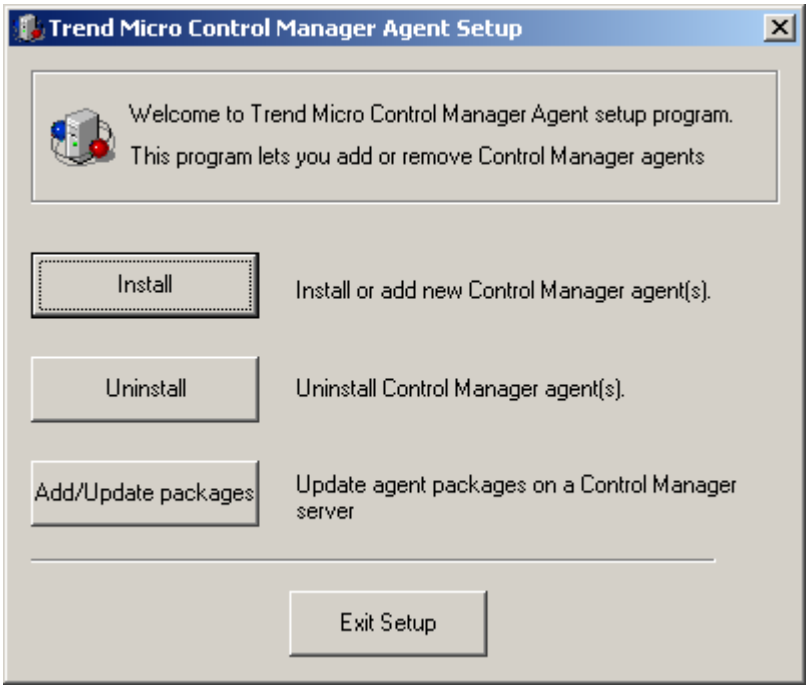


FIGURE 5-1. Trend Micro Control Manager Agent setup program

5. Click **Uninstall**.

   The **Welcome** screen appears.

6. Click **Next**.

The **Control Manager source server logon** screen appears.

FIGURE 5-2. Control Manager source server logon

7. Specify and provide Administrator-level logon credentials for the Control Manager server. Type the following information:
   - Host name
   - User name
   - Password
8. Click **Next**. Select the product whose agent you want to remove.
9. Click **Next**. Select the servers from which to remove the agents. You have two ways to select those servers:
   - To select from the list:

   a. In the left list box, double-click the domain containing the antivirus servers, and the domain expands to show all the servers inside.

b. Select the target server(s) from the left list box, and then click **Add**. The chosen server appears on the right list box. Click **Add All** to add agents to all servers in the selected chosen domain. Alternatively, you can double-click on a server to add it to the left list.

- To specify a server name directly:

a. Type the server's FQDN or IP address in the **Server name** field.

b. Click **Add**. The server appears on the right list box. To remove servers from the list, select a server from the right list box, and then click **Remove**. To remove all servers, click **Remove All**.

10. Click **Back** to return to the previous screen, **Exit** to abort the operation, or **Next** to continue.

11. Provide Administrator-level logon credentials for the selected servers. Type the required user name and password in the appropriate field.

12. Click **OK**. The **Analyze Chosen Server** screen provides the following details about the target servers: server name, domain, and the type of agent detected.

13. 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.

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

Chapter 6

Getting Support

Trend Micro has committed to providing service and support that exceeds our users' expectations. This chapter contains information on how to get technical support. Remember, you must register your product to be eligible for support.

This chapter contains the following topics:

Before Contacting Technical Support

Before contacting Technical Support, here are two things you can quickly do to try and find a solution to your problem:

- **Check your documentation**: the manual and online help provide comprehensive information about Control Manager. Search both documents to see if they contain your solution.
- **Visit our Technical Support website**: our Technical Support website contains the latest information about all Trend Micro products. The support website has answers to previous user inquiries.

  To search the Knowledge Base, visit

  http://esupport.trendmicro.com/en-us/default.aspx

Contacting Technical Support

Trend Micro provides technical support, pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance. If you need help or just have a question, please feel free to contact us. We also welcome your comments.

- Get a list of the worldwide support offices at *http://esupport.trendmicro.com*
- Get the latest Trend Micro product documentation at *http://docs.trendmicro.com*

In the United States, you can reach the Trend Micro representatives through phone, fax, or email:

```
Trend Micro, Inc.
10101 North De Anza Blvd.,
Cupertino, CA 95014
Toll free: +1 (800) 228-5651 (sales)
Voice: +1 (408) 257-1500 (main)
Fax: +1 (408) 257-2003
Web address: http://www.trendmicro.com
Email: support@trendmicro.com
```

Resolve Issues Faster

To resolve the issue faster, when you contact our staff, provide as much of the following information as you can:

- Product serial number
- Control Manager Build version
- Operating system version, Internet connection type, and database version (for example, SQL 2005 or SQL 2008)
- Exact text of the error message, if any
- Steps to reproduce the problem

TrendLabs

Trend Micro TrendLabs℠ is a global network of antivirus research and product support centers providing continuous, 24 x 7 coverage to Trend Micro customers worldwide.

Staffed by a team of more than 250 engineers and skilled support personnel, the TrendLabs dedicated service centers worldwide ensure rapid response to any virus outbreak or urgent customer support issue, anywhere in the world.

The TrendLabs modern headquarters earned ISO 9002 certification for its quality management procedures in 2000. TrendLabs is one of the first antivirus research and support facilities to be so accredited. Trend Micro believes that TrendLabs is the leading service and support team in the antivirus industry.

For more information about TrendLabs, please visit:

http://us.trendmicro.com/us/about/company/trendlabs/

Other Useful Resources

Trend Micro offers a host of services through its website, http://www.trendmicro.com.

Internet-based tools and services include:

- **Trend Micro™ Smart Protection Network™**: monitor security threat incidents around the world
- **HouseCall™**: Trend Micro online virus scanner

Appendix A

Control Manager System Checklists

Use the checklists in this appendix to record relevant system information as a reference.

This appendix contains the following sections:

Server Address Checklist

You must provide the following server address information during the installation process, as well as during the configuration of the Control Manager server to work with your network. Record the information here for easy reference.

TABLE A-1. Server Address Checklist

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
Control Manager server information		
IP address	10.1.104.255	
Fully qualified domain name (FQDN)	server.company.com	
NetBIOS (host) name	yourserver	
Web server information		
IP address	10.1.104.225	
Fully qualified domain name (FQDN)	server.company.com	
NetBIOS (host) name	yourserver	
SQL-based Control Manager database information		
IP address	10.1.104.225	
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	

Information Required	Sample	Your Value
SMTP server information (Optional; for email message notifications)		
IP address	10.1.123.225	
Fully qualified domain name (FQDN)	mail.company.com	
NetBIOS (host) name	mailserver	
SNMP Trap information (Optional; for SNMP Trap notifications)		
Community name	trendmicro	
IP address	10.1.194.225	

Ports Checklist

Control Manager uses the following ports for the indicated purposes.

Port	Sample	Your value
SMTP	25	
Proxy	8088	
Pager COM	COM1	
Proxy for Trend VCS Agent (Optional)	223	
Web Console and Update/ Deploy components	80	
Firewall, "forwarding" port (Optional; used during the Control Manager Agent installation)	224	

PORT	SAMPLE	YOUR VALUE
Trend Micro Management Infrastructure (TMI) internal process communication (for remote products)	10198	
TMI external process communication	10319	
Entity emulator	10329	

Note

Control Manager requires the exclusive use of ports 10319 and 10198.

Control Manager 2.x Agent Installation Checklist

The following information is used during agent installation.

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
Control Manager server administrator account user name	root	
Encryption key location	`C:\MyDocuments \E2EPulic.dat`	

Note

You can use any user name instead of the root account. However, Trend Micro recommends using the root account, because deleting the user name specified while installing the agent makes managing the agent very difficult.

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

Control Manager Conventions

Refer to the following conventions applicable for the Control Manager installation or web console configuration.

- User names

Max. length	32 characters
Allowed	A-Z, a-z, 0-9, -, _

- Folder names

Max. length	40 characters
Not allowed	/ > & "

Note

For the Control Manager server host name, the setup program supports servers with underscores ("_") as part of the server name.

Core Process and Configuration Files

Control Manager saves system configuration settings and temporary files in XML format.

The following tables describe the configuration files and processes used by Control Manager.

TABLE A-2. Control Manager Configuration Files

CONFIGURATION FILE	DESCRIPTION
AuthInfo.ini	Configuration file that contains information about private key file names, public key file names, certificate file names, and the encrypted passphrase of the private key as well as the host ID and port.
aucfg.ini	ActiveUpdate configuration file
TVCS_Cert.pem	Certificate used by SSL authentication
TVCS_Pri.pem	Private Key used by SSL
TVCS_Pub.pem	Public Key used by SSL
ProcessManager.xml	Used by ProcessManager.exe
CmdProcessorEventHandler.xml	Used by CmdProcessor.exe
UIProcessorEventHandler.xml	Used by UIProcessor.exe
DMRegisterinfo.xml	Used by CasProcessor.exe
DataSource.xml	Stores the connection parameters for Control Manager processes
SystemConfiguration.xml	Control Manager system configuration file
CascadingLogConfiguration.xml	Log upload configuration file used for child servers
agent.ini	MCP agent file
TMI.cfg	Trend Micro Management Infrastructure configuration file

TABLE A-3. Control Manager Processes

PROCESSES	DESCRIPTION
ProcessManager.exe	Launches and stops other Control Manager core processes.
CmdProcessor.exe	Sends XML instructions, formed by other processes, to managed products, processes product registration, sends alerts, performs scheduled tasks, and applies Outbreak Prevention Policies.
UIProcessor.exe	Processes and transforms user input made in the Control Manager web console into actual commands.
LogReceiver.exe	Receives managed product logs and messages.
LogProcessor.exe	Receives new messages from managed products and receives the entity information from child Control Manager servers.
LogRetriever.exe	Retrieves and saves logs in the Control Manager database.
ReportServer.exe	Generates Control Manager reports.
MsgReceiver.exe	Receives messages from the Control Manager server, managed products, and child servers.
CasProcessor.exe	Allows a Control Manager server (a parent server) to manage other Control Manager servers (child servers).
DCSProcessor.exe	Performs Damage Cleanup Services functions.
Ntpd.exe	Network Time Protocol service.
inetinfo.exe	Microsoft Internet Information Service process.

PROCESSES	DESCRIPTION
jk_nt_service.exe java.exe	Java server side extensions used to build Web-based user interface by defining the interface instead of using a lot of standalone CGI programs.
cm.exe	Manages dmserver.exe and mrf.exe.
mrf.exe	The Communicator process.
dmserver.exe	Provides the Control Manager web console log on page and manages the Product Directory (Control Manager-side).
sCloudProcessor.NET.exe	Manages tasks related to Policy Management.

Communication and Listening Ports

These are the default Control Manager communication and listening ports.

TYPE	COMMUNICATION PORT
Internal communication	10198
External communication	10319

SERVICE	SERVICE PORT
ProcessManager.exe	20501
CmdProcessor.exe	20101
UIProcessor.exe	20701
LogReceiver.exe	20201
LogProcessor.exe	21001
LogRetriever.exe	20301

Service	Service Port
ReportServer.exe	20601
MsgReceiver.exe	20001
EntityEmulator.exe	20401
CasProcessor.exe	20801
DcsProcessor.exe	20903

Control Manager Product Version Comparison

The following table provides a comparison of features between Control Manager versions.

Table A-4. Product Version Comparison

Features	Control Manager Version					
	5.0 Adv	5.0 Std	5.5 Adv	5.5 Std	6.0 Adv	6.0 Std
2.x and MCP agent interfaces with the managed products	●	●	●	●	●	●
Ad Hoc Query	●	●	●	●	●	●
Automatic component (for example, patterns/rules) update	●	●	●	●	●	●
Cascading management structure	●		●		●	
Central database for all virus log and system events	●	●	●	●	●	●
Centralized, web-based, virus management solution for the enterprise	●	●	●	●	●	●

Features	Control Manager Version					
	5.0 Adv	5.0 Std	5.5 Adv	5.5 Std	6.0 Adv	6.0 Std
Child server monitoring	●		●		●	
Child server task issuance	●		●		●	
Command Tracking	●	●	●	●	●	●
Communicator Heartbeat	●	●	●	●	●	●
Communicator Scheduler	●	●	●	●	●	●
Component download granularity	●	●	●	●	●	●
Configuration by group	●	●	●	●	●	●
Configure multiple download sources	●	●	●	●	●	●
Consistent managed product and Control Manager UI	●	●	●	●	●	●
Control Manager MIB files (previously called HP OpenView MIB)	●	●	●	●	●	●
Customized user types	●	●	●	●	●	●
Deployment Plans	●	●	●	●	●	●
Directory Manager	●	●	●	●	●	●
Enhanced Security Communication	●	●	●	●	●	●
Event Center	●	●	●	●	●	●
Improved Navigation	●	●	●	●	●	●
Improved User Interface	●	●	●	●	●	●

Features	Control Manager Version					
	5.0 Adv	5.0 Std	5.5 Adv	5.5 Std	6.0 Adv	6.0 Std
InterScan Web Security Service integration	●	●	●	●	●	●
Logging Enhancements	●	●	●	●	●	●
Log processing speed enhancements			●	●	●	●
Manage antivirus and content security products	●	●	●	●	●	●
Manage services	●	●	●	●	●	●
Managed product license manager	●		●		●	
Managed product reporting	●		●		●	
Web console rendering enhancement			●	●	●	●
Microsoft SQL Express or Microsoft SQL 2005	●	●	●	●	●	●
Microsoft SQL Express or Microsoft SQL 2008			●	●	●	●
Microsoft SQL 2012					●	●
MSDE or Microsoft SQL 7/2000	●	●				
MSN Messenger notification	●	●	●	●	●	●
Notification and Outbreak Alert	●	●	●	●	●	●
OfficeScan Integration Enhancements			●	●	●	●

Features	Control Manager Version					
	5.0 Adv	5.0 Std	5.5 Adv	5.5 Std	6.0 Adv	6.0 Std
Outbreak Commander / Outbreak Prevention Services (OPS) • Automatic Download and Deployment of OPP • Manual Download and Deployment of OPP	●	●	●	●	●	●
Passive Support for 3rd Party Product	●		●		●	
Policy management					●	●
Remote and Local Agent Installation	●	●	●	●	●	●
Remote management	●	●	●	●	●	●
Reporting	●		●		●	
Secure communication between Server and Agents	●	●	●	●	●	●
Single sign-on (SSO) for managed products that support SSO	●	●	●	●	●	●
Smart Protection Network integration			●	●	●	●
SNMP trap notification	●		●		●	
SSL support for ActiveUpdate	●	●	●	●	●	●
SSL support for web console	●	●	●	●	●	●
Support Control Manager 2.x agents	●	●	●	●	●	●

Features	Control Manager Version					
	5.0 Adv	5.0 Std	5.5 Adv	5.5 Std	6.0 Adv	6.0 Std
Support HTTPS communication between server, agents, and managed products	●	●	●	●	●	●
Support MCP agents	●	●	●	●	●	●
Syslog notification	●		●		●	
Threat Intelligence-Oriented Dashboard			●	●	●	●
Trend Micro InterScan for Cisco Content Security and Control Security Services Module (ISC CSC SSM) integration	●	●	●	●	●	●
Trend Micro Network VirusWall 1200 integration	●	●	●	●	●	●
Trend Micro Network VirusWall 2500 integration	●	●	●	●	●	●
Trend Micro Product Registration server integration	●	●	●	●	●	●
TrendLabs Message Board	●	●	●	●		
User account management	●	●	●	●	●	●
Vulnerability Assessment	●	●	●	●	●	●
Windows Authentication	●	●	●	●	●	●
Work-hour control	●	●	●	●	●	●

Index