TREND MICRO™

# 7.0 TREND MICRO™ Control Manager

## Installation and Upgrade Guide

Centralized Security Management for the Enterprise

Document Part No.: CMEM77943/170818

Release Date: November 2017

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

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

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.

Evaluate this documentation on the following site:

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

# Table of Contents

## Preface



## Chapter 1: Introducing Control Manager



## Chapter 2: Installation Planning

## Chapter 3: Installation



## Chapter 4: Upgrades and Migration

## Chapter 5: Post-installation Tasks



## Chapter 6: Removing Control Manager



## Chapter 7: Control Manager System Checklists

## Index

# Preface

## Preface

Welcome to the Trend Micro™ Control Manager™ *Installation and Upgrade Guide*. This document discusses requirements and procedures for installing the Control Manager server, and upgrading from a previous installation.

Topics in this section:

# Documentation

Control Manager documentation includes the following:

| DOCUMENT | DESCRIPTION |
|---|---|
| Readme file | Contains a list of known issues and may also contain late-breaking product information not found in the Online Help or printed documentation |
| Installation and Upgrade Guide | A PDF document that discusses requirements and procedures for installing the Control Manager<br><br>**Note**<br>The Installation and Upgrade Guide may not be available for minor release versions, service packs, or patches. |
| System Requirements | A PDF document that discusses requirements and procedures for installing Control Manager |
| Administrator's Guide | A PDF document that provides detailed instructions of how to configure and manage Control Manager and managed products, and explanations on Control Manager concepts and features |
| Online Help | HTML files compiled in WebHelp format that provide "how to's", usage advice, and field-specific information. The Help is also accessible from the Control Manager console |
| Connected Threat Defense Primer | A PDF document that explains how use Control Manager to bring together a host of Trend Micro products and solutions to help you detect, analyze, and respond to targeted attacks and advanced threats before they unleash lasting damage |
| Widget and Policy Management Guide | A PDF document that explains how to configure dashboard widgets and policy management settings in Control Manager |
| Data Protection Lists (Chapter 1 only) | A PDF document that lists predefined data identifiers and templates for Data Loss Prevention |

| DOCUMENT | DESCRIPTION |
|---|---|
| Knowledge Base | An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following website: http://esupport.trendmicro.com |

Download the latest version of the PDF documents and readme at:

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

# Audience

Control Manager documentation is intended for the following users:

- Control Manager Administrators: Responsible for Control Manager installation, configuration, and management. These users are expected to have advanced networking and server management knowledge.
- Managed Product Administrators: Users who manage Trend Micro products that integrate with Control Manager. These users are expected to have advanced networking and server management knowledge.

# Document Conventions

The documentation uses the following conventions.

**TABLE 1. Document Conventions**

| CONVENTION | DESCRIPTION |
|---|---|
| UPPER CASE | Acronyms, abbreviations, and names of certain commands and keys on the keyboard |
| **Bold** | Menus and menu commands, command buttons, tabs, and options |
| *Italics* | References to other documents |

| CONVENTION | DESCRIPTION |
|---|---|
| `Monospace` | Sample command lines, program code, web URLs, file names, and program output |
| **Navigation** > **Path** | The navigation path to reach a particular screen<br>For example, **File** > **Save** means, click **File** and then click **Save** on the interface |
|  **Note** | Configuration notes |
|  **Tip** | Recommendations or suggestions |
|  **Important** | Information regarding required or default configuration settings and product limitations |
|  **WARNING!** | Critical actions and configuration options |

# Terminology

The following table provides the official terminology used throughout the Control Manager documentation:

| TERMINOLOGY | DESCRIPTION |
|---|---|
| Administrator (or Control Manager administrator) | The person managing the Control Manager server |
| Agent | The managed product program installed on an endpoint |
| Components | Responsible for scanning, detecting, and taking actions against security risks |

| TERMINOLOGY | DESCRIPTION |
|---|---|
| Control Manager console, web console, or management console | The web-based user interface for accessing, configuring, and managing a Control Manager<br><br>**Note**<br>Consoles for integrated managed products are indicated by the managed product name. For example, the OfficeScan web console. |
| Managed endpoint | The endpoint where the managed product agent is installed |
| Managed product | A Trend Micro product that integrates with Control Manager |
| Managed server | The endpoint where the managed product is installed |
| Server | The endpoint where the Control Manager server is installed |
| Security risk | The collective term for virus/malware, spyware/grayware, and web threats |
| Product service | Control Manager services hosted through Microsoft Management Console (MMC). |
| Dual-stack | Entities that have both IPv4 and IPv6 addresses. |
| Pure IPv4 | An entity that only has an IPv4 address |
| Pure IPv6 | An entity that only has an IPv6 address |

# Chapter 1

# Introducing Control Manager

This section introduces Trend Micro™ Control Manager™ and provides an overview of its features and capabilities.

Topics include:

# About Control Manager

Trend Micro™ Control Manager™ is a web-based console that provides centralized management for 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 components, such as antivirus pattern files, scan engines, and antispam rules, throughout the network to ensure up-to-date protection. 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.

# Key Features and Benefits

Control Manager provides the following features and benefits.

| FEATURE | BENEFITS |
|---|---|
| Operation Center | Use the **Operation Center** tab to gain instant insights into the antivirus pattern and Data Loss Prevention compliance status, critical threat detections, as well as resolved and unresolved events on your network. |
| Dashboard | Use the **Dashboard** tabs and widgets for extensive visibility of managed product and Control Manager information about threat detections, component statuses, policy violations, and more. |
| User/Endpoint Directory | View detailed information about all the users and endpoints within the Control Manager network and any security threat detections. |

| FEATURE | BENEFITS |
|---|---|
| Product Directory | System administrators can immediately deploy configuration modifications to managed products or even run a manual scan from the Control Manager web console during a virus/malware outbreak. |
| Global Policy Management | System administrators can use policies to configure and deploy product settings to managed products and endpoints from a single management console to ensure consistent enforcement of your organization's virus/malware and content security policies. |
| Logs | Use a single management console to view consolidated logs from all registered managed products without having to log on to each individual product console. |
| Event Notifications | Keep administrators informed of network events at all times by configuring Control Manager to send notifications by email, Windows syslog, SNMP trap, or an in-house or industry-standard application used by your organization. |
| Reports | Create comprehensive reports from custom or static templates to obtain the actionable information you need to ensure network protection and security compliance. |
| Component Updates | Securely download and deploy antivirus patterns, antispam rules, scan engines, and other antivirus or content security components to help ensure that all managed products are up to date. |
| Connected Threat Defense | Control Manager brings together a host of Trend Micro products and solutions to help you detect, analyze, and respond to targeted attacks and advanced threats before they unleash lasting damage. |
| Secure communication infrastructure | Control Manager uses a communications infrastructure built on the Secure Socket Layer (SSL) protocol and can even encrypt messages with authentication. |
| Role-based Administration | Grant and control access to the Control Manager web console by assigning specific web console privileges to administrators and providing only the tools and permissions necessary to perform specific tasks. |

| FEATURE | BENEFITS |
|---|---|
| Command Tracking | Command Tracking allows you to continuously monitor whether commands executed using the Control Manager web console, such as antivirus pattern updates and component deployment, have successfully completed. |
| License management | Deploy new Activation Codes or reactivate existing Activation Codes on managed products. |
| Security Agent installation | Create and download Security Agent installation packages for OfficeScan or Trend Micro Security (for Mac) directly from the Control Manager console. |

# 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 describes the components that Control Manager uses.

| COMPONENT | DESCRIPTION |
|---|---|
| Control Manager server | Acts as a repository for all data collected from the agents. A Control Manager server includes the following features:<br>• An SQL database that stores managed product configurations and logs<br>Control Manager uses the Microsoft SQL Server database (`db_ControlManager.mdf`) to store data included in logs, managed product information, user account, network environment, and notification settings.<br>• A web server that hosts the Control Manager web console<br>• A mail client that delivers event notifications through email messages<br>Control Manager can send notifications to individuals or groups of recipients about events that occur on the Control Manager network. Send event notifications by email, SNMP trap, syslog, or any in-house/industry standard application used by your organization to send notifications.<br>• A report server that generates antivirus and content security product reports<br>A Control Manager report is an online collection of figures about security threat and content security events that occur on the Control Manager network. |
| Trend Micro Management Communication Protocol | MCP handles the Control Manager server interaction with managed products that support the next generation agent.<br>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. |
| Web Service Integration communication | An agent-less integration model that allows Control Manager to communicate with managed products |

| COMPONENT | DESCRIPTION |
|---|---|
| Web-based management console | Allows an administrator to manage Control Manager from virtually any computer with an Internet connection and web browser<br><br>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. |
| Widget Framework | Allows an administrator to create a customized dashboard to monitor the Control Manager network. |

# Smart Protection Network Participation

Trend Micro Smart Feedback continually gathers and analyzes threat information to help provide better protection. Your participation in Trend Micro Smart Feedback means that Trend Micro will gather information from your devices to help identify new threats. The information that Trend Micro collects from your devices is as follows:

- File checksums
- Web addresses accessed
- File information, including sizes and paths
- Names of executable files

**Tip**

You do not need to participate in Smart Feedback to protect your devices. Your participation is optional and you may opt out at any time. Trend Micro recommends that you participate in Smart Feedback to help provide better overall protection for all Trend Micro customers.

For more information on the Smart Protection Network, visit http://www.smartprotectionnetwork.com .

# Chapter 2

# Installation Planning

This chapter helps you plan for deployment and manage a Control Manager test deployment.

Topics include:

# 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 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.

## Understanding Single-Site Deployment

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

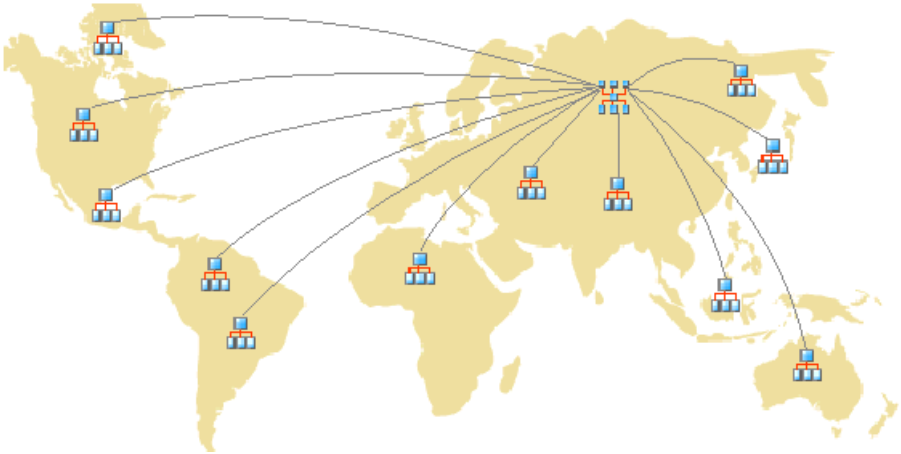


**FIGURE 2-1. A single-site deployment using a single Control Manager server**

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

1. Determine the number of managed products and endpoints
2. Plan for the optimal ratios of server, managed products and endpoints
3. Designate the Control Manager server

### Determining the Number of Managed Products and Endpoints

Determine how many managed products and endpoints 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 to Managed Products

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

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

### Designating Control Manager Servers

Based on the number of managed products and endpoints, 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 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 other servers and access the Control Manager web console using Internet Explorer over the Internet.

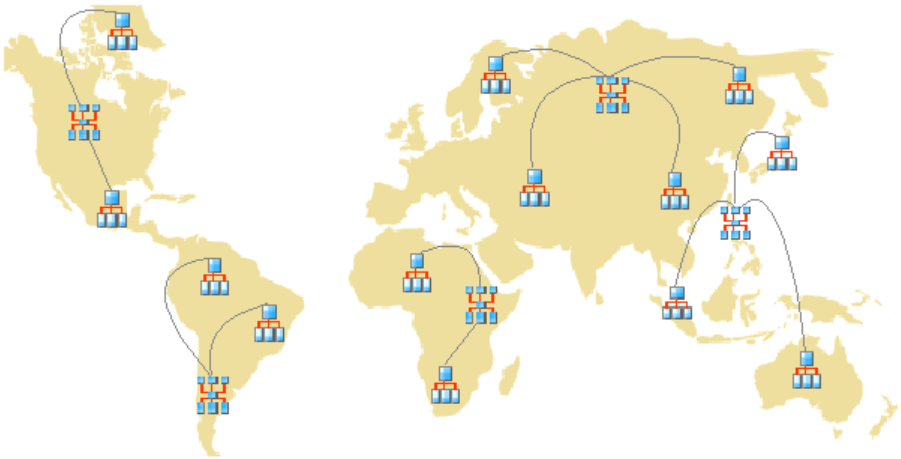


**FIGURE 2-2. A multi-site deployment using multiple Control Manager servers**

Consider the following for multi-site deployment:

- Group managed products, endpoints, or servers
- Determine the number of sites
- Determine the number of managed products, endpoints, and servers
- Plan for network traffic
- Decide where to install the Control Manager server

## Grouping Managed Products

Consider the following when you group managed products:

**TABLE 2-1. Considerations Grouping Managed Products**

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

## Determining the Number of Sites

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

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

## Determining the Number of Managed Products and Endpoints

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

When deploying Control Manager across a WAN, the Control Manager server in the main office administers managed products, endpoints, and other servers in remote offices. Managed products, endpoints, or servers in remote offices may require different network bandwidth when communicating with the Control Manager server over a WAN. Control Manager prioritizes communication with the managed products, endpoints, or servers with the faster connections.

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

## Designating Control Manager Servers

Based on the number of managed products and endpoints, 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 server management:

- **Central office**: A central office is the facility where the majority of the managed products, endpoints, and 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 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 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 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
- 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.

- Downloading and deploying updates
- Policy deployment
- Suspicious object synchronization

## 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 6.0) 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. 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 2-14*.

# 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
- 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

## 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 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 |
| 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. |
| Data Loss Prevention Log | Detections related to Data Loss Prevention policy violations |
| Behavior Monitoring Log | Behavior-based malicious activity detections |
| Network Inspection Log | Includes IP address or domain detections |
| Predictive Machine Learning Log | Predictive Machine Learning detections |

| Log | Contains Information About |
|---|---|
| Virtual Analyzer Log | Detections reported by Virtual Analyzer for suspicious sample submissions |
| File Hash Detection Log | Detections triggered by **File** or **File SHA-1** suspicious objects |

## Trend Micro Management Communication Protocol Policies

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

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

## Product Registration Traffic

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

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

- Category (for example, antivirus)
- Product name

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

By default, Control Manager servers contain all the product profiles for managed products that use Web Services Integration communication. Managed products that use the Trend Micro Management Communication Protocol (MCP) upload product profiles during initial registration with 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 24 hours.

- 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.

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

    **Note**

    The minimum memory requirement to install Control Manager is 4GB, and the recommended requirement is 8GB. 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 agents 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 Driver

Control Manager installs Open Database Connectivity (ODBC) Driver 13 for SQL Server to support Microsoft SQL Server communications and Transport Layer Security (TLS) 1.2.

## Authentication

Control Manager supports both SQL database authentication and 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

# Installation

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.

Topics include:

# System Requirements

Control Manager 7.0 requires specific Windows features and hotfixes in order to run the installation program.

- For a complete list of system requirements for a fresh installation, go to http://docs.trendmicro.com/en-us/enterprise/control-manager.aspx.
- For detailed managed product and Security Agent system requirements, see the managed product documentation.

The following table lists the minimum requirements for running the Control Manager installation program.

**Note**

- The following Windows hotfixes are not automatically installed by Windows Updates but are required for the respective operating systems prior to Control Manager installation:
  - KB2999226
  - KB2919355
  - KB2919442
- The following Windows hotfixes are only required for the respective operating systems to support TLS 1.2:
  - KB2973337
  - KB2975331
  - KB3000850

<table>
<tr><th rowspan="2">Operating System</th><th rowspan="2">Edition</th><th rowspan="2">Service Pack</th><th colspan="3">System Requirements</th></tr>
<tr><th colspan="2">Windows Features</th><th>Windows Hotfixes</th></tr>
<tr><td>Windows Server 2008 (32-bit/64-bit)</td><td rowspan="2">Standard<br>Enterprise<br>Datacenter</td><td>SP2</td><td rowspan="4">.NET Framework 4.6.1 or above<br>Microsoft Message Queuing Service (MSMQ)<br>Microsoft IIS ASP<br>Microsoft IIS CGI<br>IIS Windows Authentication<br>IIS 6 Management Compatibility</td><td rowspan="2">ASP.NET<br>.NET Extensibility</td><td>N/A</td></tr>
<tr><td>Windows Server 2008 R2 (64-bit)</td><td>SP1</td><td>KB2973337</td></tr>
<tr><td>Windows Server 2012 (64-bit)</td><td rowspan="3">Standard<br>Datacenter</td><td rowspan="3">N/A</td><td>ASP.NET 4.5<br>.NET Extensibility 4.5</td><td>KB2999226<br>KB2975331</td></tr>
<tr><td>Windows Server 2012 R2 (64-bit)</td><td rowspan="2">ASP.NET 4.5<br>.NET Extensibility 4.5</td><td>KB2919355<br>KB2919442<br>KB3000850</td></tr>
<tr><td>Windows Server 2016 (64-bit)</td><td>ASP.NET 4.6<br>.NET Extensibility 4.6</td><td>N/A</td></tr>
</table>

# 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 7-2* 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
- Prepare the following information about the SQL database for Control Manager:
  - User name for the database
  - Password

  **Note**

  Control Manager allows you to use Windows authentication or 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 2016 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 7.0 instead of doing a fresh installation.

## Installing All Required Components

**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, go to the relevant folder on your computer.
2. The installation program checks your system for required components.

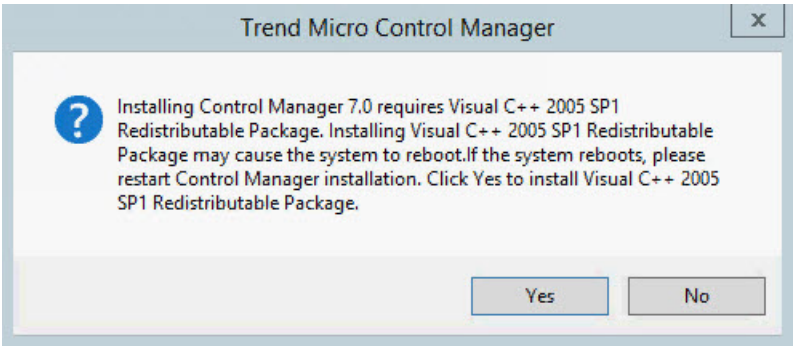
   If the installation program does not detect the following components on the server, dialog boxes appear prompting you to install the missing component.

| COMPONENT | DESCRIPTION |
|---|---|
| Visual C++ 2005 SP1 Redistributable Package | Included in the Control Manager installation package |
| Visual C++ 2008 SP1 Redistributable Package | Included in the Control Manager installation package |

| COMPONENT | DESCRIPTION |
|---|---|
| Visual C++ 2012 Update 4 Redistributable Package | Included in the Control Manager installation package |
| Visual C++ 2015 Redistributable Package | Included in the Control Manager installation package |
| PHP 7.1 | Included in the Control Manager installation package<br><br>**Important**<br>If the server uses a previous version of PHP version, remove the previous version before starting Control Manager installation. Control Manager then installs PHP 7.1 during the installation process. |

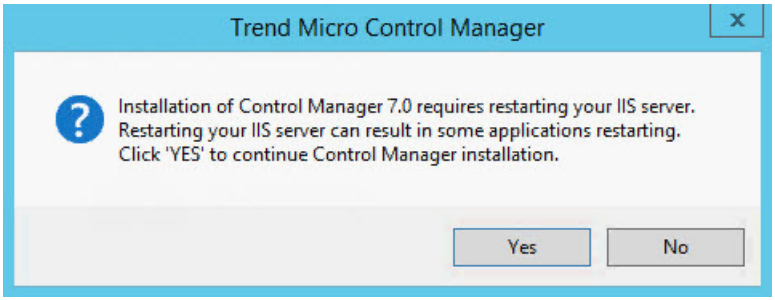
3. Install all missing components.

   A confirmation dialog box appears.




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

Another confirmation dialog box appears.




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

   The **Welcome** screen appears.

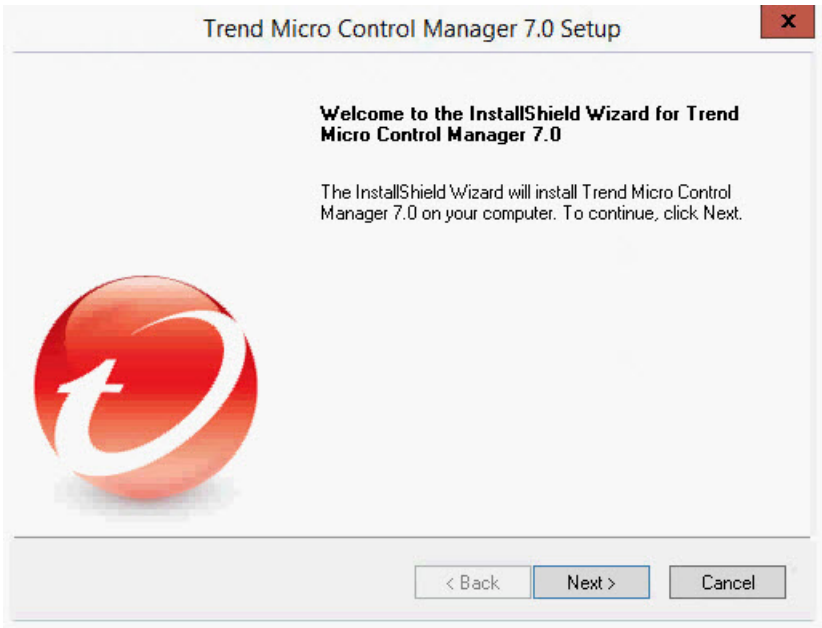



**FIGURE 3-1. The Welcome screen**

The installation program checks your system for existing components. Before proceeding with the installation, close all instances of the **Microsoft Management Console**.

6. Click **Next**.

   The **Software License Agreement** screen appears.

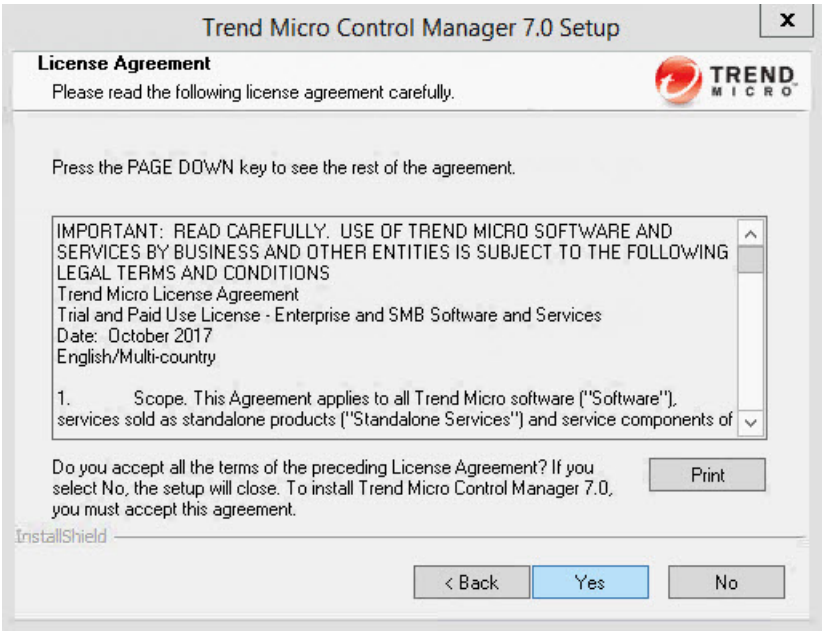



**FIGURE 3-2. Agree with the License Agreement**

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

8. If you install Control Manager on Windows 2008 R2 (or earlier), a summary of detected components appears.

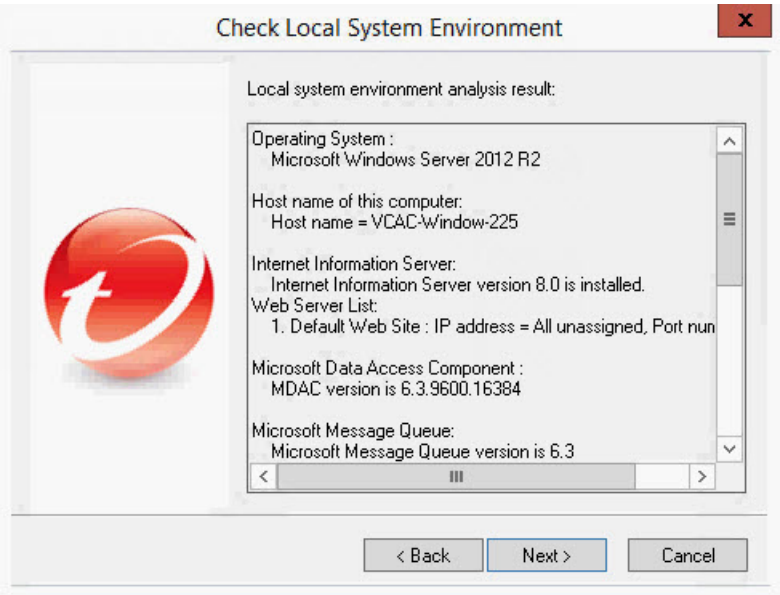



**FIGURE 3-3. Displays local system environment information**

9. Click **Next**.

   The installation checks your system for an existing SQL server.

   If you do not have an existing SQL, a dialog box prompts you to install Microsoft SQL Server 2016 Express SP1.

## 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.

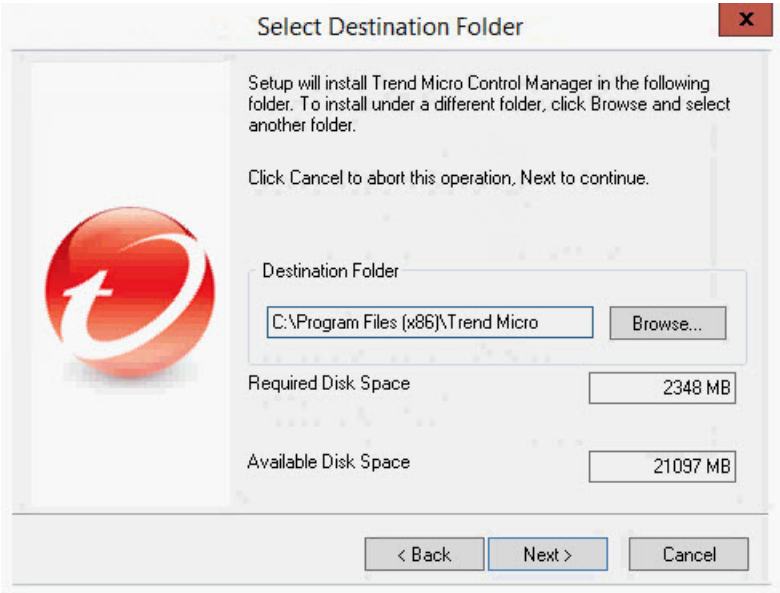



**FIGURE 3-4. Select a destination folder**

2. Specify a location for Control Manager files. Click **Browse** to specify an alternate location.

**Note**

- The default location on 64-bit operating systems is `C:\Program Files (x86)\Trend Micro`.
- The setup program installs files related to Control Manager communication (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.

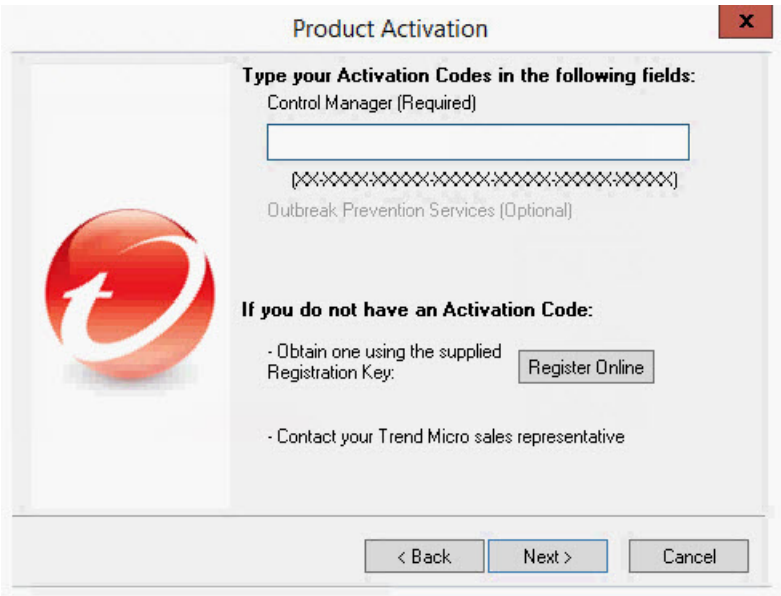



**FIGURE 3-5. Provide the Activation Code to activate Control Manager and services**

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, 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.

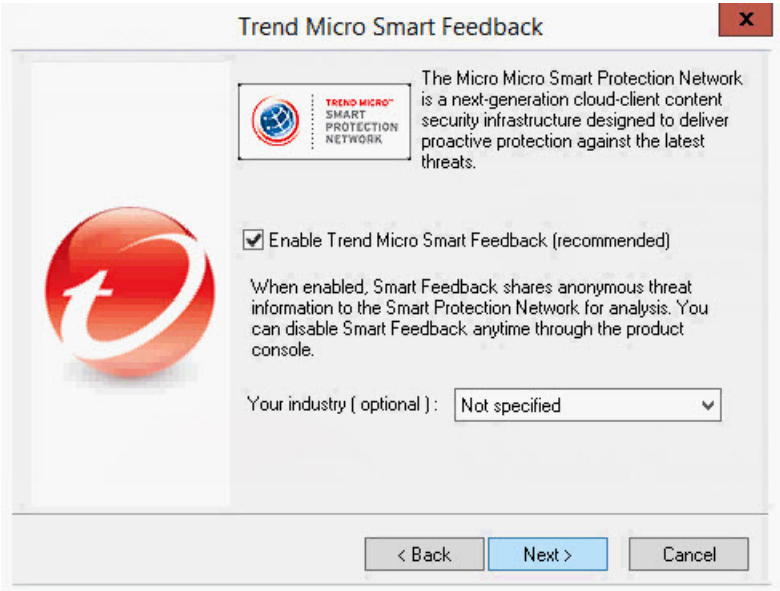



**FIGURE 3-6. Smart Protection Network settings**

4. Select **Enable Trend Micro Smart Feedback (recommended)** 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.

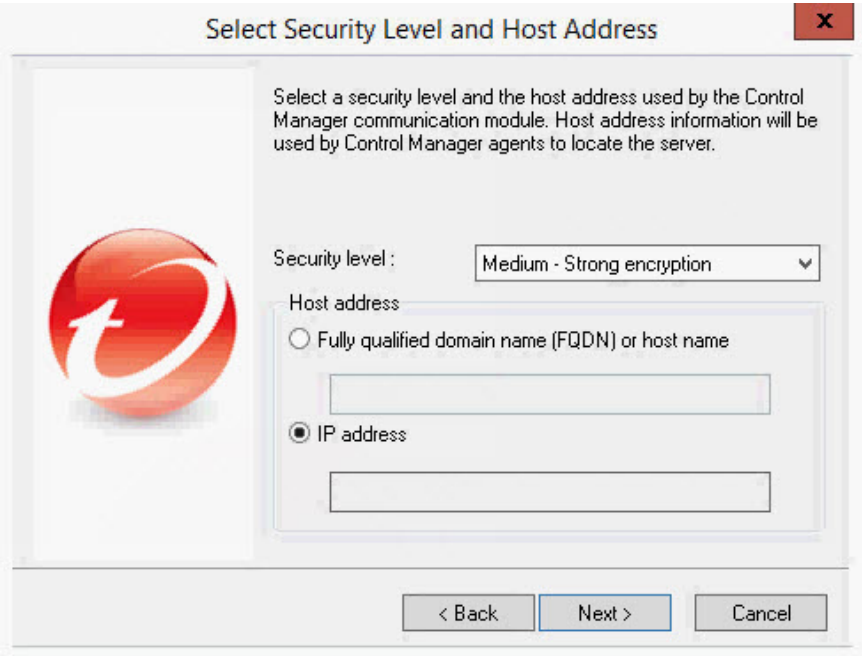



**FIGURE 3-7. Select a security level**

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.

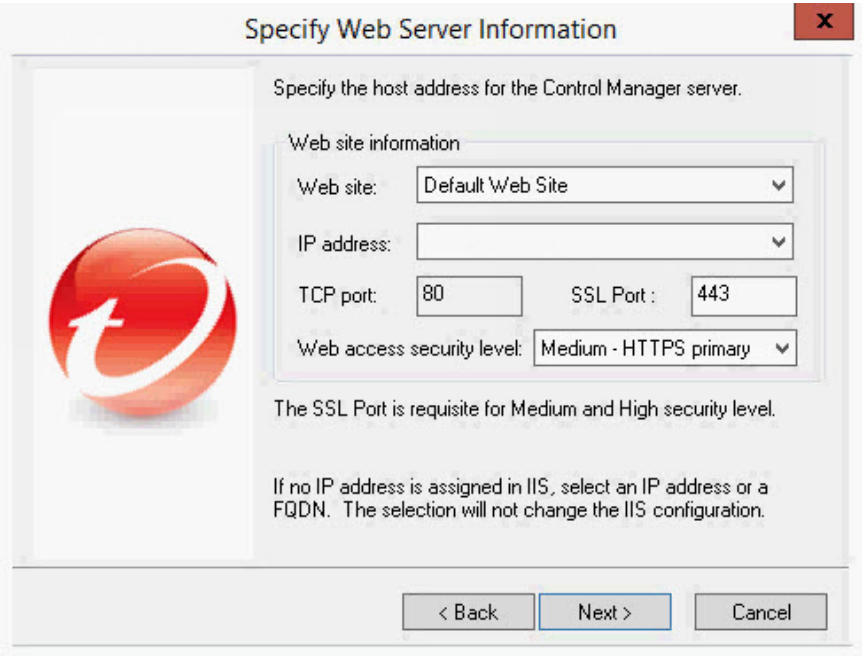



**FIGURE 3-8. Specify web server information**

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 one of the following security security levels for Control Manager communication:

   - **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.

   **Note**

   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.

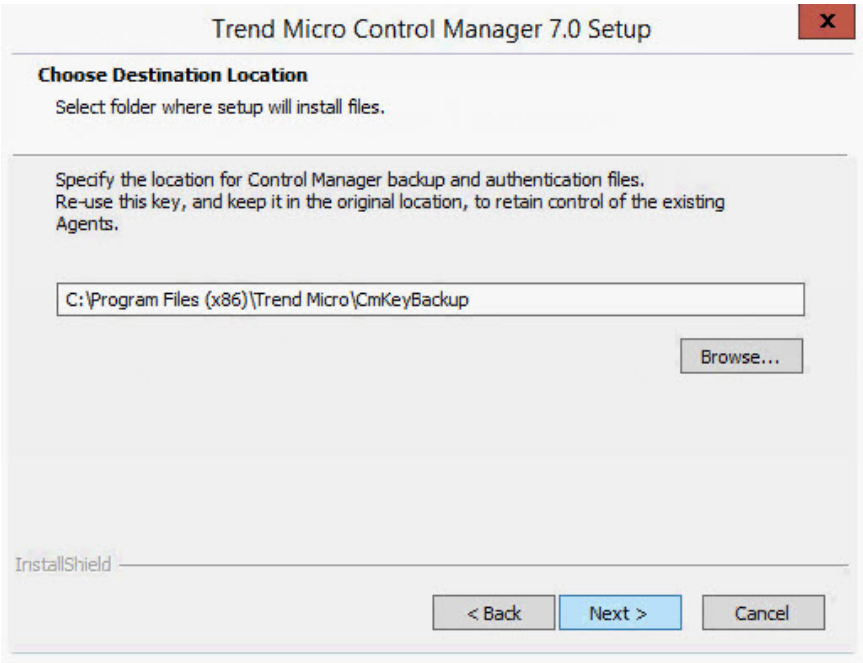



**FIGURE 3-9. Choose a destination location for backup and authentication files**

2. Specify the location of the Control Manager backup and authentication files. Click **Browse** to specify an alternate location.

**Note**

The default location on 64-bit operating systems is `C:\Program Files (x86)\Trend Micro\CmKeyBackup`.

For more information, see *Control Manager Files to Back Up on page 4-2*.

## Configuring Notification Settings

**Procedure**

1. Click **Next**.

   The **Specify Message Routing Path** screen appears.

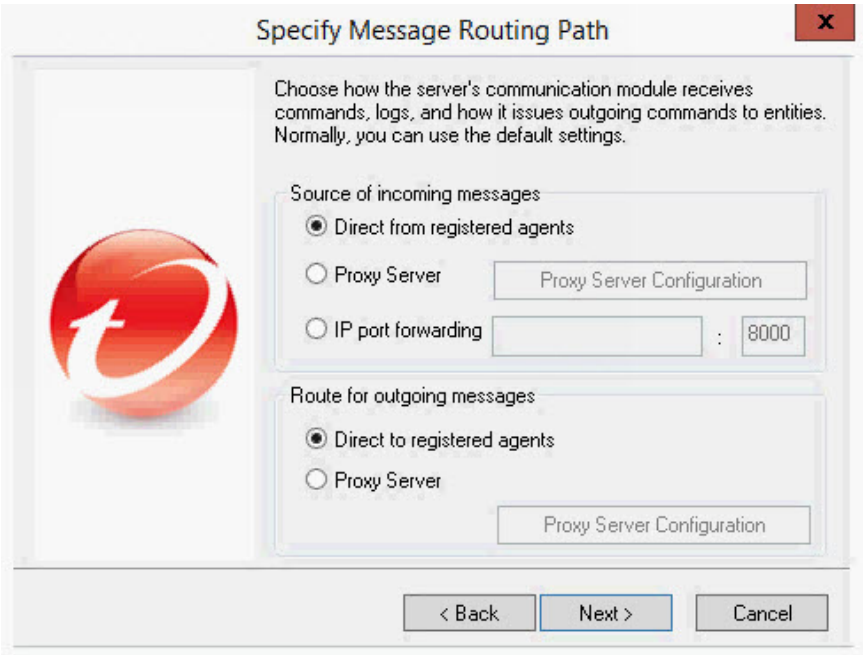



**FIGURE 3-10. Define routes for messages or requests**

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

**Procedure**

1. Click **Next**.

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

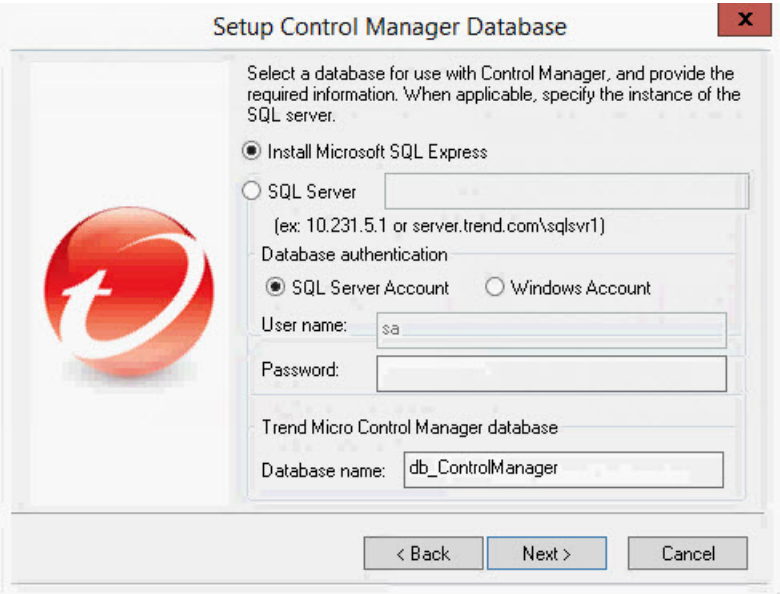



**FIGURE 3-11. Choose the Control Manager database**

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.

**Note**

If your operating system is not Windows Server 2012 (x64) or above, this option is unavailable.

**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" user right
     - 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 7.0, 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 the Root Account

**Procedure**

1. Click **Next**.

The **Create Root Account** screen appears.

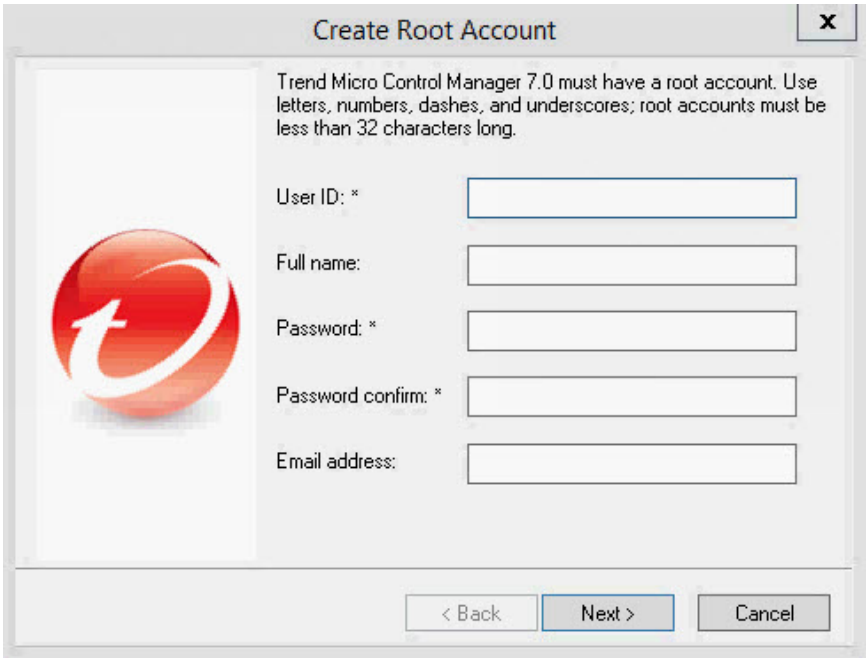



**FIGURE 3-12. Provide information for the Control Manager root account**

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

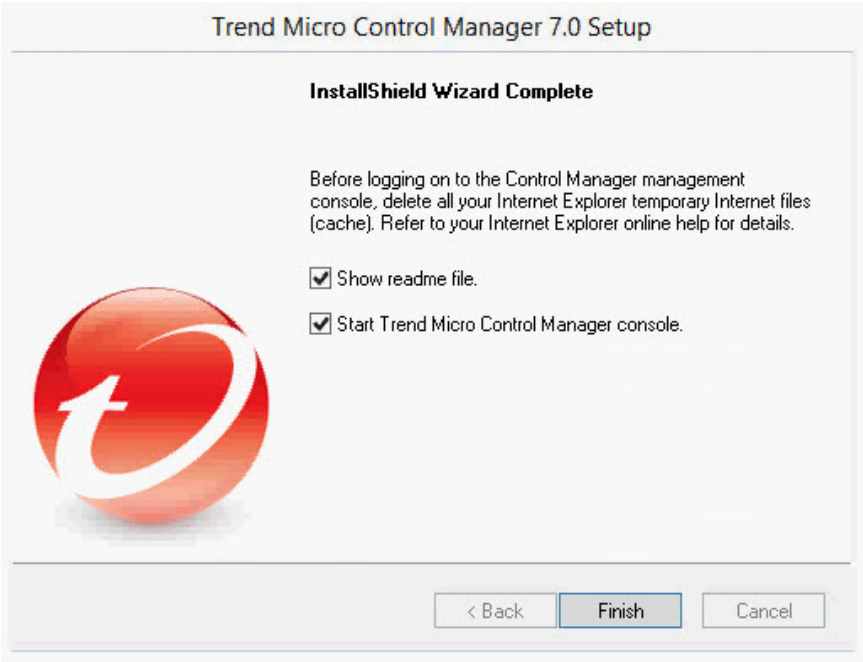



**FIGURE 3-13. Setup complete**

# Chapter 4

# Upgrades and Migration

This chapter discusses how to upgrade or migrate to Control Manager 7.0 from a previous version of Control Manager.

Topics include:

# Upgrading to Control Manager 7.0

Migrating a Control Manager 6.0 installation to Control Manager 7.0 preserves all your previous settings, logs, reports, Product Directory structure, and integrated Active Directory structure.

**Important**

- You can only migrate to Control Manager 7.0 from a Control Manager 6.0 installation.
- Before migrating to Control Manager 7.0, ensure that your server has sufficient system resources.

  For more information, see the *Control Manager 7.0 System Requirements*.

## Supported Versions for Upgrade

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

- Control Manager 6.0
- Control Manager 6.0 Service Pack 1
- Control Manager 6.0 Service Pack 2
- Control Manager 6.0 Service Pack 3

**WARNING!**

Always back up the existing server before performing the upgrade.

## Control Manager Files to Back Up

Before performing an upgrade, create a backup of the following Control Manager files:

**TABLE 4-1. Control Manager files that should be backed up**

| CONTROL MANAGER 6.0 INFORMATION | LOCATION |
|---|---|
| Database | Use the SQL Server Management Studio or osql to back up the Control Manager database. Refer to the Control Manager backup db_ControlManager using SQL Server Management Studio / osql online help topics for detailed steps. |
| Authentication information | `\Program Files (x86)\Trend Micro\CmKeyBackup\*.*`<br>(Ensures that managed products reporting to the Control Manager server will report to the same server if Control Manager is restored) |
| ActiveUpdate files | `\Program Files (x86)\Trend Micro\Control Manager\webui\download\Activeupdate` |
| Control Manager registry | For 32-bit operating systems:<br>`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\TVCS\`<br>`HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\CommonCGI`<br>`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TMCM`<br>`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer`<br>`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMCM` |

| CONTROL MANAGER 6.0 INFORMATION | LOCATION |
|---|---|
| Control Manager registry | For 64-bit operating systems:<br>HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\TVCS<br>HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\CommonCGI<br>HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\TMCM<br>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer<br>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMCM |
| Control Manager registry | HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TrendMicro_NTP<br>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSSQL$SQLEXPRESS |

# Upgrade and Migration Scenarios

Control Manager supports the following migration scenarios.

- *Scenario 1: Upgrading a Control Manager 6.0 Server to Control Manager 7.0 on page 4-4*
- *Scenario 2: Migrating to a Fresh Control Manager 7.0 Installation Using the Agent Migration Tool on page 4-6*

## Scenario 1: Upgrading a Control Manager 6.0 Server to Control Manager 7.0

When upgrading Control Manager 6.0 directly to Control Manager 7.0, 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 6.0 database.
2. Back up all the files under `\Trend Micro\CmKeyBackup\*.*`.
3. Back up all folders of the current Control Manager 6.0 server.
4. Back up the registries of the current Control Manager 6.0 server.
5. Install Control Manager 7.0 over Control Manager 6.0.

## 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 6.0 server.
2. Back up the existing Control Manager 6.0 database.
3. Install Control Manager 7.0 over Control Manager 6.0.

## Upgrade Flow

To upgrade Control Manager 6.0 to Control Manager 7.0, run the installation program (`Setup.exe`) as described in step 1 of *Installing All Required Components on page 3-5*.

## Scenario 2: Migrating to a Fresh Control Manager 7.0 Installation Using the Agent Migration Tool

This scenario involves installing Control Manager 7.0 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 4-8* for more information about migrating agents.

### Migrating a Control Manager 6.0 Server to a Fresh Installation of Control Manager 7.0

**Procedure**

1. Back up the existing Control Manager 6.0 database.
2. Perform a fresh installation of Control Manager 7.0 on a different computer.
3. Use the Agent Migration Tool to migrate entities from the Control Manager 6.0 server to the Control Manager 7.0 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.

# Rolling Back to Control Manager 6.0 Servers

If upgrading to Control Manager 7.0 is unsuccessful, perform the following steps to roll back to your Control Manager 6.0 system.

## Rolling Back a Control Manager 7.0 Server to Control Manager 6.0

Use one of the following methods to roll back the Control Manager 6.0 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 7.0 server.
2. Install the Control Manager 6.0 server.
3. Apply the required Control Manager 6.0 service packs and hot fixes.

**WARNING!**

Apply only the service packs and hot fixes that the original Control Manager 6.0 server had installed.

4. Restore the Control Manager 6.0 database with the backup database.
5. Restore all the Control Manager 6.0 folders with the backed up folders.
6. Restore Control Manager 6.0 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 6.0 database with the backup database.

2. Restore the operating system of the server with the backed up operating system.

# Planning Control Manager Agent Migration

There are two ways to migrate agents to a Control Manager 7.0 server:

- Rapid upgrade
- Phased upgrade

## Rapid Upgrade

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

**TABLE 4-2. Rapid Upgrade**

| ORIGINAL SERVER/ AGENT | ACTION |
|---|---|
| Control Manager 6.0 with MCP agents | Register MCP agents to the Control Manager 7.0 server and then re-organize the Product Directory structure |
| Control Manager 6.0 with mixed agents | Register MCP agents to the Control Manager 7.0 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 2-9*). 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 6.0 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 7.0 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 7.0 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.

# Migrating the Control Manager Database

To migrate a Control Manager 6.0 database, install Control Manager 7.0 on a Control Manager 6.0 server. This is the recommended method.

The Control Manager 7.0 setup program automatically upgrades the database to version 7.0.

## 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 Database Configuration Tool (DBConfig.exe)

The `DBConfig.exe` 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 authentication mode (SQL Server Authentication or Windows Authentication)

**Note**

The default database authentication mode is SQL Server Authentication mode. However, Windows Authentication mode is necessary when configuring for Windows authentication.

**Procedure**

1. Open a command prompt on the Control Manager server.
2. Use the following command to locate the directory which contains the `DBConfig.exe` file:

   **`cd <Control Manager installation directory>\DBConfig`**

3. Type `dbconfig` and press `ENTER`.

   The DBConfig tool interface appears.

4. 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

# Post-installation Tasks

This chapter discusses the tasks Trend Micro recommends performing after the Control Manager installation completes.

Topics include:

# Automatic Post-installation Tasks

Control Manager automatically performs the following tasks after the installation completes successfully.

- Remove unused patterns and engines
- Migrate previously configured Active Directory server settings
- Synchronize Active Directory server data

# Verifying the Server Installation or Upgrade

After completing the installation or upgrade, verify the following items:

| ITEM | DESCRIPTION |
|---|---|
| Programs list | The following programs appear on the **Add/Remove Programs** list (**Control Panel** > **Add/Remove Programs**) on the server computer.<br>• Trend Micro Control Manager<br>• Microsoft Visual C++ 2005, 2008, 2012, 2015 Redistributable<br>• Microsoft Report Viewer 2012 Runtime<br>• Microsoft SQL Server 2016<br>• Microsoft SQL Server 2016 Native Client<br>• Microsoft SQL Server 2016 Setup<br>• Microsoft SQL Server 2016 Setup Support Files<br>• Microsoft SQL Server Browser<br>• Microsoft SQL Server VSS Writer |

| ITEM | DESCRIPTION |
|---|---|
| Directory folders | The following folders appear in the `C:\Program Files (x86)` directory on the server computer:<br>• `Trend Micro\CmKeyBackup`<br>• `Trend Micro\COMMON\TMI`<br>• `Trend Micro\Control Manager` |
| Control Manager Database files | • `db_ControlManager.mdf`<br>• `db_ControlManager_Log.LDF` |
| The setup program creates the following services and processes: | |
| Control Manager services | • Trend Micro Control Manager<br>• Trend Micro Management Infrastructure |
| IIS process | • `w3wp.exe` (Internet Information Services) |
| ISAPI filters | • ReverseProxy<br>• TmcmRedirect |
| Control Manager processes | • `CasProcessor.exe`<br>• `CmdProcessor.exe`<br>• `CmdProcessor.NET.exe`<br>• `LogReceiver.exe`<br>• `LogRetriever.exe`<br>• `MsgReceiver.exe`<br>• `ProcessManager.exe`<br>• `ReportServer.exe`<br>• `sCloudProcessor.NET.exe` |
| Message Queue process | `LogProcessor.exe` |

# 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.

## Control Manager Activation and License Information

Activating Control Manager allows you to use all of the product features, including downloading updated program components.

### Activating Control Manager

You can activate Control Manager after obtaining an Activation Code from your Trend Micro sales representative or reseller.

---

**Procedure**

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

   The **License Information** screen appears and displays the current license information.

2. Click **View license information online**.

   The Trend Micro Customer Licensing Portal **Sign In** screens appears.

3. Sign in to the Customer Licensing Portal using your Trend Micro account and password.
4. Click the **My Products/Services** menu tab.
5. Click **Provide Key**.

   The **License Key** screen appears.
6. Type your Activation Code.
7. Click **Continue**.

   The **My Products/Services** screen appears and displays the updated license information.

### 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.

## Configuring Active Directory Connection Settings

Specify the connection settings to allow Control Manager to synchronize endpoint and user information from Active Directory servers.

**Note**

Control Manager supports synchronization with multiple Active Directory forests. Adding an Active Directory domain automatically synchronizes all domains from the same forest.

For more information about forest trusts, contact your Active Directory administrator.

### Procedure

1. Go to **Administration** > **Settings** > **Active Directory and Compliance Settings**.
2. Click the **Active Directory Settings** tab.
3. Select **Enable Active Directory synchronization and authentication**.
4. Configure the connection settings to access an Active Directory server.

| FIELD | DESCRIPTION |
|---|---|
| Server address | Type the FQDN or IP address (IPv4 or IPv6) of the Active Directory server. |
| User name | Type the domain name and user name required to access the Active Directory server.<br>Example format, `domain\user_name` |
| Password | Type the password required to access the Active Directory server. |

**Note**

- To add another Active Directory server, click the add icon ( + ).
- To delete an Active Directory server, click the delete icon ( – ).

5. From the **Synchronize every** drop-down list, select how often Control Manager synchronizes data with Active Directory servers.

**Note**

Active Directory synchronization times vary based on the size and complexity of the Active Directory database. You may need to wait for more than an hour before synchronization completes.

6. (Optional) Click **Test Connection** to test the server connection.

**Note**

Testing the connection does not save the Active Directory server settings.

The Active Directory server connection status icon ( or ) appears in front of the server address.

7. Click **Save**.

After configuring and saving Active Directory server connection settings, you can perform the following tasks:

- Click **Synchronize Now** to manually synchronize data with Active Directory servers.

  The Active Directory server connection status icon ( or ) appears in front of the server address.

- Click **Clear Data** to manually clear data for removed Active Directory servers from the Control Manager database.

**Note**

Clicking **Clear Data** triggers a scheduled task, which runs every 2 minutes, to purge all data from removed Active Directory servers.

# 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 more advanced functions, 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**).

## Configuring Event 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, go to **Notifications and Reports** > **Event Notifications**).

# Chapter 6

# Removing 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.

Topics include:

# Removing a Control Manager Server

You have two ways to remove Control Manager automatically (the following instructions apply to a Windows Server 2008 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. Click **Trend Micro Control Manager** and select **Uninstall**.

  A confirmation dialog appears.

  c. Click **Yes** to uninstall Control Manager.

  **WARNING!**

  This action automatically removes related services as well as the Control Manager database.

  d. 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 2008.

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
- Common CGI Modules
- Control Manager Database (optional)
- PHP
- FastCGI

Other Trend Micro products also use the 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:

1. *Stopping Control Manager Services on page 6-4*
2. *Removing Control Manager IIS Settings on page 6-5*
3. *Removing Crystal Reports, PHP, and FastCGI on page 6-7*
4. *Deleting Control Manager Files/Directories and Registry Keys on page 6-8*
5. *Removing the Database Components on page 6-9*
6. *Removing Control Manager and NTP Services on page 6-10*

## Stopping Control Manager Services

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

- 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
```

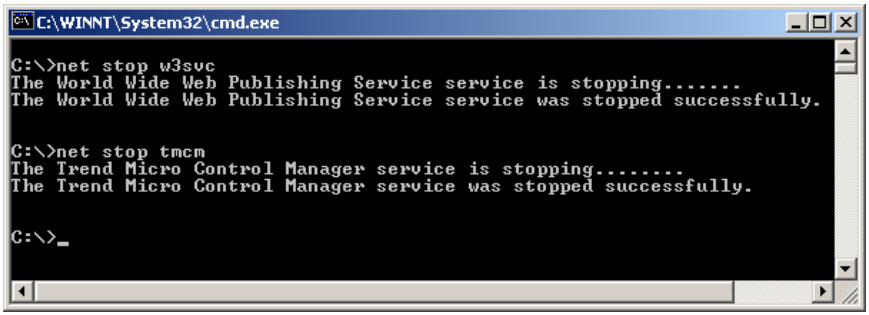



**FIGURE 6-1. View of the command line with the necessary services stopped**

## Removing Control Manager IIS Settings

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

**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, and FastCGI

Removal of Crystal Reports, PHP, and FastCGI 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 CCGI

**Procedure**

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

```
sc delete "TrendCGI"
```

## Deleting Control Manager Files/Directories and Registry Keys

**Procedure**

1. Delete the following directories:

   - `.Trend Micro\Control Manager`
   - `.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\TVCS`
   - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\VulnerabilityAssessmentServices`
   - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\TMCM`
   - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMCM`

- `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"
```

# Chapter 7

# Control Manager System Checklists

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

Topics include:

# 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 7-1. Server Address Checklist**

| INFORMATION REQUIRED | EXAMPLE | 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 | EXAMPLE | 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 | |
| Syslog server information (Optional; for syslog notifications) | | |
| IP address | 10.1.194.225 | |
| Server port | 514 | |

# Port Checklist

Control Manager uses the following ports for the indicated purposes.

| PORT | SAMPLE | YOUR VALUE |
|---|---|---|
| SMTP | 25 | |
| Proxy | 8088 | |
| Web Console and Update/ Deploy components | 80 | |
| Firewall, "forwarding" port (Optional; used during the Control Manager Agent installation) | 224 | |

# 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 Processes 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 7-2. 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 |

| CONFIGURATION FILE | DESCRIPTION |
|---|---|
| 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 |
| DMRegisterinfo.xml | Used by CasProcessor.exe |
| DataSource.xml | Stores the connection parameters for Control Manager processes |
| SystemConfiguration.xml | Control Manager system configuration file |
| agent.ini | MCP agent file |

**TABLE 7-3. 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 |
| LogReceiver.exe | Receives managed product logs and messages. Starting with Control Manager 3.0 Service Pack 4, LogReceiver.exe only handles logs coming from Trend Micro Damage Control Services and Trend Micro Vulnerability Assessment |
| LogProcessor.exe | Receives logs from managed products, and receives entity information from managed products |
| LogRetriever.exe | Retrieves and saves logs in the Control Manager database |

| PROCESSES | DESCRIPTION |
|---|---|
| ReportServer.exe | Generates Control Manager reports |
| MsgReceiver.exe | Receives messages from the Control Manager server and managed products |
| CasProcessor.exe | Allows a Control Manager server to manage other Control Manager servers |
| inetinfo.exe | Microsoft Internet Information Service process |
| cm.exe | Manages dmserver.exe and mrf.exe |
| dmserver.exe | Provides the Control Manager web console log on page and manages the Product Directory (Control Manager-side) |
| sCloudProcessor.NET.exe | Requests the Control Manager web console or other processes to provide a job ID for the issuer to query statuses, query results, and cancel requests; used by the User/Endpoint Directory |

# Communication and Listening Ports

These are the default Control Manager communication and listening ports.

| SERVICE | SERVICE PORT |
|---|---|
| ProcessManager.exe | 20501 |
| CmdProcessor.exe | 20101 |
| comdProcessor.NET.exe | 21003 |
| LogReceiver.exe | 20201 |
| LogProcessor.exe | 21001 |
| LogRetriever.exe | 20301 |
| ReportServer.exe | 20601 |

| SERVICE | SERVICE PORT |
|---|---|
| MsgReceiver.exe | 20001 |
| CasProcessor.exe | 20801 |
| sCloudProcessor.NET.exe | 21002 |

# Index

## T



## U



## V



## W


**TREND MICRO INCORPORATED**

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: CMEM77943/170818