TREND MICRO™

5.0

TREND MICRO™ Endpoint Encryption

Installation & Migration Guide

Comprehensive Endpoint Encryption for Data at Rest

Endpoint Security

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, please review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

http://docs.trendmicro.com/en-us/enterprise/endpoint-encryption.aspx

Trend Micro, the Trend Micro t-ball logo, OfficeScan, and Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2015. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM56168_130917

Release Date: July 2015

Protected by U.S. Patent No.: Patents pending.

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 in the Trend Micro Online Help and/or the Trend Micro Knowledge Base at the Trend Micro website.

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

Evaluate this documentation on the following site:

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

Table of Contents

Preface

Preface ix

Document Set x

Intended Audience x

Document Conventions xi

About Trend Micro xii

Chapter 1: Introducing Endpoint Encryption

About Endpoint Encryption 1-2

Key Features and Benefits 1-2

What's New in Version 5.0 Patch 3 1-3

About Encryption 1-10
- About FIPS 1-10

Endpoint Encryption Components 1-11
- About PolicyServer 1-14
- Management Consoles 1-16
- Endpoint Encryption Agents 1-18

Endpoint Encryption Devices 1-20

Endpoint Encryption Users 1-21
- Endpoint Encryption User Roles 1-21

Chapter 2: System Requirements

PolicyServer Requirements 2-2
- PolicyServer System Requirements 2-2
- Database Considerations 2-4
- Required Installation Files 2-5
- Required Accounts 2-5

Management Consoles 2-6
PolicyServer MMC System Requirements 2-6
Control Manager System Requirements 2-7
OfficeScan System Requirements 2-7

Agents 2-9
Full Disk Encryption System Requirements 2-9
Encryption Management for Microsoft BitLocker System Requirements 2-11
Encryption Management for Apple FileVault System Requirements 2-12
File Encryption System Requirements 2-13

Chapter 3: Deployment and Upgrade Overview

Deployment Planning 3-2

Predeployment Checklist 3-2

Deployment Summary of Operations 3-4

Management Options 3-5
Managing Endpoint Encryption with PolicyServer MMC Only 3-6
Control Manager and OfficeScan Integration 3-6

Deployment Options 3-11
Simple Deployment 3-12
Control Manager Deployment 3-13
OfficeScan Deployment 3-14
Complex Distributed Deployment 3-15

Scaling Recommendations 3-17

Upgrade Deployments 3-21
Upgrade Considerations 3-22
Upgrade Paths 3-23
Supported Agent Versions 3-25
Upgrade Summary of Operations 3-26

Chapter 4: PolicyServer Deployment

About PolicyServer 4-2

PolicyServer Installation and Configuration 4-3
Installing PolicyServer 4-3
Configuring PolicyServer 4-7
PolicyServer Active Directory Synchronization 4-16
Configure Services on Multiple Endpoints 4-20

Upgrade 4-23
Upgrade Paths 4-23
Supported Agent Versions 4-25
Upgrading PolicyServer 4-27
Upgrading Multiple PolicyServer Services Connected to the Same Database 4-30
Upgrading PolicyServer MMC 4-30

Migration to Control Manager 4-31

Uninstallation 4-31
Uninstalling the PolicyServer MMC 4-31
Uninstalling PolicyServer 4-32

Chapter 5: Control Manager Integration

About Control Manager Integration 5-2

Migrating to Control Manager 5-3

Adding PolicyServer as a Managed Product to Control Manager 5-4

Configuring Groups for Control Manager Policies 5-7

Creating a Policy 5-8
Specifying Policy Targets 5-9

Changing a PolicyServer Managed Product in Control Manager 5-11

Removing a PolicyServer Managed Product from Control Manager ... 5-11

Chapter 6: Endpoint Encryption Agent Deployment

Endpoint Encryption Agents 6-2

About Full Disk Encryption 6-3

About File Encryption 6-4

Installation 6-4
Before Installing Endpoint Encryption Agents 6-4
Requirements for Managed Endpoints 6-5
Automating Agent Deployment 6-6
Full Disk Encryption Deployment 6-6
File Encryption Deployment 6-28
Automated Deployments 6-33

Upgrade 6-46
Upgrading the Endpoint to Windows 8 6-46
Upgrading Full Disk Encryption 6-47
Upgrading File Encryption 6-49
Upgrading Encryption Management for Apple FileVault 6-50
Upgrading Encryption Management for Microsoft BitLocker 6-50

Migration 6-51
Replacing a Previously Installed Encryption Product 6-51
Full Disk Encryption PolicyServer Settings 6-52
Migrating Full Disk Encryption to a New Enterprise 6-54
Migrating Endpoints to a New PolicyServer 6-56

Uninstallation 6-59
Manually Uninstalling Endpoint Encryption Agents 6-59
Using OfficeScan to Uninstall Endpoint Encryption Agents 6-64

Chapter 7: OfficeScan Integration

About Trend Micro OfficeScan Integration 7-2

Installing OfficeScan 7-3

About Plug-in Manager 7-4

Endpoint Encryption Deployment Tool Installation 7-5
Installing Endpoint Encryption Deployment Tool 7-5

Plug-in Program Management 7-6
Managing Endpoint Encryption Deployment Tool 7-7

Using Plug-in Programs 7-7
Plug-in Program Management 7-7
Endpoint Encryption Deployment Tool Upgrades 7-8
Endpoint Encryption Deployment Tool Uninstallation 7-9

Managing the Agent Tree 7-9
The OfficeScan Agent Tree 7-10
Agent Tree Specific Tasks 7-10
Deploying Server Settings 7-11

Endpoint Encryption Agent Deployment 7-12
Deploying the Agent with OfficeScan 7-12
Confirming Agent Deployment 7-13
Endpoint Encryption Agent Deployment Statuses 7-14
Endpoint Encryption Agent Installation Error Codes 7-16
Using OfficeScan to Uninstall Endpoint Encryption Agents 7-19

Chapter 8: Maintenance and Technical Support

Maintenance Agreement 8-2
Renewing the Maintenance Agreement 8-2
Trial License 8-3
Activating the New Product License 8-3
Viewing the Product License 8-4
Product Maintenance 8-5

Troubleshooting Resources 8-5
Trend Community 8-6
Using the Support Portal 8-6
Security Intelligence Community 8-6
Threat Encyclopedia 8-7

Contacting Trend Micro 8-7
Speeding Up the Support Call 8-8

Other Resources 8-8
TrendEdge 8-9
Download Center 8-9
TrendLabs 8-9

Appendices

Appendix A: Introducing Trend Micro Control Manager

Control Manager Standard and Advanced A-3

Introducing Control Manager Features A-3
Control Manager Architecture A-5
Registering Endpoint Encryption to Control Manager A-8
Understanding User Access A-9
Understanding the Product Directory A-15
Downloading and Deploying New Components A-38
Using Logs A-65
Understanding Reports A-68

Appendix B: Deployment Considerations

Initial Deployment Checklist B-2
Security Infrastructure Checklist B-4
Establishing Policy and Security Profiles B-6
Change Management Considerations B-7
Full Disk Encryption Pre-installation Checklist B-7
End User Communication B-11

Appendix C: Endpoint Encryption Pilot Deployment

About a Pilot Program C-2
Assigning a Project Team C-2
Implement a Phased Roll-out Strategy C-2
Endpoint Encryption Pilot Checklist C-3

Appendix D: Endpoint Encryption Services

Appendix E: Glossary

Index

Index IN-1

Preface

Preface

Welcome to the Trend Micro™ Endpoint Encryption Installation and Migration Guide. This document encourages you to get "up and running" in the shortest possible time by introducing Endpoint Encryption functions and the security architecture. This guide explains system requirements, how to prepare for deployment, how to install PolicyServer and Endpoint Encryption agent software, describes how to communicate the deployment to end users, and how to perform upgrades and migrations.

Topics include:

- *Document Set on page x*
- *Intended Audience on page x*
- *Document Conventions on page xi*
- *About Trend Micro on page xii*

Document Set

The documentation set for Trend Micro Endpoint Encryption includes the following:

TABLE 1. Product Documentation

DOCUMENT	DESCRIPTION
Administrator's Guide	Describes product concepts, features and detailed instructions about how to configure and manage PolicyServer, Full Disk Encryption, and File Encryption.
Installation and Migration Guide	Explains system requirements and contains detailed instructions about how to deploy, install, migrate, and upgrade PolicyServer, Full Disk Encryption, and File Encryption.
Online Help	All products contain an entry point to access the online help. The online help provides access the context-sensitive HTML help topics.
Readme File	Contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history.
Support Portal	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

Intended Audience

This guide is for IT Administrators deploying Trend Micro Endpoint Encryption in medium to large enterprises and Help Desk personnel who manage users, groups, policies, and devices. The documentation assumes basic device, networking and security knowledge, including:

- Endpoint hardware setup and configuration

- Basic endpoint encryption concepts
- Hard drive partitioning, formatting, and maintenance
- Client-server architecture

Document Conventions

The documentation uses the following conventions:

TABLE 2. 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
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen 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

Convention	Description
WARNING!	Critical actions and configuration options

About Trend Micro

As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to exchange digital information. With over 20 years of experience, Trend Micro provides top-ranked client, server, and cloud-based solutions that stop threats faster and protect data in physical, virtual, and cloud environments.

As new threats and vulnerabilities emerge, Trend Micro remains committed to helping customers secure data, ensure compliance, reduce costs, and safeguard business integrity. For more information, visit:

http://www.trendmicro.com

Trend Micro and the Trend Micro t-ball logo are trademarks of Trend Micro Incorporated and are registered in some jurisdictions. All other marks are the trademarks or registered trademarks of their respective companies.

Chapter 1

Introducing Endpoint Encryption

This chapter introduces Endpoint Encryption features, capabilities, devices, and users.

Topics include:

- *About Endpoint Encryption on page 1-2*
- *Key Features and Benefits on page 1-2*
- *What's New in Version 5.0 Patch 3 on page 1-3*
- *About Encryption on page 1-10*
- *Endpoint Encryption Components on page 1-11*
- *Endpoint Encryption Devices on page 1-20*
- *Endpoint Encryption Users on page 1-21*

About Endpoint Encryption

Trend Micro™ Endpoint Encryption ensures privacy by encrypting data stored on endpoints, files and folders, and removable media in a variety of platform options. Endpoint Encryption provides granular policy controls and flexibly integrates with other Trend Micro management tools, including Control Manager and OfficeScan. Innovative deployment capabilities help you easily deploy agent software using FIPS 140-2 hardware-based or software-based encryption that is fully transparent to end users, without disrupting productivity. Once deployed, automated reporting, auditing, and policy synchronization with Endpoint Encryption PolicyServer simplifies endpoint security management.

Endpoint Encryption has capabilities to deploy remote commands, recover lost data, and protect user identity while maintaining real-time policy synchronization. In the event that an endpoint is lost or stolen, remotely initiate a reset or "kill" command to immediately protect corporate information. Many recovery tools are also available to help end users rescue data from a corrupted hard disk. Assimilating into existing corporate identity controls, Endpoint Encryption has a variety of authentication methods, including Active Directory integration and resources for end users who have forgotten their credentials.

Key Features and Benefits

The following table explains Endpoint Encryption key features and benefits.

TABLE 1-1. Endpoint Encryption Key Features

FEATURE	BENEFITS
Encryption	• Protection for the full disk, including the master boot record (MBR), operating system, and all system files • Hardware-based and software-based encryption for mixed environments • Comprehensive data protection of files, folders, and removable media

Feature	Benefits
Authentication	• Flexible authentication methods, including both single and multi-factor • Control password strength and regularity for password changes • Policy updates before authentication and system boot • Configurable actions on failed password attempt threshold
Device management	• Policies to protect data on endpoints and removable media • Ability to remotely lock, reset, wipe, or kill a device
Central administration	• Flexibly use either PolicyServer MMC or Control Manager to manage PolicyServer • Deploy Endpoint Encryption agents to endpoints already managed by OfficeScan • Enforce security policies to individual users and policy groups from a single policy server • Instantly protect end user data by sending lock or erase commands to lost or stolen Endpoint Encryption devices • Automate policy enforcement with remediation of security events • Update security policies in real-time, before authentication, to revoke user credentials before booting the operating system
Record keeping, reports, and auditing	• Advanced real-time reporting and auditing to ensure security compliance • Analyze usage statistics with scheduled reports and alert notifications

What's New in Version 5.0 Patch 3

Trend Micro Endpoint Encryption 5.0 Patch 3 offers the following new features and enhancements.

TABLE 1-2. What's New in Endpoint Encryption 5.0 Patch 3

FEATURES / ENHANCEMENTS	DESCRIPTION
Supported Platforms	Endpoint Encryption supports agent installation on the following platforms: • Windows 10 (32-bit/64-bit) Supported agents: Full Disk Encryption and File Encryption • Windows 10 Enterprise and Professional editions (32-bit/64-bit) Supported agent: Encryption Management for Microsoft BitLocker • Windows Embedded POSReady 7 (32-bit/64-bit) Supported agents: Full Disk Encryption, File Encryption, and Encryption Management for Microsoft BitLocker • Mac OS X El Capitan Supported agent: Encryption Management for Apple FileVault
In-place Windows Upgrade	Endpoint Encryption supports upgrading devices encrypted by Full Disk Encryption to Windows 8.1 and Windows 10 without decrypting the boot device. To perform an in-place Windows upgrade, you will need to modify the Windows ISO file.

Features / Enhancements	Description
Wi-Fi Settings Enhancements	To prevent users from unintentionally modifying Wi-Fi settings, the Wi-Fi settings have been enhanced as follows: • Adminstrators can apply a policy to prevent or allow users to configure Wi-Fi settings. To modify the Wi-Fi settings policy, on PolicyServer MMC, go to **Policies** > **Full Disk Encryption** > **Agent** > **Allow User to Configure Wi-Fi**. • Wi-Fi settings have been moved to the Recovery Console accessible from the Full Disk Encryption Preboot. To see the Wi-Fi settings, on the preboot Recovery Console, go to the **Wi-Fi** tab on the **Network Setup** screen. If users are allowed to configure Wi-Fi settings, users can still use the wireless connection icon ( ) to access Wi-Fi settings.
Active Directory Fine-Grained Password Policy Support	Endpoint Encryption supports fine-grained password and account lockout policies for Windows Server 2008 and Windows Server 2012 Active Directory servers. To enable this feature, add the PolicyServer computer to the Password Setting object (PSO) Security list on the Active Directory server.
Usability Enhancement	The Full Disk Encryption preboot logon screen now displays indicators if Caps Lock or Num Lock are enabled.

Table 1-3. What's New in Endpoint Encryption 5.0 Patch 2

New Feature	Description
Active Directory Synchronization across Multiple OUs	Endpoint Encryption now supports policy enforcement, authentication, and synchronization across multiple organizational units (OUs). This enhancement allows administrators to manage users with the same policy over different security groups, cross-functional groups, or regional groups. Endpoint Encryption requires that separate OUs must be within the same Active Directory tree.

New Feature	Description
Simplified Active Directory Integration	The process for enabling automatic account synchronization from Active Directory has been streamlined. When managing Endpoint Encryption from Control Manager, administrators no longer need to access PolicyServer MMC in addition to the Control Manager web console. In addition, when configuring Active Directory from PolicyServer MMC, administrators no longer need to use the AD Synchronization Configuration Tool to complete configuration.
Supported Platforms	Endpoint Encryption supports PolicyServer installation on the following operating systems: • Windows Server 2012 • Windows Server 2012 R2 Endpoint Encryption supports the following database management systems for PolicyServer: • Microsoft SQL Server 2012 • Microsoft SQL Server 2012 Express Endpoint Encryption supports Encryption Management for Apple FileVault installation on the following operating system: • Mac OS X Yosemite™
Automated Deployment of Encryption Management for Apple FileVault	Endpoint Encryption supports automated deployments of Encryption Management for Apple FileVault agents. The process uses the same parameters and Command Line Helper tool for automated deployments of Full Disk Encryption, File Encryption, and Encryption Management for Microsoft BitLocker agents.
SanDisk Self-Encrypting SSD Support	Endpoint Encryption supports enabling and disabling of hardware-based full disk encryption of SanDisk™ self-encrypting solid-state drives (SSDs).

TABLE 1-4. What's New in Endpoint Encryption 5.0 Patch 1

NEW FEATURE	DESCRIPTION
Control Manager License Management	Endpoint Encryption PolicyServer integrates with Control Manager License Management. Control Manager supports the following features with Endpoint Encryption: • View the current Endpoint Encryption license information • Deploy a full license to PolicyServer • Renew a license to PolicyServer
Control Manager User-Centered Visibility	Endpoint Encryption integrates with Control Manager User-Centered Visibility. The status logs sent to Control Manager include the user information for the following Endpoint Encryption agents: • Full Disk Encryption • File Encryption • Encryption Management for Microsoft BitLocker • Encryption Management for Apple FileVault
NIC and Wi-Fi adapter Support	Endpoint Encryption supports the following groups of network interface controllers (NIC): • Intel Ethernet Controller I217 Family • Intel Ethernet Controller I218 Family Endpoint Encryption also supports the Intel Dual Band AC 7260 Wi-Fi adapter.

TABLE 1-5. What's New in Endpoint Encryption 5.0

NEW FEATURE	DESCRIPTION
New Communication Interface	Endpoint Encryption 5.0 introduces a new communication interface (Endpoint Encryption Service) that all Endpoint Encryption 5.0 agents and management consoles use to communicate with PolicyServer. Endpoint Encryption Service uses a Representational State Transfer web API (RESTful) with an AES-GCM encryption algorithm. Endpoint Encryption Service has three key features: • Access control: After user authentication, PolicyServer generates a token for that user in that session only. • Policy control: Before user authentication, Endpoint Encryption Service restricts all PolicyServer MMC, Control Manager, and OfficeScan policy transactions until after user authentication. • Automatic policy updates: After successfully registering with PolicyServer, Endpoint Encryption agents automatically obtain new policies without user authentication.
Control Manager Integration	Endpoint Encryption 5.0 integrates Control Manager for PolicyServer management. For information about Control Manager, see *About Control Manager Integration on page 5-2*.
OfficeScan Integration	Endpoint Encryption 5.0 provides support for OfficeScan deployments. Use the new Endpoint Encryption Deployment Tool plug-in to centrally deploy or uninstall Endpoint Encryption agents to any endpoint currently managed by OfficeScan.
License Management	Endpoint Encryption 5.0 integrates with the Trend Micro licensing portal. As in previous product versions, you can try Endpoint Encryption free for 30 days. After the trial license expires, an Activation Code is required. For information about licensing, see *Maintenance Agreement on page 8-2*.

New Feature	Description
Support for Apple FileVault™ and Microsoft BitLocker™	Endpoint Encryption 5.0 advances Full Disk Encryption by integrating with encryption solutions built into the host operating system through two new Endpoint Encryption agents: • Encryption Management for Microsoft BitLocker • Encryption Management for Apple FileVault PolicyServer centrally manages both agents with policy controls to remotely wipe or kill the Endpoint Encryption device.
FileArmor Name Change and Move to Common Framework	Endpoint Encryption 5.0 renames the FileArmor agent to File Encryption to better match the Endpoint Encryption agent's new functionality. File Encryption has the benefits from FileArmor 3.1.3, including improved support for removable media. File Encryption is also now better aligned with Full Disk Encryption for improved password and policy management.
Maintenance, Log, and Report Enhancements	Endpoint Encryption 5.0 has several improvements to product maintenance, logs and reports. • Mechanism to purge log database: It is now possible to purge the log database based on specific criteria. • Delete inactive Endpoint Encryption users and devices: To clean up the Enterprise devices and users, it is now possible to purge devices and users that are inactive for a specified time period. • Enterprise report for inactive users: The new Enterprise report shows all Endpoint Encryption users who have not logged on Endpoint Encryption devices for a specified period of time. • Enterprise report for inactive devices: The new Enterprise report shows all Endpoint Encryption devices that have not been logged on to for a specified duration of time.

New Feature	Description
Smart Card Enhancements	Endpoint Encryption 5.0 provides the following smart card enhancements: • Improved Endpoint Encryption agent deployment in environments using smart cards • Support for smart card password-sharing

About Encryption

Encryption is the process of making data unreadable unless there is access to the encryption key. Perform encryption via software or hardware (or a combination of the two) to protect data locally on an endpoint hard drive, on removable media, or in specific files and folders, and on data in transit across networks or the Internet. Endpoint encryption is the most important way to assure data security and to ensure that regulatory compliance mandates for data protection are met.

About FIPS

The *Federal Information Processing Standard (FIPS) Publication 140-2* is a United States government device security standard that specifies the security requirements for encryption modules. The following table explains the four levels of FIPS 140-2 security:

Table 1-6. FIPS 140-2 Security Levels

Level	Description
1	Requires all encryption components to be production grade, and absent of obvious security holes.
2	Includes level 1 requirements and adds physical tamper-evidence and role-based authentication.
3	Includes level 2 requirements and adds physical tamper-resistance and identity-based authentication.

LEVEL	DESCRIPTION
4	Includes level 3 requirements and adds additional physical security requirements.

Endpoint Encryption Components

Endpoint Encryption consists of one central management server (PolicyServer) that manages the policy and log databases, authentication, and all client-server activity. Deploy several unique Endpoint Encryption agents that each perform specific encryption tasks. All Endpoint Encryption agents communicate via an encrypted channel.

Flexibly manage Endpoint Encryption using only PolicyServer MMC or manage Endpoint Encryption using Control Manager for policy, user and device management and PolicyServer MMC for advanced log management and reporting.

Endpoint Encryption integrates with OfficeScan. Use the Endpoint Encryption Deployment Tool plug-in to deploy the Endpoint Encryption agent software to any OfficeScan managed endpoint.

Note

For information about deployment scenarios, see *Deployment and Upgrade Overview on page 3-1*.

The following illustration shows the Endpoint Encryption components and communication protocols.

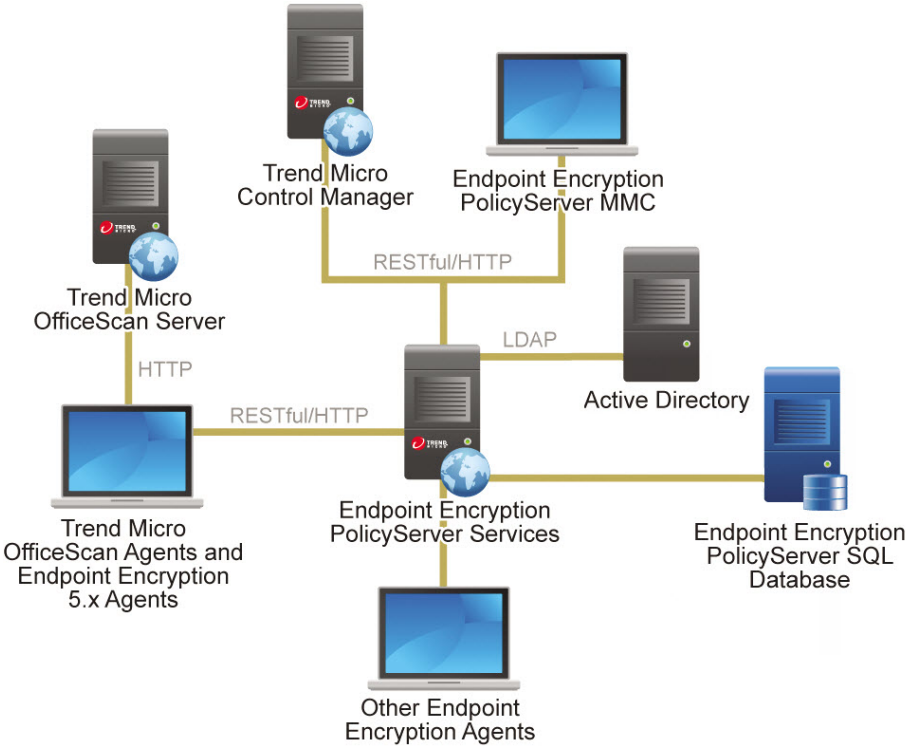


FIGURE 1-1. Endpoint Encryption Architecture

The following table describes these components.

TABLE 1-7. Endpoint Encryption Components

COMPONENT	DESCRIPTION
Endpoint Encryption PolicyServer Services	PolicyServer consists of several services that centrally control policies, authentication, and reporting. PolicyServer consists of the following: • Endpoint Encryption Service • Legacy Web Service • PolicyServer Windows Service For information about PolicyServer, see *About PolicyServer on page 1-14*.
Endpoint Encryption PolicyServer SQL Database	The Microsoft™ SQL Server database stores all user, policy, and log information. Install the database on the same server as PolicyServer, or separately. Flexibly configure PolicyServer using Microsoft SQL Server or Microsoft SQL Express. For information about database configuration options, see *Scaling Recommendations on page 3-17*.
Endpoint Encryption PolicyServer MMC	PolicyServer MMC is the native interface option to remotely manage PolicyServer.
Trend Micro Control Manager	Trend Micro Control Manager is an option to remotely manage PolicyServer while also integrating with other managed Trend Micro products. 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.

Component	Description
Endpoint Encryption 5.0 Patch 3 agents	All Endpoint Encryption 5.0 Patch 3 agents communicate with the PolicyServer Endpoint Encryption Service using a RESTful web API. For more information about Endpoint Encryption agents, see: • *About Full Disk Encryption on page 6-3* • *About File Encryption on page 6-4* For information about Endpoint Encryption agent communications, see *About PolicyServer on page 1-14*. **Note** Configure port settings during Endpoint Encryption agent installation. Full Disk Encryption can use Recovery Console to change the assigned port number.
Other Endpoint Encryption agents	All legacy Endpoint Encryption agents (3.1.3 and older) communicate to the Legacy Web Service on PolicyServer. For details about agent communications, see *About PolicyServer on page 1-14*.
Active Directory	PolicyServer synchronizes user account information by communicating with Active Directory using LDAP. Account information is cached in the Microsoft SQL database. **Note** Active Directory is optional.

About PolicyServer

Trend Micro PolicyServer manages encryption keys and synchronizes policies across all endpoints in the organization. PolicyServer also enforces secure authentication and provides real-time auditing and reporting tools to ensure regulatory compliance. You can flexibly manage PolicyServer with PolicyServer MMC or with Trend Micro Control

Manager. Other data management features include user-based self-help options and device actions to remotely reset or "kill" a lost or stolen device.

The following table describes the PolicyServer components that you can deploy on one server or multiple servers, depending on environmental needs.

TABLE 1-8. PolicyServer Components

COMPONENT	DESCRIPTION
Enterprise	The Endpoint Encryption Enterprise is the unique identifier about the organization in the PolicyServer database configured when installing PolicyServer. One PolicyServer database may have one Enterprise configuration.
Database	The PolicyServer Microsoft SQL database securely stores all user, device, and log data. The database is either configured on a dedicated server or added to an existing SQL cluster. The log and other databases can reside separately.
PolicyServer Windows Service	PolicyServer Windows Service manages all communication transactions between the host operating system, Endpoint Encryption Service, Legacy Web Service, Client Web Proxy, and SQL databases.
Endpoint Encryption Service	All Endpoint Encryption 5.0 Patch 3 agents use Endpoint Encryption Service to communicate with PolicyServer. Endpoint Encryption Service uses a Representational State Transfer web API (RESTful) with an AES-GCM encryption algorithm. After a user authenticates, PolicyServer generates a token related to the specific policy configuration. Until the Endpoint Encryption user authenticates, the service denies all policy transactions. To create a three level network topography, the service can also be separately deployed to an endpoint residing in the network DMZ, which allows PolicyServer to safely reside behind the firewall. For information about deployment scenarios, see the *Endpoint Encryption Installation and Migration Guide*.

COMPONENT	DESCRIPTION
Legacy Web Service	All Endpoint Encryption 3.1.3 and older agents use Simple Object Access Protocol (SOAP) to communicate with PolicyServer. Under certain situations, SOAP may allow insecure policy transactions without user authentication. Legacy Web Service filters SOAP calls by requiring authentication and limiting the commands that SOAP accepts. To create a three level network topography, the service can also be separately deployed to an endpoint residing in the network DMZ, which allows PolicyServer to safely reside behind the firewall. For information about deployment scenarios, see the *Endpoint Encryption Installation and Migration Guide*.

Management Consoles

Depending on endpoint security and existing infrastructure needs, you can manage Endpoint Encryption using only one management console or a combination of several management consoles. The following table describes the management consoles available to manage Endpoint Encryption.

TABLE 1-9. Endpoint Encryption Management Consoles

MANAGEMENT CONSOLE	DESCRIPTION
PolicyServer MMC	The PolicyServer Microsoft Management Console plug-in (PolicyServer MMC) is the native management console for Endpoint Encryption policy, user, and device administration. Use PolicyServer MMC to centrally manage: • All Endpoint Encryption users, devices, and groups • All policies including encryption, password complexity and authentication • Remote device actions, including killing a device, erasing data, or delaying authentication • Event logs about authentication events, management events, device encryption status, and security violations • Remote Help password reset process • Auditing and reporting options

Management Console	Description
Control Manager	Trend Micro Control Manager is a central management console that manages Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. Administrators can use the policy management feature to configure and deploy product settings to managed products and endpoints. The Control Manager web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network. Create multilayer security by integrating Endpoint Encryption with Control Manager as a managed Trend Micro product. Flexibly manage Endpoint Encryption using only PolicyServer MMC or manage Endpoint Encryption using Control Manager for policy, user and device management and PolicyServer MMC for advanced log management and reporting.
OfficeScan	OfficeScan protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks. An integrated solution, OfficeScan consists of an agent that resides at the endpoint and a server program that manages all agents. Use the OfficeScan Endpoint Encryption Deployment Tool plug-in to centrally deploy or uninstall Endpoint Encryption agents to any endpoint currently managed by OfficeScan.

Endpoint Encryption Agents

The following table describes the Endpoint Encryption agents available for a variety of environments.

Agent	Description
File Encryption	The Endpoint Encryption agent for file and folder encryption on local drives and removable media. Use File Encryption to protect files and folders located on virtually any device that appears as a drive within the host operating system. For more information, see *About File Encryption on page 6-4*.
Full Disk Encryption	The Endpoint Encryption agent for hardware and software encryption with preboot authentication. Use Full Disk Encryption to secure data files, applications, registry settings, temporary files, swap files, print spoolers, and deleted files on any Windows endpoint. Strong preboot authentication restricts access vulnerabilities until the user is validated. For more information, see *About Full Disk Encryption on page 6-3*.
Encryption Management for Microsoft BitLocker	The Endpoint Encryption Full Disk Encryption agent for Microsoft Windows environments that simply need to enable Microsoft BitLocker on the hosting endpoint. Use the Encryption Management for Microsoft BitLocker agent to secure endpoints with Trend Micro full disk encryption protection in an existing Windows infrastructure. For more information, see *About Full Disk Encryption on page 6-3*.
Encryption Management for Apple FileVault	The Endpoint Encryption Full Disk Encryption agent for Mac OS environments that simply need to enable Apple FileVault on the hosting endpoint. Use the Encryption Management for Apple FileVault agent to secure endpoints with Trend Micro full disk encryption protection in an existing Mac OS infrastructure. For more information, see *About Full Disk Encryption on page 6-3*.

Note

Endpoint Encryption 5.0 does not have KeyArmor devices. However, legacy KeyArmor devices are supported.

Endpoint Encryption Devices

Endpoint Encryption devices are Endpoint Encryption agents that have registered with PolicyServer. Installing any Endpoint Encryption agent automatically registers the endpoint with PolicyServer as a new Endpoint Encryption device. Since multiple Endpoint Encryption agents may protect a given endpoint, a single endpoint may appear as more than one Endpoint Encryption device on PolicyServer.

You can set policy rules that automatically trigger after too many failed authentication attempts or when the Endpoint Encryption agent has outdated policies. The following policy rules are available:

- Time delay
- Remote authentication required
- Erase device

PolicyServer can instantly act upon a lost or stolen endpoint by initiating a remote action upon the associated Endpoint Encryption device. The following remote actions are available:

- Software token
- Recovery key
- Kill device
- Lock device
- Soft reset

Note

For more information about Endpoint Encryption devices, see *Devices and Users* in the *Endpoint Encryption Administrator's Guide*.

Endpoint Encryption Users

Endpoint Encryption users are any user account manually added to PolicyServer or synchronized with Active Directory.

Endpoint Encryption has several types of account roles and authentication methods for comprehensive identity-based authentication and management. Using Control Manager or PolicyServer MMC, you can add or import user accounts, control authentication, synchronize with the Active Directory, and manage policy group membership, as needed.

Note

For more information about Endpoint Encryption users and authentication, see *Devices and Users* in the *Endpoint Encryption Administrator's Guide*.

Endpoint Encryption User Roles

The following table explains the Endpoint Encryption user account types intended for different roles within the Enterprise or policy group. Each role determines the permissions granted when the user accesses Endpoint Encryption management consoles and devices.

TABLE 1-10. Endpoint Encryption Account Roles

ROLE	DESCRIPTION
Enterprise Administrator	Intended for administrators who control the Enterprise and require administrative rights to all groups, users, devices, and policies regardless of where they reside.

Role	Description
Group or Policy Administrator*	Intended for administrators who control any assigned group or policy. **Note** Privileges do not apply to parent groups, groups at the same level in the hierarchy or their subgroups.
Enterprise Authenticator	Intended for Help Desk personnel who provide remote assistance when users forget their Endpoint Encryption password or have a technical problem. Enterprise Authenticators have configurable privileges for the Enterprise.
Group or Policy Authenticator*	Intended for Help Desk personnel with the same privileges as the Enterprise Authenticator except for being limited to the assigned group or policy only.
User	Intended for basic end users with no special privileges. The user role cannot log on to Endpoint Encryption management consoles.

Note

*Due to differences in policy architecture, Control Manager merges the policy and group structure of PolicyServer MMC. The following roles are the same between PolicyServer MMC and Control Manager:

- Group Administrator (PolicyServer MMC) and Policy Administrator (Control Manager)
- Group Authenticator (PolicyServer MMC) and Policy Authenticator (Control Manager)

Chapter 2

System Requirements

This chapter outlines the system requirements for Trend Micro Endpoint Encryption.

Topics include:

- *PolicyServer Requirements on page 2-2*
- *Management Consoles on page 2-6*
- *Agents on page 2-9*

PolicyServer Requirements

This section outlines the hardware and software requirements for PolicyServer, the files needed for the installations, and also the accounts needed to set up the database and Windows server environments.

PolicyServer System Requirements

TABLE 2-1. PolicyServer System Requirements

SPECIFICATION	REQUIREMENTS
Processor	See *Database Considerations on page 2-4*
RAM	
Disk space	
Operating system	• Windows Server 2003 SP2 32-bit/64-bit • Windows Server 2008 / 2008 R2 64-bit **Note** For additional Windows Server 2008 / 2008 R2 requirements, see *Windows Server 2008 and 2008 R2 Considerations on page 2-3*. • Windows Server 2012 / 2012 R2 64-bit
Database server	• Microsoft SQL Server 2005 SP3 (32-bit/64-bit) / 2008 / 2008 R2 / 2012 • Microsoft SQL Server Express 2005 SP3 / 2008 / 2012 • Mixed Mode Authentication (SA password) installed • Reporting services installed

SPECIFICATION	REQUIREMENTS

Application server	PolicyServer 5.0 Patch 3 requires Microsoft IIS with the following roles installed and enabled:
	• Application Development
	  • ASP.NET
	  • ASP
	  • ISAPI Extensions
	  • ISAPI Filters
	• Management Tools
	  • IIS Management Console
	  • IIS Management Scripts and Tools
	  • Management Service
	  • IIS 6 Management Compatibility
	  • IIS 6 Metabase Compatibility
	Legacy Endpoint Encryption environments (version 3.1.3 and earlier) require Client Web Service. If you install Client Web Service on a remote endpoint, install Microsoft IIS on that endpoint.

Other software	• Both Microsoft .Net Framework 2.0 SP2 (or 3.5) and 4.0 • Windows Installer 4.5 (SQL Express)

Windows Server 2008 and 2008 R2 Considerations

The following table explains the additional requirements to install PolicyServer on Microsoft Windows Server 2008 or Microsoft Windows Server 2008 R2.

Operating System	Roles	Features	Other
2008	• Install application server role • Install web server role	• Add SMTP • Add Microsoft IIS support	• Install Microsoft .Net Framework 4.0
2008 R2			• Must install SQL 2008 SP1 to run SQL 2008 • No .NET upgrade required

Database Considerations

When installing PolicyServer, it is recommended to have at least two dedicated servers:

1. A dedicated server for the database, or add the database to an existing SQL cluster.
2. A dedicated server for the PolicyServer services.

Note

Virtual hardware is supported under VMware Virtual Infrastructure.

Table 2-2. PolicyServer Hardware Requirements

Separate Hosts		Single Host
PolicyServer Host (3,000 Users)	SQL Server Host (3,000 Users)	PolicyServer and SQL Server (1,500 Users)
• 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Processors • 4 GB RAM • 40 GB hard disk space	• 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Processors • 8 GB RAM • 100 GB hard disk space	• 2 GHz Quad Core Core2 Intel™ Xeon™ Processors • 8 GB RAM • 120 GB hard disk space

Required Installation Files

Copy all installation files to the local drive before installation.

TABLE 2-3. Required Files to Install PolicyServer

FILE	PURPOSE
`PolicyServerInstaller.exe`	Installs PolicyServer databases and services. Optionally, the PolicyServer MMC can install at the same time.
`PolicyServer MMCSnapinSetup.msi`	Installs the PolicyServer MMC only.
`TMEEProxyInstaller.exe`	Installs the Client Web Service and the Traffic Forwarding Service. These services function as web proxies and communication protocols for environments that have PolicyServer and Endpoint Encryption agents in different LANs. Client Web Service functions for 3.1.3 or earlier agents and Traffic Forwarding Service functions for 5.0 or later agents.

Note

PolicyServer includes a 30-day trial license. A license file is not longer required to upgrade to the full product version. For more information, see *Maintenance and Technical Support on page 8-1*.

Required Accounts

The following table explains the function and description of the accounts required by PolicyServer.

TABLE 2-4. Accounts Needed to Install PolicyServer

ACCOUNT	FUNCTION	DESCRIPTION
SQL SA	PolicyServer Installer	Account is used only to create the PolicyServer databases

Account	Function	Description
SQL MADB	PolicyServer Windows Service	Account created during installation to authenticate to PolicyServer databases
Local Administrator	PolicyServer Windows Service and IIS	Account used to run the PolicyServer Windows Service and web service application pools

Management Consoles

This section outlines the requirements for the management consoles.

PolicyServer MMC System Requirements

The following table explains the system requirements for PolicyServer MMC. It can be installed when installing PolicyServer or separately installed on a different endpoint.

Table 2-5. PolicyServer MMC System Requirements

Specification	Requirements
Processor	Intel™ Core™ 2 or compatible processor
RAM	512 MB
Disk space	100 MB minimum
Network connectivity	Connectivity with PolicyServer
Operating system	Any Microsoft Windows operating system supported by PolicyServer or the Endpoint Encryption agents
Others	• Microsoft .NET Framework 4.0

Control Manager System Requirements

The following table explains the requirements to use Control Manager for server management.

TABLE 2-6. Control Manager Requirements

SPECIFICATION	REQUIREMENTS
Control Manager Server	Control Manager, Patch 3
RAM	• 2 GB minimum • 4 GB recommended
Disk Space	• 10 GB minimum • 20 GB recommended
Network connectivity	Connectivity with PolicyServer
Others	For additional Control Manager system requirements and setup instructions, see the Control Manager documentation available at: http://docs.trendmicro.com/en-us/enterprise/control-manager.aspx

OfficeScan System Requirements

The following tables explain the system requirements to install OfficeScan, use the Endpoint Encryption Deployment Tool plug-in to deploy Endpoint Encryption agents, or install the OfficeScan agent.

TABLE 2-7. OfficeScan Server Requirements

SPECIFICATION	REQUIREMENTS
OfficeScan Server	Any of the following versions: • 10.6 SP3 • 10.5 Patch 5

Specification	Requirements
Plug-in Manager	2.0
RAM	• 1 GB minimum with at least 500 MB dedicated to OfficeScan • 2 GB recommended

Disk space for OfficeScan	• 3.1 GB minimum if the server has:
	  • OfficeScan server
	  • OfficeScan client
	  • Policy Server for Cisco™ NAC
	  • Integrated Smart Protection Server (local)
	• 3.5 GB minimum if the server has:
	  • OfficeScan server
	  • OfficeScan client
	  • Integrated Smart Protection Server (remote)

Disk space for Endpoint Encryption Deployment Tool	1 GB minimum
Network connectivity	• Connectivity with PolicyServer • Connectivity with OfficeScan endpoints
Others	For additional OfficeScan system requirements and setup instructions, see the OfficeScan documentation available at: http://docs.trendmicro.com/en-us/enterprise/officescan.aspx

Table 2-8. OfficeScan Agent Requirements

Specification	Requirements
RAM	• 512 MB minimum
Disk space	• 1 GB minimum

Specification	Requirements
Network connectivity	• Connectivity with PolicyServer • Connectivity with OfficeScan endpoints
Others	Microsoft .NET Framework 2.0 SP1 **Note** Although OfficeScan agents can run on any Windows version, make sure to review the system requirements for Endpoint Encryption each agent.

Agents

This section outlines the requirements for all Endpoint Encryption agents.

Full Disk Encryption System Requirements

The following table describes the minimum and recommended system requirements to install Full Disk Encryption.

Table 2-9. Full Disk Encryption System Requirements

Specification	Requirements
Processor	Intel™ Core™ 2 or compatible processor
RAM	1 GB minimum
Disk space	• 30 GB minimum • 20% free disk space required • 256 MB contiguous free space required
Network connectivity	Communication with PolicyServer required for managed agents

Specification	Requirements
Operating system	• Windows™ Embedded POSReady 7 (32-bit/64-bit) • Windows™ 10 (32-bit/64-bit) • Windows™ 8.1 (32-bit/64-bit) • Windows™ 8 (32-bit/64-bit) • Windows™ 7 (32-bit/64-bit) • Windows™ Vista with SP1 (32-bit/64-bit) • Windows™ XP with SP3 (32-bit only)
Other software	Additional Windows 8 requirements: • Microsoft .NET Framework 3.5 enabled • For devices with UEFI, set the boot priority to **Legacy First**. See the *Endpoint Encryption Installation and Migration Guide*. Additional Windows XP requirements: • Microsoft .NET Framework 2.0 SP1 or later • Microsoft Windows Installer 3.1
Hard disk	• Seagate DriveTrust drives • Seagate OPAL and OPAL 2 drives • SanDisk self-encrypting solid-state drives **Note** • Do not install Full Disk Encryption on endpoints with multiple hard disks. Multiple disk environments are not supported • RAID and SCSI disks are not supported • Full Disk Encryption for Windows 8 does not support RAID, SCSI, or eDrive drives

Specification	Requirements
Other hardware	• Software encryption: ATA, AHCI, or IRRT hard disk controller **Note** RAID and SCSI BIOS settings are not supported. • Hardware encryption: AHCI hard disk controller **Note** No other BIOS settings are not supported.

Encryption Management for Microsoft BitLocker System Requirements

This following table explains the minimum and recommended Encryption Management for Microsoft BitLocker system requirements.

Table 2-10. Encryption Management for Microsoft BitLocker System Requirements

Specification	Requirements
Processor	Intel™ Core™ 2 or compatible processor
RAM	Requirements are the based on Windows system requirements: • 64-bit systems: 2 GB • 32-bit systems: 1 GB
Disk space	• 30 GB minimum • 20% free disk space required • 256 MB contiguous free space required
Hard disk	• Standard drives supported by Windows
Network connectivity	Connectivity with PolicyServer

Specification	Requirements
Operating system	• Windows™ Embedded POSReady 7 (32-bit/64-bit) • Windows™ 10 Enterprise and Professional editions (32-bit/64-bit) • Windows™ 8.1 (32-bit/64-bit) • Windows™ 8 (32-bit/64-bit) • Windows™ 7 (32-bit/64-bit)
Other software	• Trusted Platform Module (TPM) 1.2 or higher • Full Disk Encryption is not installed • Windows BitLocker is disabled • Microsoft .NET Framework 3.5 enabled

Encryption Management for Apple FileVault System Requirements

This following table explains the minimum and recommended Encryption Management for Apple FileVault system requirements.

Table 2-11. Encryption Management for Apple FileVault System Requirements

Specification	Requirement
Processor	Intel™ Core™ 2 or compatible processor
Memory	• 512 MB minimum • 1 GB recommended
Disk space	• 400 MB minimum
Network connectivity	Connectivity with PolicyServer

Specification	Requirement
Operating system	• Mac OS X El Capitan™ • Mac OS X Yosemite™ • Mac OS X Mavericks™ • Mac OS X Mountain Lion™ • Mac OS X Lion™ **Note** Mac OS local accounts or mobile accounts are able to initiate encryption on Mac OS X Mountain Lion or above. Other Mac OS user account types will be unable to initiate encryption. To create a mobile account for Active Directory on your Mac, see *Creating a Mobile Account for Active Directory on Mac OS on page 6-27*.
Other software	• Mono runtime environment (MRE) 2.1 • Apple FileVault is disabled

File Encryption System Requirements

The following table explains the File Encryption system requirements.

Table 2-12. File Encryption System Requirements

Specification	Requirements
Processor	Intel™ Core™ 2 or compatible processor
RAM	1 GB minimum
Disk space	• 30 GB minimum • 20% free disk space required
Network connectivity	Communication with PolicyServer required for managed agents

Specification	Requirements
Operating system	• Windows™ 10 (32-bit/64-bit) • Windows™ 8.1 (32-bit/64-bit) • Windows™ 8 (32-bit/64-bit) • Windows™ 7 (32-bit/64-bit) • Windows™ Vista with SP1 (32-bit/64-bit) • Windows™ XP with SP3 (32-bit only)
Other software	Additional Windows 8 requirements: • Microsoft .NET Framework 3.5 enabled • For devices with UEFI, set the boot priority to **Legacy First**. See the *Endpoint Encryption Installation and Migration Guide*. Additional Windows XP requirements: • Microsoft .NET Framework 2.0 SP1 or later • Microsoft Windows Installer 3.1

Important

The Full Disk Encryption agent can only install on an endpoint with one physical drive. Remove all other drives before installing Full Disk Encryption.

Chapter 3

Deployment and Upgrade Overview

This chapter summarizes deployment options and explains the technical requirements for the initial Endpoint Encryption agent deployments across the enterprise, various scaling and network topology options, and upgrading the entire organization from a previous Endpoint Encryption version to Endpoint Encryption 5.0 Patch 3.

For information about designing a product team or the best practices to communicate with end users, see *Deployment Considerations on page B-1*.

Topics include:

- *Deployment Planning on page 3-2*
- *Predeployment Checklist on page 3-2*
- *Management Options on page 3-5*
- *Deployment Options on page 3-11*
- *Scaling Recommendations on page 3-17*
- *Upgrade Deployments on page 3-21*

Deployment Planning

When addressing any encryption project, it is important to identify the implementation goals. Organizations needing to satisfy explicit regulatory compliance requirements often require broad encryption solutions with a heavy emphasis on reporting, whereas organizations looking to improve data security may have more targeted needs to protect specific data assets.

No single plan can fit every use-case scenario, and understanding what is required of an encryption solution will greatly decrease deployment times, minimize or eliminate performance degradation, and ensure the project's success. Careful planning is required to understand the deployment requirements and limitations when scaling Endpoint Encryption across a large enterprise. Planning is especially important when introducing this change across thousands of endpoints, affecting all end users.

Predeployment Checklist

The following tables explain supported operating systems for each Endpoint Encryption agent and the requirements before deployment.

TABLE 3-1. PolicyServer 5.0 Patch 3

PLATFORM	PRE-DEPLOYMENT CHECKLIST
Windows Server 2003 (32/64-bit)	• Install both Microsoft .Net Framework 2.0 SP2 (or 3.5) and 4.0 • Use an Administrator account to install PolicyServer MMC • To log on to PolicyServer MMC, connectivity with the PolicyServer database is required
Windows Server 2008/2008 R2 (64-bit)	

TABLE 3-2. Full Disk Encryption

PLATFORM	PRE-DEPLOYMENT CHECKLIST
Windows 8™ (32/64-bit)	• Set UEFI-compatible endpoint's BIOS boot priority to **Legacy** instead of **UEFI** first. • Verify that Microsoft .Net 3.5 is enabled • Run `sfc /scannow` and `defrag` before installation • Confirm standard boot sector MBR • Verify that there is 20% free disk space • Back up user data **Note** Full Disk Encryption on Windows 8 does not support RAID, SCSI, eDrive, or OPAL 2 drives.
Windows 7™ (32/64-bit)	• Verify that Microsoft .NET 2.0 SP1 or later is installed • Verify that Windows Installer version 3.1 is install • Connection to PolicyServer, if managed • Run `scandisk` and `defrag` before installation • Confirm standard boot sector MBR • Verify that there is 20% free disk space • Back up user data **Note** Full Disk Encryption does not support RAID or SCSI drives.
Windows Vista™ with SP1 (32/64-bit)	
Windows XP™ with SP3 (32-bit)	

TABLE 3-3. File Encryption

PLATFORM	PRE-DEPLOYMENT CHECKLIST
Windows 8™ (32/64-bit)	• Set UEFI-compatible endpoint's BIOS boot priority to **Legacy** instead of **UEFI** first. • Verify that Microsoft .Net 3.5 is enabled

Platform	Pre-deployment Checklist
Windows 7™ (32/64-bit)	• Verify that Microsoft .NET 2.0 SP1 or later is installed
Windows Vista™ with SP1 (32/64-bit)	
Windows XP™ with SP3 (32-bit)	

Note

For information about designing a product team or the best practices to communicate with end users, see *Deployment Considerations on page B-1*.

Deployment Summary of Operations

The following procedure explains the high level summary of operations required to deploy Endpoint Encryption 5.0 Patch 3 across the enterprise.

Note

For information about fresh installations, see *Deployment Options on page 3-11*.

For information about upgrading the enterprise, see *Upgrade Deployments on page 3-21*.

Procedure

1. Plan for the deployment.

   See *Deployment Considerations on page B-1*.

2. Run a pilot program.

   See *Endpoint Encryption Pilot Deployment on page C-1*.

3. Decide how to manage Endpoint Encryption.

   See *Management Options on page 3-5*.

4. Decide whether to integrate with other Trend Micro products.

   See *Control Manager Integration on page 5-1*.

   See *OfficeScan Integration on page 7-1*.

5. Review all system requirements.

   See *System Requirements on page 2-1*

6. Install or upgrade PolicyServer.

   See *PolicyServer Deployment on page 4-1*.

7. Decide whether to configure Active Directory authentication.

   See *PolicyServer Active Directory Synchronization on page 4-16*.

8. Install or upgrade Endpoint Encryption agents.

   See *Endpoint Encryption Agent Deployment on page 6-1*.

9. Manage the Endpoint Encryption implementation.

   See the *Endpoint Encryption Administrator's Guide*.

Management Options

This section explains how to deploy Endpoint Encryption security with only PolicyServer MMC management, or to integrate with Control Manager and OfficeScan for additional management options.

Note

For management console introductions, see *Management Consoles on page 1-16*.

Managing Endpoint Encryption with PolicyServer MMC Only

The following procedure explains how to configure Endpoint Encryption for PolicyServer MMC policy, user, and device management without Control Manager or OfficeScan integration.

Note

For more information, see *PolicyServer Deployment on page 4-1*

Procedure

1. Install PolicyServer.

   See *Installing PolicyServer on page 4-3*.

2. Configure groups.

3. Add users to each group.

4. Use third-party products to deploy the agents, or manually install on the agent on each endpoint.

   See*Endpoint Encryption Agent Deployment on page 6-1*

Control Manager and OfficeScan Integration

Endpoint Encryption allows administrators to use Trend Micro Control Manager to control PolicyServer and manage Endpoint Encryption agent policies or use Trend Micro OfficeScan to deploy Endpoint Encryption agent software on managed endpoints.

The Endpoint Encryption implementation fits into the existing data loss prevention security infrastructure that is already managed by Control Manager. You simply add PolicyServer as a managed product to gain access to all aspects of user, policy, and device management that exist in PolicyServer MMC. You can still use PolicyServer MMC for some advanced Enterprise management functionality.

In environments with OfficeScan managed endpoints, use the Endpoint Encryption Deployment Tool plug-in to remotely deploy the Endpoint Encryption agent software. Although traditional methods of Endpoint Encryption agent software deployment are still available (see *Automated Deployments on page 6-33*, OfficeScan allows you to precisely control the deployment, see the Endpoint Encryption agent installation status, and easily control the deployment from a web-based console.

Note

For information about management consoles available to control PolicyServer or manage Endpoint Encryption agents, see *Management Consoles on page 2-6*.

For information about integrating with Control Manager, see *Control Manager Integration on page 5-1*.

For information about integrating with OfficeScan, see *OfficeScan Integration on page 7-1*.

Introducing Trend Micro Control Manager

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

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

Introducing Trend Micro OfficeScan

OfficeScan protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks. An integrated solution, OfficeScan consists of an agent that resides at the endpoint and a server program that manages all agents.

The agent guards the endpoint and reports its security status to the server. The server, through the web-based management console, makes it easy to set coordinated security policies and deploy updates to every agent.

Use the OfficeScan Endpoint Encryption Deployment Tool plug-in to deploy Endpoint Encryption agents to OfficeScan managed endpoints. You can select endpoints based on specific criteria and see the status of the deployment. After the Endpoint Encryption Deployment Tool plug-in deploys the Endpoint Encryption agent software, the Endpoint Encryption agent synchronizes to PolicyServer using the settings specified in the plug-in. OfficeScan does not manage Endpoint Encryption policies. The OfficeScan agent and the Endpoint Encryption agent are independent on the same endpoint.

About Trend Micro OfficeScan Integration

OfficeScan protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks. An integrated solution, OfficeScan consists of an agent that resides at the endpoint and a server program that manages all agents.

The agent guards the endpoint and reports its security status to the server. The server, through the web-based management console, makes it easy to set coordinated security policies and deploy updates to every agent.

Note

For information about OfficeScan, see the supporting documentation at:

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

Use the OfficeScan Endpoint Encryption Deployment Tool plug-in to deploy Endpoint Encryption agents to OfficeScan managed endpoints. You can select endpoints based on specific criteria and see the status of the deployment. After the Endpoint Encryption Deployment Tool plug-in deploys the Endpoint Encryption agent software, the Endpoint Encryption agent synchronizes to PolicyServer using the settings specified in

the plug-in. OfficeScan does not manage Endpoint Encryption policies. The OfficeScan agent and the Endpoint Encryption agent are independent on the same endpoint.

The following illustration explains how to deploy Endpoint Encryption for the first time on OfficeScan managed endpoints. In OfficeScan deployments, administrators can use either Control Manager or PolicyServer MMC to manage PolicyServer.

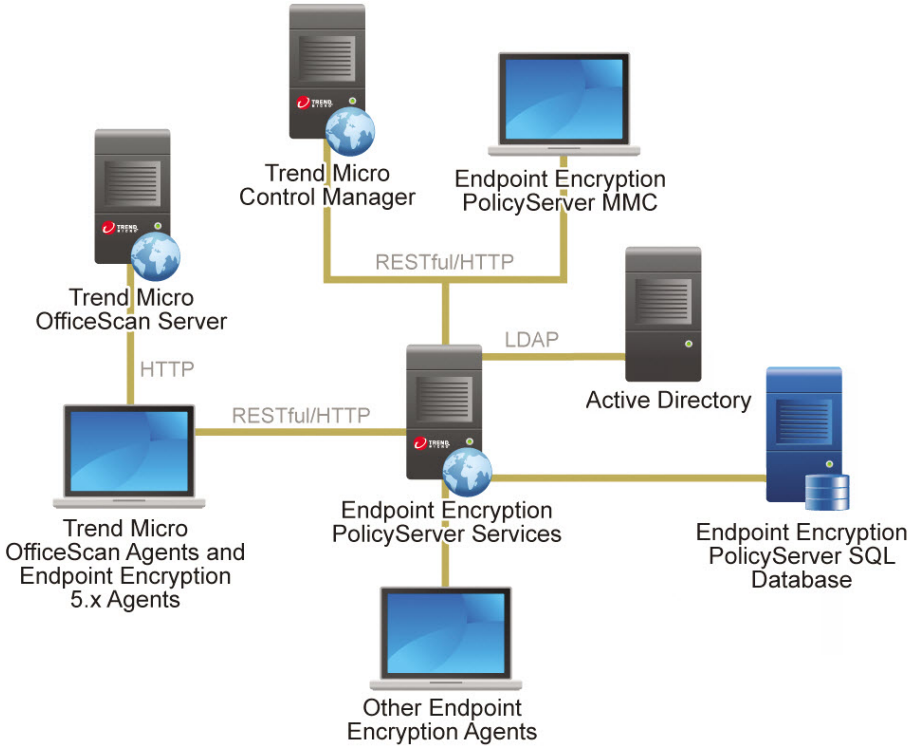


FIGURE 3-1. OfficeScan integration deployment

Summary of Operations

Endpoint Encryption allows administrators to use Trend Micro Control Manager to control PolicyServer and manage Endpoint Encryption agent policies or use Trend

Micro OfficeScan to deploy Endpoint Encryption agent software on managed endpoints.

The following procedure provides a high-level summary of operations to install the management consoles and deploy the Endpoint Encryption agent software and security policies.

Note

For information about management consoles available to control PolicyServer or manage Endpoint Encryption agents, see *Management Consoles on page 2-6*.

For information about integrating with Control Manager, see *Control Manager Integration on page 5-1*.

For information about integrating with OfficeScan, see *OfficeScan Integration on page 7-1*.

Procedure

1. Review all system requirements for compatible product versions.

   See *System Requirements on page 2-1*.

2. Install PolicyServer.

   See *Installing PolicyServer on page 4-3*.

3. Install and configure OfficeScan.

   See the supporting documentation at:

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

4. Add PolicyServer to OfficeScan.

   See *Deploying Server Settings on page 7-11*.

5. Prepare endpoints for deployment.

   See *Before Installing Endpoint Encryption Agents on page 6-4*.

6. Use OfficeScan to deploy Endpoint Encryption agents.

See *OfficeScan Integration on page 7-1*

7. Install and configure Control Manager.

   See the supporting documentation at:

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

8. Add PolicyServer to Control Manager.

   See *Adding PolicyServer as a Managed Product to Control Manager on page 5-4*

9. Use Control Manager to deploy policies.

   See *Creating a Policy on page 5-8*.

Deployment Options

When deploying Endpoint Encryption across the entire organization, there are several network options available depending on existing infrastructure or security needs. This section explains the deployment options available for Endpoint Encryption deployment.

Simple Deployment

The following illustration explains how to deploy Endpoint Encryption for the first time and using only PolicyServer MMC to manage PolicyServer. For more information, see *PolicyServer Installation and Configuration on page 4-3*.

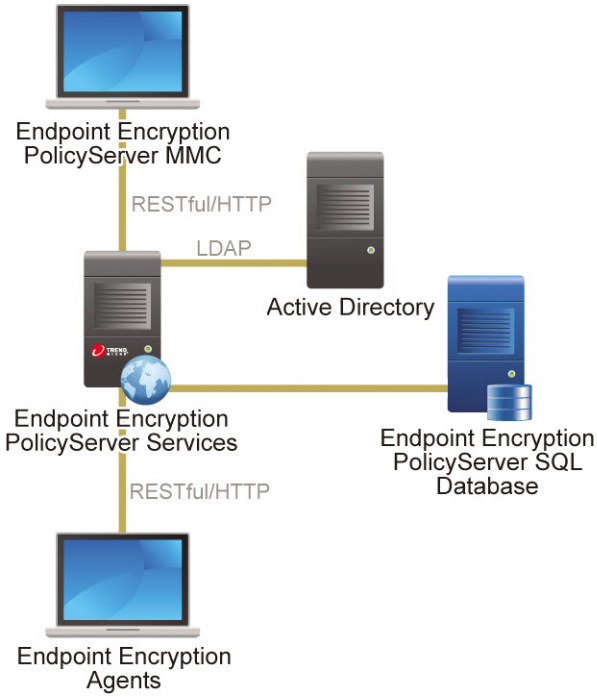


FIGURE 3-2. Simple Endpoint Encryption Deployment

Note

For information about an upgrade deployment that may have Endpoint Encryption 3.1.3 (or older) agents, see *Upgrade Deployments on page 3-21*.

Control Manager Deployment

The following illustration explains how to deploy Endpoint Encryption for the first time using Control Manager to manage PolicyServer. In a Control Manager deployment, administrators use Control Manager for all Endpoint Encryption policy, user, and device controls, and only use PolicyServer MMC for advanced Enterprise maintenance.

For more information, see *Control Manager Integration on page 5-1*.

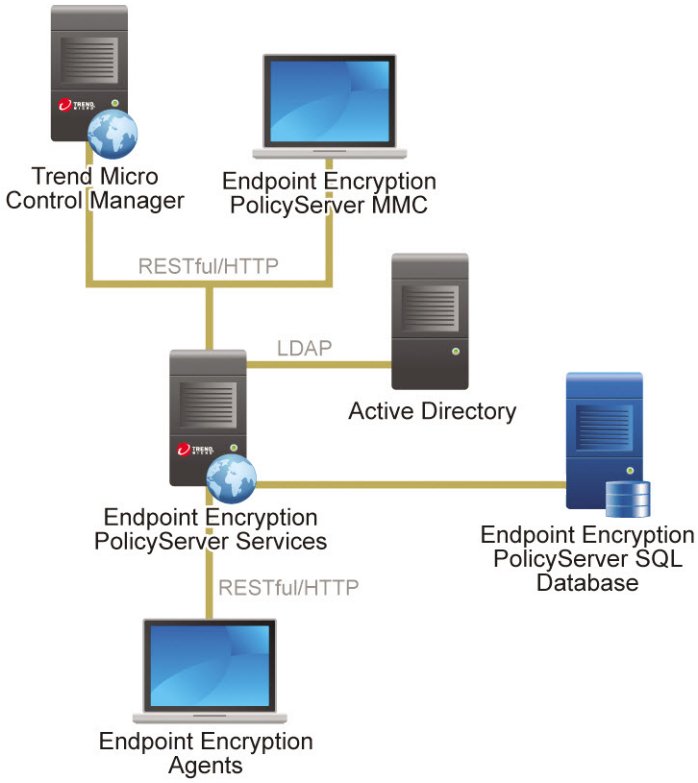


FIGURE 3-3. Control Manager integration deployment

Note

In environments that use Control Manager, changes to PolicyServer policies are always controlled by Control Manager. Any changes made using PolicyServer MMC are overwritten the next time that Control Manager synchronizes policies to the PolicyServer database.

OfficeScan Deployment

The following illustration explains how to deploy Endpoint Encryption for the first time on OfficeScan managed endpoints. In OfficeScan deployments, administrators can use either Control Manager or PolicyServer MMC to manage PolicyServer.

For more information, see *OfficeScan Integration on page 7-1*

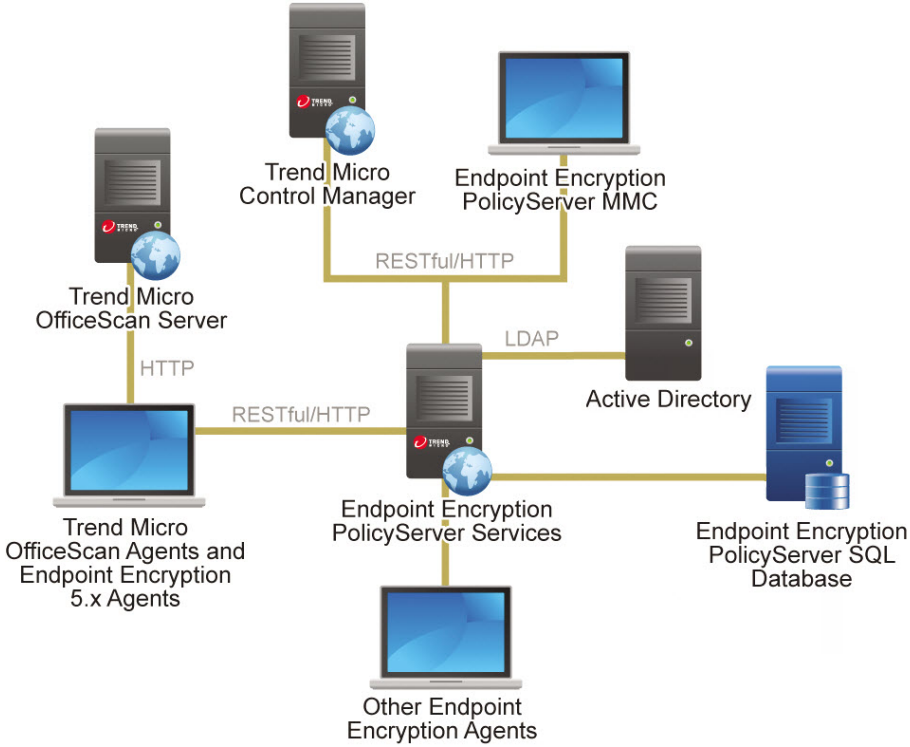


FIGURE 3-4. OfficeScan integration deployment

Complex Distributed Deployment

The following illustration explains the network environment of a complex distributed deployment using both Endpoint Encryption 5.0 Patch 3 and Endpoint Encryption legacy agents. You can configure Traffic Forwarding Service and Client Web Service on

the same endpoint separate from PolicyServer. For more information, see *Configure Services on Multiple Endpoints on page 4-20*.

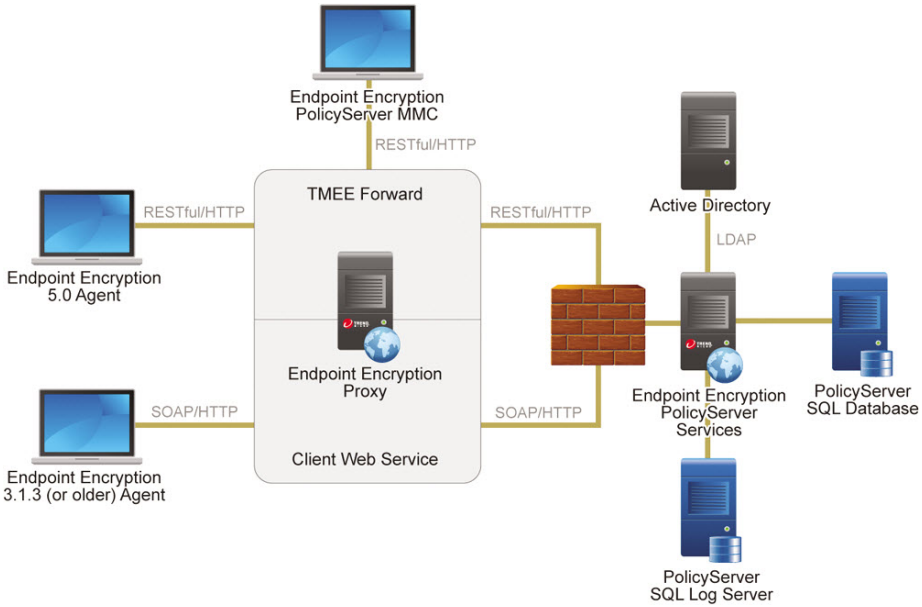


FIGURE 3-5. Complex Distributed Deployment

Scaling Recommendations

Below are recommendations for scaling a single site deployment offering a range of hardware options, accounting for system redundancy and zero point of failure.

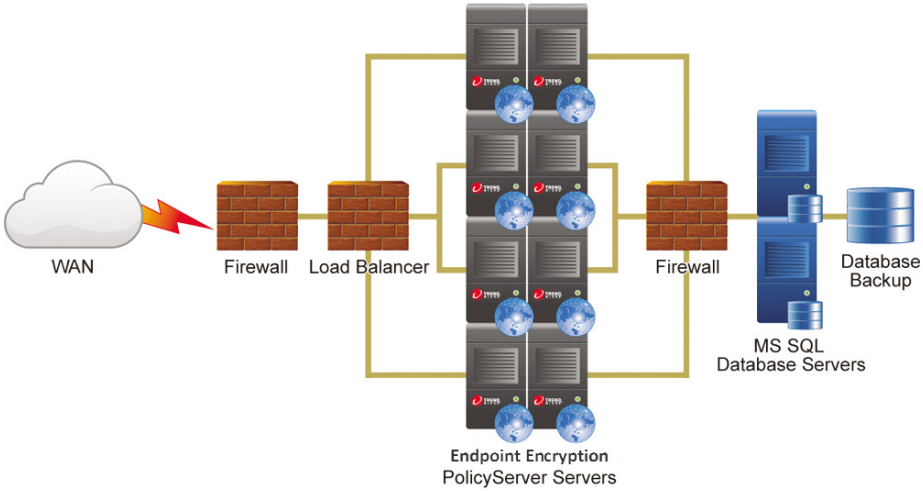


FIGURE 3-6. PolicyServer Scaled to Support 40,000 Users

TABLE 3-4. Scaling with No Redundancy

DEVICES	MINIMUM REQUIREMENTS	
	POLICYSERVER FRONT-END	POLICYSERVER SQL DATABASE
1,500	• PolicyServer and database multi-role server • 2 GHz Quad Core Core2 Intel™ Xeon™ Processors • 8 GB RAM • 120 GB RAID 5 hard disk drive space	• Installed on PolicyServer front-end host

Devices	Minimum Requirements	
	PolicyServer front-end	PolicyServer SQL Database
3,000	• 1 PolicyServer front-end host • 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Processors • 4 GB RAM • 40 GB RAID 1 hard disk drive space	• 1 PolicyServer SQL database host • 2 GHz Quad Core Core2 Intel™ Xeon™ Processors • 8 GB RAM • 100 GB RAID 5 hard disk drive space

Table 3-5. Scaling with Redundancy and High-Availability

Devices	Minimum Requirements	
	PolicyServer front-end	PolicyServer SQL Database
10,000	• 2 PolicyServer front-end hosts • 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Processors • 4 GB RAM • 40 GB RAID 1 hard disk drive space	• 1 PolicyServer SQL database hosts • 2 GHz Quad Core Core2 Intel™ Xeon™ Processors • 8 GB RAM • 120 GB RAID 5 hard disk drive space
20,000	• 4 PolicyServer front-end hosts • 2 GHz Dual Quad Core2 Intel™ Xeon™ Processors • 4 GB RAM • 40 GB RAID 1 hard disk drive space	• 1 PolicyServer SQL database hosts • 2 GHz Quad Core2 Intel™ Xeon™ Processors • 16 GB RAM • 160 GB RAID 5 hard disk drive space

Devices	Minimum Requirements	
	PolicyServer front-end	PolicyServer SQL Database
40,000	• 8 PolicyServer front-end hosts • 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Processors • 4 GB RAM • 40 GB RAID 1 hard disk drive space	• 2 PolicyServer SQL database cluster hosts • 2 GHz Quad Core Core2 Intel™ Xeon™ Processors • 16 GB RAM • 320 GB RAID 5 hard disk drive space

Table 3-6. Scaling with Zero Single Point of Failure

Devices	Minimum Requirements	
	PolicyServer front-end	PolicyServer SQL Database
10,000	• 2 PolicyServer front-end hosts • 2 GHz Quad Core Core2 Intel™ Xeon™ Processors • 4 GB RAM • 40 GB RAID 1 hard disk drive space **Note** Virtual hardware is supported under VMware Virtual Infrastructure.	• 2 PolicyServer SQL database hosts • 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Processors • 8 GB RAM • 60 GB RAID 5 hard disk drive space • 130 GB RAID 5 shared SAN hard disk drive space **Note** Microsoft or VMware on virtual hardware does not support Microsoft Cluster Service.

Devices	Minimum Requirements	
	PolicyServer front-end	PolicyServer SQL Database
20,000	• 4 PolicyServer front-end hosts • 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Processors • 4 GB RAM • 40 GB RAID 1 hard disk drive space **Note** Virtual hardware is supported under VMware Virtual Infrastructure.	• 2 PolicyServer SQL database hosts • 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Processors • 8 GB RAM • 60 GB RAID 5 hard disk drive space • 180 GB RAID 5 shared SAN hard disk drive space **Note** Microsoft or VMware on virtual hardware does not support Microsoft Cluster Service.
40,000	• 8 PolicyServer front-end hosts • 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Processors • 4 GB RAM • 40 GB RAID 1 hard disk drive space **Note** Virtual hardware is supported under VMware Virtual Infrastructure.	• 4 PolicyServer SQL database hosts • 2 GHz Dual Quad Core Core2 Intel™ Xeon™ Processors • 16 GB RAM • 60 GB RAID 5 hard disk drive space • 350 GB RAID 5 shared SAN hard disk drive space **Note** Microsoft or VMware on virtual hardware does not support Microsoft Cluster Service.

Upgrade Deployments

To gain access to new product features or to upgrade older agent software for improved endpoint security, administrators may need to upgrade the Endpoint Encryption PolicyServer and all managed endpoints running any Endpoint Encryption agent. For policy synchronization and information security, make sure to always upgrade PolicyServer before the Endpoint Encryption agents.

This section explains how to safely upgrade Endpoint Encryption, including PolicyServer, PolicyServer MMC, and the Endpoint Encryption agent software to the most current versions. For more information, see *Upgrade Summary of Operations on page 3-26*

Upgrade Considerations

The following illustration shows how the initial upgrade may appear before all Endpoint Encryption agents are upgraded to the Endpoint Encryption 5.0 Patch 3 agent.

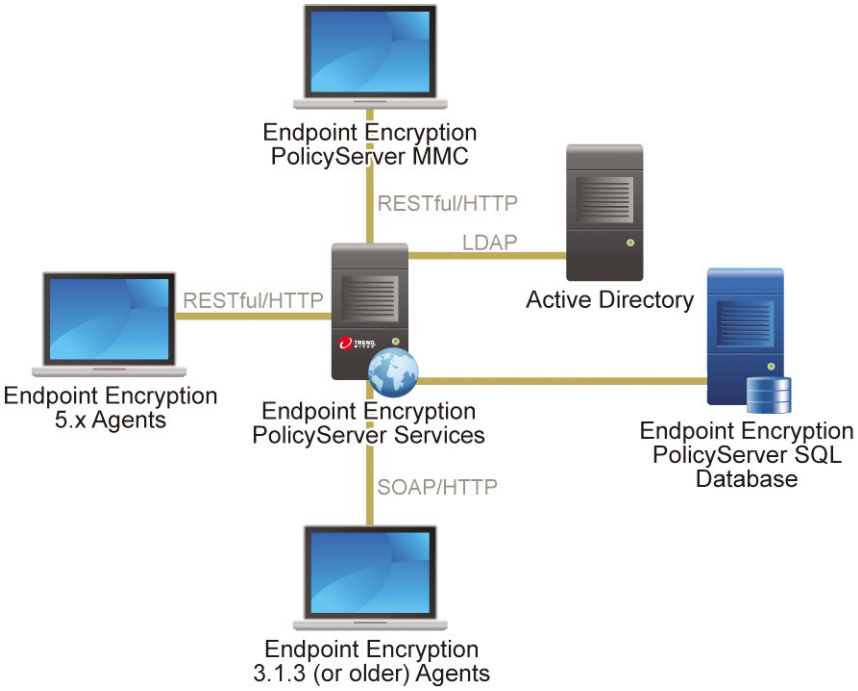


FIGURE 3-7. Endpoint Encryption upgrade deployment

Before upgrading PolicyServer, be aware of the following:

- Make sure to upgrade PolicyServer before upgrading the Endpoint Encryption agents. For information about the correct upgrade order, see *Upgrade Summary of Operations on page 3-26*.
- Upgrading environments with multiple PolicyServer instances has different requirements than in a single PolicyServer environment. For more information, see

Upgrading Multiple PolicyServer Services Connected to the Same Database on page 4-30.

Upgrade Paths

The following table describes the upgrade path from each previous product version to version 5.0 Patch 3. Some older versions cannot upgrade directly to 5.0 Patch 3 and must first upgrade to a newer version of that product. For information about installing legacy versions of Endpoint Encryption products, see the documentation available at:

http://docs.trendmicro.com/en-us/enterprise/endpoint-encryption.aspx

Endpoint Encryption performs in-place upgrades when upgrading directly to version 5.0 Patch 3. For older versions of Endpoint Encryption that require multiple upgrades, you may need to perform reconfiguration for proper agent validation and PolicyServer synchronization.

TABLE 3-7. Upgrade Paths

PRODUCT/AGENT	VERSION	UPGRADE PATH
PolicyServer	5.0 Patch 1	5.0 Patch 1 → 5.0 Patch 3
	5.0	5.0 → 5.0 Patch 3
	3.1.3 SP1	3.1.3 SP1 → 5.0 Patch 3
	3.1.3	3.1.3 → 5.0 Patch 3
	3.1.2	3.1.2 → 5.0 → 5.0 Patch 3
Full Disk Encryption	5.0 Patch 1	5.0 Patch 1 → 5.0 Patch 3
	5.0	5.0 → 5.0 Patch 3
	3.1.3 SP1	3.1.3 SP1 → 5.0 Patch 3
	3.1.3	3.1.3 → 5.0 Patch 3

Product/Agent	Version	Upgrade Path
MobileArmor Full Disk Encryption Product	3.1.2	3.1.2 → Full Disk Encryption 5.0 → Full Disk Encryption 5.0 Patch 3
	SP7g	SP7g → 3.1.3 → Full Disk Encryption 5.0 → Full Disk Encryption 5.0 Patch 3
	SP7-SP7f	SP7-SP7f → SP7g → 3.1.3 → Full Disk Encryption 5.0 → Full Disk Encryption 5.0 Patch 3
File Encryption	5.0 Patch 1	5.0 Patch 1 → 5.0 Patch 3
	5.0	5.0 → 5.0 Patch 3
FileArmor	3.1.3 SP1	FileArmor 3.1.3 SP1 → File Encryption 5.0 → File Encryption 5.0 Patch 3
	3.1.3	FileArmor 3.1.3 → File Encryption 5.0 → File Encryption 5.0 Patch 3
	3.0.14	FileArmor 3.0.14 → FileArmor 3.1.3 → File Encryption 5.0 → File Encryption 5.0 Patch 3
	3.0.13	FileArmor 3.0.13 → FileArmor 3.1.3 → File Encryption 5.0 → File Encryption 5.0 Patch 3
Encryption Management for Microsoft BitLocker	5.0 Patch 1	5.0 Patch 1 → 5.0 Patch 3
	5.0	5.0 → 5.0 Patch 3
Encryption Management for Apple FileVault	5.0 Patch 1	5.0 Patch 1 → 5.0 Patch 3
	5.0	5.0 → 5.0 Patch 3
OfficeScan Plug-in Service (Full Disk Encryption Deployment Tool)	5.0 Patch 1	5.0 Patch 1 → 5.0 Patch 3
	5.0	5.0 → 5.0 Patch 3
Control Manager widgets	5.0 Patch 1	5.0 Patch 1 → 5.0 Patch 3
	5.0	5.0 → 5.0 Patch 3
DriveArmor	3.0	Not supported.

Product/Agent	Version	Upgrade Path
KeyArmor	3.0.2	There is no KeyArmor 5.0 version.
	3.0.1	

Supported Agent Versions

Although PolicyServer supports policy management for all agents, older agents cannot register as a new device in PolicyServer 5.0 Patch 3 or Control Manager. The following table explains which legacy versions can register as a new device. Trend Micro recommends using the newest versions of all agents.

Table 3-8. Supported Legacy Agents for New Devices

Agent	Version	Can Register as a New Device	Policies Supported
Full Disk Encryption	5.0 Patch 1	●	●
	5.0	●	●
	3.1.3 SP1	●	●
	3.1.3	●	●
MobileArmor Full Disk Encryption Product	3.1.2		
	SP7g		
File Encryption	5.0 Patch 1	●	●
	5.0	●	●
FileArmor	3.1.3	●	●
	3.0.14		
	3.0.13		

Agent	Version	Can Register as a New Device	Policies Supported
Encryption Management for Microsoft BitLocker	5.0 Patch 1	●	●
	5.0	●	●
Encryption Management for Apple FileVault	5.0 Patch 1	●	●
	5.0	●	●
DriveArmor	3.0		
KeyArmor	3.02		●*

Note

*Only supported on PolicyServer upgrades from Endpoint Encryption 3.1.2 or 3.1.3

Upgrade Summary of Operations

To reduce the risk of endpoints losing connection to PolicyServer, upgrade the environment in the following order. If the agent cannot connect to PolicyServer after the upgrade, manually run the upgrade installer on the endpoint.

Procedure

1. Review the new system requirements.

   See *System Requirements on page 2-1*.

2. Review the upgrade path for the currently installed PolicyServer and Endpoint Encryption agents.

3. Make sure that Endpoint Encryption 5.0 Patch 3 supports the upgrade.

   See *Supported Agent Versions on page 3-25*.

4. Upgrade PolicyServer.

   See *Upgrade Considerations on page 3-22*.

See *Upgrading PolicyServer on page 4-27*.

5. Optionally install and configure Control Manager.

   See *OfficeScan Integration on page 7-1*.

6. Optionally install and configure OfficeScan.

   See *Control Manager Integration on page 5-1*.

7. Upgrade Endpoint Encryption agents.

   See *Upgrade on page 6-46*.

Chapter 4

PolicyServer Deployment

This chapter provides an overview of the required files and accounts to install PolicyServer and the installation process.

Note

For system requirements, see *PolicyServer Requirements on page 2-2*.

Topics include:

- *About PolicyServer on page 1-14*
- *PolicyServer Requirements on page 2-2*
- *Trial License on page 8-3*
- *PolicyServer Installation and Configuration on page 4-3*
- *Upgrade on page 4-23*
- *Migration to Control Manager on page 4-31*
- *Uninstallation on page 4-31*

About PolicyServer

Trend Micro PolicyServer manages encryption keys and synchronizes policies across all endpoints in the organization. PolicyServer also enforces secure authentication and provides real-time auditing and reporting tools to ensure regulatory compliance. You can flexibly manage PolicyServer with PolicyServer MMC or with Trend Micro Control Manager. Other data management features include user-based self-help options and device actions to remotely reset or "kill" a lost or stolen device.

The following table describes the PolicyServer components that you can deploy on one server or multiple servers, depending on environmental needs.

TABLE 4-1. PolicyServer Components

COMPONENT	DESCRIPTION
Enterprise	The Endpoint Encryption Enterprise is the unique identifier about the organization in the PolicyServer database configured when installing PolicyServer. One PolicyServer database may have one Enterprise configuration.
Database	The PolicyServer Microsoft SQL database securely stores all user, device, and log data. The database is either configured on a dedicated server or added to an existing SQL cluster. The log and other databases can reside separately.
PolicyServer Windows Service	PolicyServer Windows Service manages all communication transactions between the host operating system, Endpoint Encryption Service, Legacy Web Service, Client Web Proxy, and SQL databases.
Endpoint Encryption Service	All Endpoint Encryption 5.0 Patch 3 agents use Endpoint Encryption Service to communicate with PolicyServer. Endpoint Encryption Service uses a Representational State Transfer web API (RESTful) with an AES-GCM encryption algorithm. After a user authenticates, PolicyServer generates a token related to the specific policy configuration. Until the Endpoint Encryption user authenticates, the service denies all policy transactions. To create a three level network topography, the service can also be separately deployed to an endpoint residing in the network DMZ, which allows PolicyServer to safely reside behind the firewall.

Component	Description
Legacy Web Service	All Endpoint Encryption 3.1.3 and older agents use Simple Object Access Protocol (SOAP) to communicate with PolicyServer. Under certain situations, SOAP may allow insecure policy transactions without user authentication. Legacy Web Service filters SOAP calls by requiring authentication and limiting the commands that SOAP accepts. To create a three level network topography, the service can also be separately deployed to an endpoint residing in the network DMZ, which allows PolicyServer to safely reside behind the firewall.

PolicyServer Installation and Configuration

This section explains how to install and configure PolicyServer for the first time, how to set up Active Directory, and how to configure the LDAP proxy.

Installing PolicyServer

The PolicyServer installation process involves running an installer on the server endpoint to configure the following:

- Endpoint Encryption product license
- Enterprise name and Administrator logon
- Endpoint Encryption services
- PolicyServer database
- PolicyServer MMC (optional)

Note

For information about the architecture, see *Endpoint Encryption Components on page 1-11*. PolicyServer MMC can optionally be installed at the same time.

WARNING!

For security reasons, legacy Endpoint Encryption agents cannot communicate directly with a PolicyServer instance residing in a different network. For information about configuring a web proxy, see *Configure Services on Multiple Endpoints on page 4-20*.

Procedure

1. Verify that all system requirements are met.

   See *PolicyServer Requirements on page 2-2*.

2. Run `PolicyServerInstaller.exe`

   The PolicyServer Installer opens.

3. At the **PolicyServer Services** screen, click **Install** at the right.

4. At the **Product Legal Notice** screen, read the license agreement and accept the terms by clicking **Accept**.

5. The **Product Activation** screen, do the following:

   - Click **Register Online** to go to register the license.
   - Select **Use a full license** to specify the Activation Code and have full functionality.
   - Select **Use a trial license** to evaluate a managed Endpoint Encryption configuration for 30 days.

   Note

   During the trial period, PolicyServer functions normally with all agent management, unlimited devices, and up to 100 users. After 30 days, contact a Trend Micro representative for more information about the Registration Key and Activation Code. For more information, about converting the trial license to a full license, see *Activating the New Product License on page 8-3*.

6. At the **Create Enterprise Name and Administrator Logon** screen, specify the following credentials that are used to manage PolicyServer from the PolicyServer MMC or Control Manager.

Option	Description
Enterprise Name	The name of the database instance.
Administrator	The new Enterprise Administrator account user name.
Password	The new Enterprise Administrator account password.
Confirm Password	Confirm the new Enterprise Administrator account password.

7. Click **Continue**.
8. At the **Windows Service Logon** screen, click **Continue**. The default settings are appropriate for most environments.
9. At the **Database Administrator Logon** screen, do the following:
   - Select **Microsoft SQL Express** to create a new database instance.

     Note

     Microsoft SQL Express is only available in environments that do not have SQL Server configured.

   - Select **SQL Server** to specify a Microsoft SQL Server instance, and then specify the following parameters:
     - **SQL Server**: The SQL Server hostname or IP address.

       Note

       For environments with multiple SQL Server instances, append the SQL instance to the end of the PolicyServer hostname or IP address used. Use the following syntax to specify an instance:

       `<hostname_or_IP_address>\<database_instance>`

     - **User name**: The user name with the **sysadmin** role for the specified SQL Server instance.
     - **Password**: The password for the **sysadmin** account.
   - Select **Use a different log database server** to specify a different SQL Server instance for log data.

10. Click **Continue**.

    The installer verifies the database connection.

11. At the **Create Database Logon** screen, specify a new database account for the PolicyServer Windows Service to use for all database transactions.

> **Note**
>
> Do not specify the **sysadmin** account.

12. At the **Endpoint Encryption Service** screen, specify the following parameters:

Option	Description
Port number	Specify the port number that the PolicyServer MMC, Control Manager and Endpoint Encryption 5.0 Patch 3 agents use to communicate with PolicyServer (default: 8080). **Note** In environments with legacy agents, Trend Micro recommends using port 8080 for the Admin Web Service and port 80 for the Client Web Service. The port number must be a positive integer between 1 and 65535.
Automatically generate a new self-signed certificate	Select this option if no certificate is available. The installer generates a certificate for communication.
Specify an existing certificate	Select this option to use a specific certificate. There are no limitations or requirements for specifying an existing certificate except that the certificate is correctly formatted.

> **Note**
>
> Endpoint Encryption Service uses a RESTful web API to authenticate agents connecting to PolicyServer.

13. Click **Continue**.

14. At the **Legacy Agent Service** screen, select the location that legacy Endpoint Encryption agents (version 3.1.3 and below) use to communicate with PolicyServer, then click **Continue**.

15. To immediately install PolicyServer MMC, click **Yes**. To install PolicyServer MMC at a later time or on a separate endpoint, see *Installing PolicyServer MMC on page 4-8*.

    The installation process begins.

16. When prompted, click **OK**.

17. Click **Finished**.

18. Click **Exit** to close the PolicyServer installer.

19. Restart the server.

20. Add the initial Endpoint Encryption users and groups.

    See *Configuring PolicyServer on page 4-7*.

Configuring PolicyServer

The following procedure explains how to configure the PolicyServer Enterprise with the PolicyServer MMC. The Enterprise and Enterprise Administrator logon were configured during PolicyServer installation.

Note

For information about the management consoles available in Endpoint Encryption, see *Management Consoles on page 1-16*.

Procedure

1. If not set up during PolicyServer installation, install PolicyServer MMC.

   See *Installing PolicyServer MMC on page 4-8*.

2. Log on to PolicyServer MMC.

See *Installing PolicyServer MMC on page 4-8*.

3. Add the first Top Group.

   See *Adding a Top Group on page 4-11*.

4. Add Endpoint Encryption users.

   See *Adding a New User to a Group on page 4-13*.

5. Allow certain Endpoint Encryption users to install new Endpoint Encryption devices to the group.

   See *Allowing a User to Install to a Group on page 4-15*.

Installing PolicyServer MMC

The PolicyServer MMC can optionally be installed during the PolicyServer installation. For environments that do not collocate PolicyServer MMC and PolicyServer, follow this procedure to install the PolicyServer MMC.

Note

Due to improved security, it is not possible to use legacy versions of the PolicyServer MMC to manage PolicyServer 5.0 Patch 3.

Procedure

1. Run `PolicyServer MMCSnapinSetup.msi`.

   The installation begins.

2. Click **Next** to begin the Setup Wizard.

3. Read the license agreement and accept the terms by selecting **I Agree** and then clicking **Next**.

4. Select installation folder or leave at default location, and click **Next**.

5. Click **Next** to confirm installation.

   After the installation completes, note the following:

- A new PolicyServer MMC shortcut appears on the desktop:

FIGURE 4-1. PolicyServer PolicyServer MMC shortcut

- Depending on the processor, the program files are installed at `C:\Program Files\Trend Micro\PolicyServer MMC\` or `C:\Program Files (x86)\Trend Micro\PolicyServer MMC\`

6. Click **Close** to finish.
7. Click **Yes** to restart the server.
8. After logging back on the server, double-click the PolicyServer MMC shortcut on the desktop.
9. Once PolicyServer MMC opens, authenticate using the Enterprise and Enterprise Administrator account created when the PolicyServer databases and services were installed. The 30-day trial period allows for unlimited devices and up to 100 users.

See the *Endpoint Encryption Administrator's Guide* for additional post-installation tasks such as creating devices and users, and setting up policies.

Tip

Trend Micro recommends creating a backup Enterprise Administrator account and changing the default password.

Logging on to PolicyServer MMC

Configure the Enterprise name and the Enterprise Administrator account during PolicyServer installation. For information about the free 30-day Trial License, see *Trial License on page 8-3*.

Procedure

1. To open PolicyServer MMC, do one of the following:

   - Double-click the **PolicyServer MMC** shortcut on the desktop
   - Go to the folder specified during installation, then double-click `PolicyServer MMC.exe`

   The PolicyServer MMC authentication screen appears.

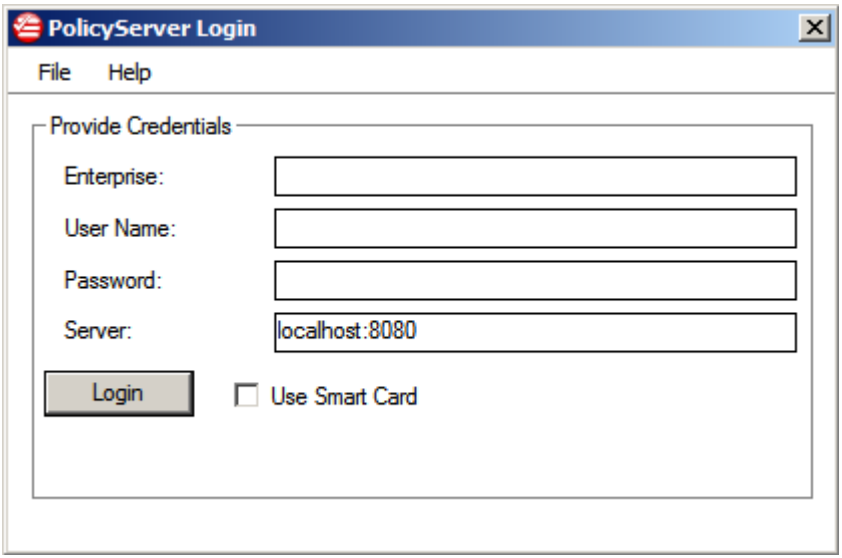


FIGURE 4-2. The PolicyServer MMC Authentication Screen

2. Specify the following parameters:

OPTION	DESCRIPTION
Enterprise	Specify the Enterprise.
User name	Specify the user name of an Enterprise Administrator account.
Password	Specify the password for the user name.

Option	Description
Server	Specify the PolicyServer IP address or host name, and include the port number assigned to that configuration.

3. Optional: To use a smart card to authenticate, select **Use Smart Card**.
4. Click **Login**.
5. Wait for PolicyServer MMC to connect to PolicyServer.

The PolicyServer MMC opens.

Adding a Top Group

Groups simplify managing Endpoint Encryption agents, users, policies, subgroups, and devices. A Top Group is the highest level group.

Note

It is not possible to add the Enterprise Administrator or Enterprise Authenticator accounts to groups. To create a Group Administrator, add a user and change the account permissions within the group.

Procedure

1. Right-click the Enterprise in the left pane, then click **Add Top Group**.

The **Add New Group** screen appears.

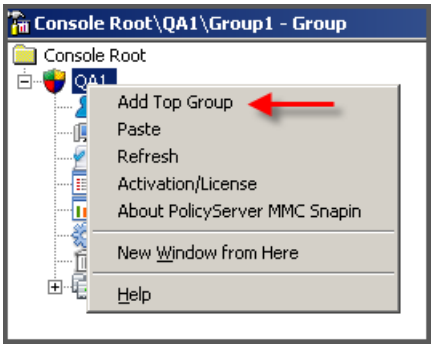


FIGURE 4-3. Add Top Group Screen

2. Specify the name and description for the group.
3. If using Endpoint Encryption devices that do not support Unicode, select **Support Legacy Devices**.

Note

Some legacy devices may not be able to communicate with PolicyServer using Unicode. Assign Unicode and legacy Endpoint Encryption devices to different groups.

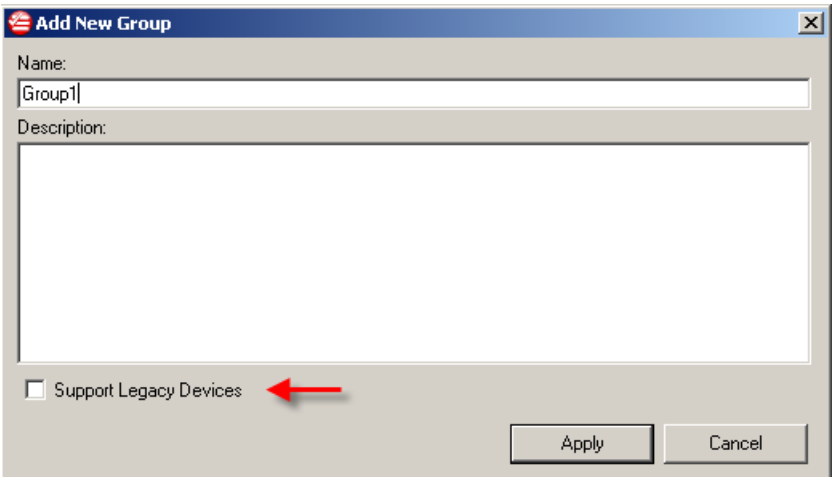


FIGURE 4-4. Add New Group Screen

4. Click **Apply**.
5. At the confirmation message, click **OK**.

   The new group is added to the tree structure in the left pane.

Adding a New User to a Group

Note

Adding a user to the Enterprise does not assign the user to any groups

Adding a user to a group adds the user to the group and to the Enterprise

Procedure

1. Expand the group and open **Users**.
2. Go to the right pane and right-click the whitespace, then select **Add New User**.

The **Add New User** screen appears.

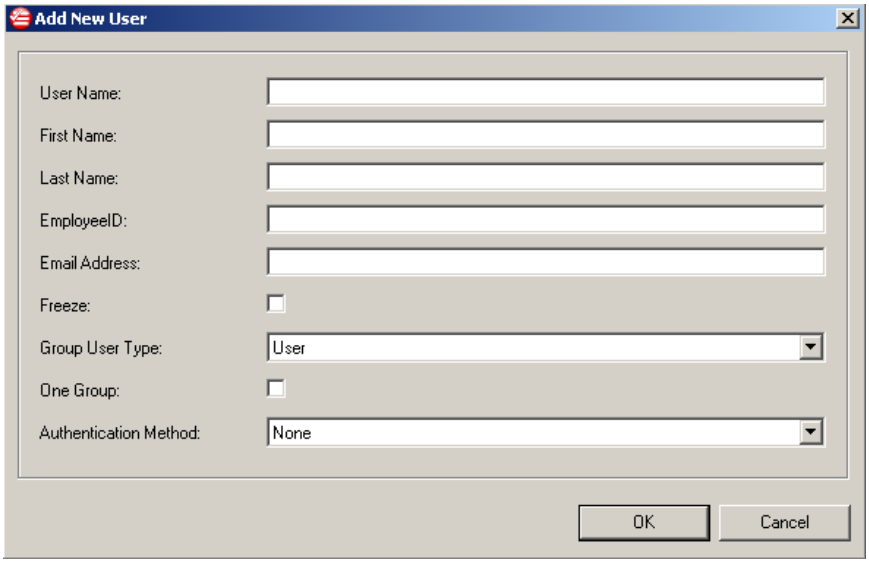


FIGURE 4-5. Add New User Screen

3. Specify the following options:

OPTION	DESCRIPTION
User name	Specify the user name for the new user account (required).
First name	Specify the first name for the new user account (required).
Last name	Specify the last name for the new user account (required).
EmployeeID	Specify the employee ID for the new user account (optional).
Freeze	Select whether to temporarily disable the new user account (optional). While frozen, the user is unable to log devices.
Group User Type	Select the privileges of the new account.

Option	Description
	Note For information about account roles, see *Endpoint Encryption User Roles on page 1-21*. Options include: • User • Authenticator • Administrator **Note** It is not possible to add Enterprise Administrator or Enterprise Authenticator accounts to groups.
One Group	Select whether the new user account is allowed to be a member of multiple group policies.
Authentication method	Select the method that the new user account uses to log on to Endpoint Encryption devices. **Note** The default authentication method for users is **None**.

4. Click **OK**.

   The new user is added to the selected group and to the Enterprise. The user can now log on to Endpoint Encryption devices.

Allowing a User to Install to a Group

Before installing the agents, allow at least one user in a group to install agents.

Procedure

1. Expand the group, open **Users**.

2. Right-click the user account and then select **Allow User to Install to This Group**.

PolicyServer Active Directory Synchronization

PolicyServer supports Active Directory (AD) synchronization for a configured PolicyServer group. Synchronization will automatically add and remove AD users from configured PolicyServer groups.

Active Directory Overview

Three items are required to enable PolicyServer AD synchronization:

1. A configured AD domain.
2. A PolicyServer group configured to point to one or more valid AD organizational units (OUs).
3. Appropriate credentials to access the AD domain that match the PolicyServer group's distinguished name.

When configured properly, synchronization automatically creates new PolicyServer users and moves them to the appropriate paired groups on PolicyServer. During synchronization, PolicyServer is updated to reflect current users and group assignments for paired groups.

Adding a new user to the domain and placing that user in an organizational unit will flag that user so that during the next synchronization, AD will create that user in PolicyServer and then move that user into the appropriate paired PolicyServer group.

Deleting a user from AD will automatically remove that user from a PolicyServer paired group and from the enterprise.

To add non-domain users to groups that are synchronized with the domain, you can create unique Endpoint Encryption users and add them to paired PolicyServer groups without having those users modified by the synchronization system.

If you remove the Endpoint Encryption user from a paired group in PolicyServer, that domain user will not automatically be re-added by the synchronization system. This prevents overriding the your action for this Endpoint Encryption user. If you manually

move a synchronized domain user back into a paired group then the synchronization system will again begin to automatically maintain the user in the group.

Configuring Active Directory

This task assumes the domain controller is set up on Windows Server 2012 and that Active Directory (AD) is installed.

Procedure

1. Go to **Start** > **Administrative Tools** > **Active Directory Users and Computers**.

   The **Active Directory Users and Computer** screen appears.

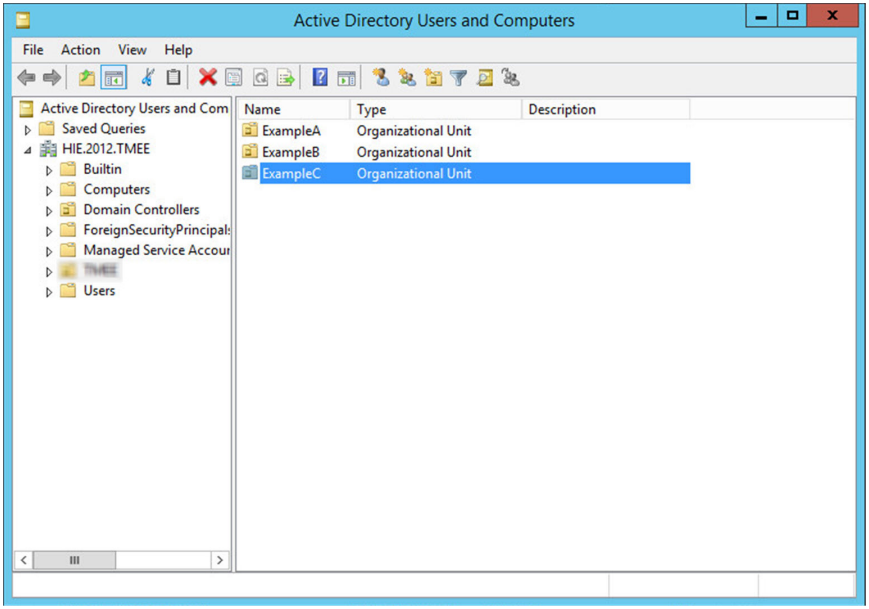


FIGURE 4-6. Active Directory Users and Computers

2. Create your organizational units (OUs).

   For each OU you intend to create, perform the following steps:

a. Right-click the new domain created when AD was installed and then select **New**.

b. Select **Organizational Unit**.

c. From the **New Object - Organizational Unit** screen, specify the new name and click **OK**.

The new group appears in the left navigation under the domain name. Perform this step for as many organizational units you intend to use with PolicyServer.

Important

Endpoint Encryption supports up to 12 OUs per policy.

The new groups will be used to synchronize with a PolicyServer group. Before synchronization, users must be added to the groups.

3. Add new users to your OUs.

For each user you intend to create, perform the following steps:

a. Right-click the intended OU and go to **New** > **User**.

b. From the **New Object - User** screen, specify the new user's account information and click **Next**.

c. Specify and confirm the new user's domain password and click **Next**.

Note

Clear **User must change password at next login** and select the **Password never expires** option to simplify other testing later.

d. When prompted to complete, click **Finish**.

The domain controller is configured with a new OU and a user in that group. To synchronize that group with PolicyServer, install PolicyServer and create a group for synchronization. This next section assumes that PolicyServer is already installed.

4. Log on to PolicyServer MMC.

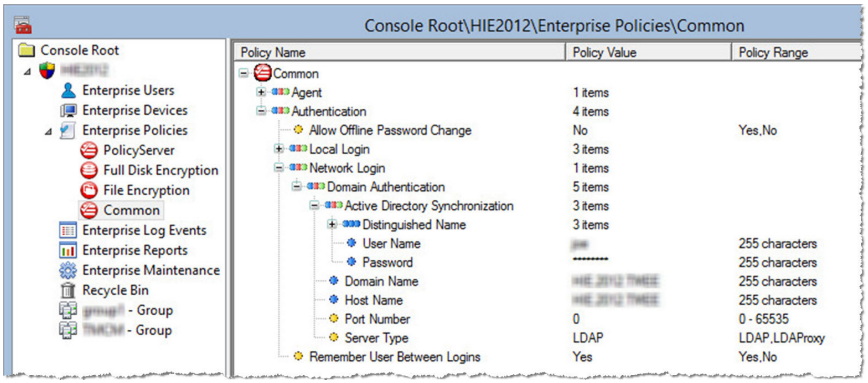
5. Set your enterprise as a top level group.

   a. Right-click the enterprise and select **Create Top level Group**.

   b. Specify the name and description for the group.

   c. Click **Apply**.

6. To configure the synchronization policy, open the group and go to **Enterprise Policies** > **Common** > **Authentication** > **Network Login** > **Domain Authentication** > **Active Directory Synchronization**.



7. Add the distinguished name for each OU you intend to synchronize.

   For each OU to synchronize, perform the following steps:

   a. Right-click **Distinguished Name** and click **Add**.

   b. In the **Policy Value** section, specify the OU by its sequence of relative distinguished names (RDN) separated by commas.

      Example: OU=TW, DC=mycompany, DC=com

   c. After specifying the OU distinguished name, click **OK**.

8. Open **Domain Name** and specify the NetBIOS domain name that was used to configure the AD server.

9. Open **Host Name** and specify the host name of the AD server.

   Synchronization between the AD and PolicyServer is complete. Synchronization automatically occurs every 45 minutes (this is the default synchronization interval used by Microsoft domain controllers). You may force synchronization by stopping and restarting the PolicyServer Windows service. Domain synchronization runs shortly after the PolicyServer Windows service startup occurs and then subsequently runs every 45 minutes.

Configure Services on Multiple Endpoints

To create a three level network topography, separately deploy services to an endpoint residing in the network DMZ, and configure PolicyServer safely behind the firewall. You can install Client Web Proxy on the separate endpoint to work as a proxy either forwarding or forwarding and filtering traffic. Client Web Proxy manages the following services:

Traffic Forwarding Service

Use Traffic Forwarding Service to forward all traffic from the Endpoint Encryption 5.0 Patch 3 agents to the associated PolicyServer. It communicates with Endpoint Encryption Service on that PolicyServer.

Client Web Service

Use Client Web Service to forward all traffic from legacy Endpoint Encryption agents (3.1.3 and below) to the associated PolicyServer. It communicates with PolicyServer Windows Service on that PolicyServer. In addition to forwarding traffic, Client Web Service also filters the traffic to prevent security threats.

For more information about services, see *About PolicyServer on page 1-14*.

About Traffic Forwarding Service

Use Traffic Forwarding Service in environments that have Endpoint Encryption 5.0 Patch 3 agents and PolicyServer residing in different local area networks. Endpoint Encryption 5.0 Patch 3 agents communicate using RESTful. Traffic Forwarding Service sits between the agents and PolicyServer to prevent insecure policy access. The Traffic

Forwarding Service installer configures TMEEservice service, which is the same RESTful service installed by the PolicyServer installer in environments that do not use a proxy.

Note

- It is not possible to install Traffic Forwarding Service and PolicyServer on the same endpoint
- The default port is 8080

About Client Web Service

Use Client Web Service in environments that have legacy Endpoint Encryption agents (3.1.3 and older) and PolicyServer residing in different local area networks. Legacy Endpoint Encryption agents communicate using SOAP. Client Web Service sits between the legacy Endpoint Encryption agents and the PolicyServer Windows Service to prevent insecure policy access. The Client Web Service installer configures MAWebService2 (Legacy Web Service), which is the same Microsoft IIS service installed by the PolicyServer installer in environments that do not use a proxy.

Note

- It is not possible to install Client Web Service and PolicyServer on the same endpoint.
- The default port for Endpoint Encryption 3.1.3 or below agents is 8080.
- In environments running using both new and legacy Endpoint Encryption, make to configure different ports for each proxy service communicating with PolicyServer.

Configuring Client Web Proxy

Note

Make sure to install PolicyServer on a different endpoint.

Procedure

1. Copy the PolicyServer installation folder to the local hard drive.
2. Open the **Tools** folder and run `TMEEProxyInstaller.exe`.

   The welcome screen appears.
3. Click **Continue**.

   The Client Web Proxy installer analyzes the endpoint.
4. Specify the PolicyServer IP address or host name and the port number of the Endpoint Encryption Service of the target PolicyServer.

   Note

   The default is `localhost:8080`.
5. Click **Continue**.

   The installation begins.
6. Wait for Client Web Proxy to install.
7. Click **Finish**.
8. Verify the Client Web Proxy installation.
   a. Go to **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

      The **Internet Information Services (IIS) Manager** screen appears.

   b. Find the previously configured site location.

   c. Verify that **MAWebService2** is configured.
9. Verify the Traffic Forwarding Service installation.
   a. Go to **Start** > **Administrative Tools** > **Services**.

      The **Services** screen appears.

   b. Make sure that **TMEEForward** service has started.

Traffic Forwarding Service is installed.

Upgrade

To gain access to new product features or to upgrade older agent software for improved endpoint security, administrators may need to upgrade the Endpoint Encryption PolicyServer and all managed endpoints running any Endpoint Encryption agent. For policy synchronization and information security, make sure to always upgrade PolicyServer before the Endpoint Encryption agents.

This section explains how to safely upgrade Endpoint Encryption, including PolicyServer, PolicyServer MMC, and the Endpoint Encryption agent software to the most current versions. For more information, see *Upgrade Summary of Operations on page 3-26*

WARNING!

Before upgrading the agent, make sure to first upgrade PolicyServer to version 5.0 Patch 3. Endpoint Encryption 5.0 Patch 3 agents cannot communicate with PolicyServer 3.1.3 or earlier.

Upgrade Paths

The following table describes the upgrade path from each previous product version to version 5.0 Patch 3. Some older versions cannot upgrade directly to 5.0 Patch 3 and must first upgrade to a newer version of that product. For information about installing legacy versions of Endpoint Encryption products, see the documentation available at:

http://docs.trendmicro.com/en-us/enterprise/endpoint-encryption.aspx

Endpoint Encryption performs in-place upgrades when upgrading directly to version 5.0 Patch 3. For older versions of Endpoint Encryption that require multiple upgrades, you may need to perform reconfiguration for proper agent validation and PolicyServer synchronization.

TABLE 4-2. Upgrade Paths

PRODUCT/AGENT	VERSION	UPGRADE PATH
PolicyServer	5.0 Patch 1	5.0 Patch 1 → 5.0 Patch 3
	5.0	5.0 → 5.0 Patch 3
	3.1.3 SP1	3.1.3 SP1 → 5.0 Patch 3
	3.1.3	3.1.3 → 5.0 Patch 3
	3.1.2	3.1.2 → 5.0 → 5.0 Patch 3
Full Disk Encryption	5.0 Patch 1	5.0 Patch 1 → 5.0 Patch 3
	5.0	5.0 → 5.0 Patch 3
	3.1.3 SP1	3.1.3 SP1 → 5.0 Patch 3
	3.1.3	3.1.3 → 5.0 Patch 3
MobileArmor Full Disk Encryption Product	3.1.2	3.1.2 → Full Disk Encryption 5.0 → Full Disk Encryption 5.0 Patch 3
	SP7g	SP7g → 3.1.3 → Full Disk Encryption 5.0 → Full Disk Encryption 5.0 Patch 3
	SP7-SP7f	SP7-SP7f → SP7g → 3.1.3 → Full Disk Encryption 5.0 → Full Disk Encryption 5.0 Patch 3
File Encryption	5.0 Patch 1	5.0 Patch 1 → 5.0 Patch 3
	5.0	5.0 → 5.0 Patch 3
FileArmor	3.1.3 SP1	FileArmor 3.1.3 SP1 → File Encryption 5.0 → File Encryption 5.0 Patch 3
	3.1.3	FileArmor 3.1.3 → File Encryption 5.0 → File Encryption 5.0 Patch 3
	3.0.14	FileArmor 3.0.14 → FileArmor 3.1.3 → File Encryption 5.0 → File Encryption 5.0 Patch 3
	3.0.13	FileArmor 3.0.13 → FileArmor 3.1.3 → File Encryption 5.0 → File Encryption 5.0 Patch 3

PRODUCT/AGENT	VERSION	UPGRADE PATH
Encryption Management for Microsoft BitLocker	5.0 Patch 1	5.0 Patch 1 → 5.0 Patch 3
	5.0	5.0 → 5.0 Patch 3
Encryption Management for Apple FileVault	5.0 Patch 1	5.0 Patch 1 → 5.0 Patch 3
	5.0	5.0 → 5.0 Patch 3
OfficeScan Plug-in Service (Full Disk Encryption Deployment Tool)	5.0 Patch 1	5.0 Patch 1 → 5.0 Patch 3
	5.0	5.0 → 5.0 Patch 3
Control Manager widgets	5.0 Patch 1	5.0 Patch 1 → 5.0 Patch 3
	5.0	5.0 → 5.0 Patch 3
DriveArmor	3.0	Not supported.
KeyArmor	3.0.2	There is no KeyArmor 5.0 version.
	3.0.1	

Supported Agent Versions

Although PolicyServer supports policy management for all agents, older agents cannot register as a new device in PolicyServer 5.0 Patch 3 or Control Manager. The following table explains which legacy versions can register as a new device. Trend Micro recommends using the newest versions of all agents.

TABLE 4-3. Supported Legacy Agents for New Devices

AGENT	VERSION	CAN REGISTER AS A NEW DEVICE	POLICIES SUPPORTED
Full Disk Encryption	5.0 Patch 1	●	●
	5.0	●	●
	3.1.3 SP1	●	●
	3.1.3	●	●
MobileArmor Full Disk Encryption Product	3.1.2		
	SP7g		
File Encryption	5.0 Patch 1	●	●
	5.0	●	●
FileArmor	3.1.3	●	●
	3.0.14		
	3.0.13		
Encryption Management for Microsoft BitLocker	5.0 Patch 1	●	●
	5.0	●	●
Encryption Management for Apple FileVault	5.0 Patch 1	●	●
	5.0	●	●
DriveArmor	3.0		
KeyArmor	3.02		●*

Note

*Only supported on PolicyServer upgrades from Endpoint Encryption 3.1.2 or 3.1.3

Upgrading PolicyServer

Upgrade PolicyServer to gain access to server enhancements and new security features available in the latest product version. During the upgrade, PolicyServer services are temporarily stopped. However, there is no interruption to Endpoint Encryption device access. Existing policy configurations are maintained.

Note

For information about fresh installs, see *Installing PolicyServer on page 4-3*.

For information about the architecture, see *Endpoint Encryption Components on page 1-11*. PolicyServer MMC can optionally be installed at the same time.

WARNING!

For security reasons, legacy Endpoint Encryption agents cannot communicate directly with a PolicyServer instance residing in a different network. For information about configuring a web proxy, see *Configure Services on Multiple Endpoints on page 4-20*.

Procedure

1. Verify that all system requirements are met.

   See *PolicyServer Requirements on page 2-2*.

2. Run `PolicyServerInstaller.exe`

   The PolicyServer Installer opens.

3. At the **Product Legal Notice** screen, read the license agreement and accept the terms by clicking **Accept**.

4. Verify the PolicyServer version and then click **Upgrade**.

   Make sure to follow the correct upgrade path for PolicyServer. For more information, see *Upgrade Paths on page 3-23*.

5. At the **License Registration** message, click **OK** to continue.

6. At the **Windows Service Logon** screen, click **Continue**. The default settings are appropriate for most environments.

7. At the **Database Administrator Logon** screen, provide the following in the **Primary Database** section:

Option	Description
Server	The Microsoft SQL Server hostname (localhost) or IP address.
User name	The user name with the **sysadmin** role for the specified Microsoft SQL Server.
Password	The password for the **sysadmin** account.

Note

For environments with multiple SQL Server instances, append the SQL instance to the end of the PolicyServer hostname or IP address used. Use the following syntax to specify an instance:

```
<hostname_or_IP_address>\<database_instance>
```

The installer verifies the database connection.

8. At the **PolicyServer Question** message, do one of the following:

- Click **Yes** to back up existing data
- Click **No** to overwrite existing data

9. At the **Endpoint Encryption Service** screen, specify the following parameters:

Option	Description
Port number	Specify the port number that the PolicyServer MMC, Control Manager and Endpoint Encryption 5.0 Patch 3 agents use to communicate with PolicyServer (default: 8080). **Note** In environments with legacy agents, Trend Micro recommends using port 8080 for the Admin Web Service and port 80 for the Client Web Service. The port number must be a positive integer between 1 and 65535.

Option	Description
Automatically generate a new self-signed certificate	Select this option if no certificate is available. The installer generates a certificate for communication.
Specify an existing certificate	Select this option to use a specific certificate. There are no limitations or requirements for specifying an existing certificate except that the certificate is correctly formatted.

Note

Endpoint Encryption Service uses a RESTful web API to authenticate agents connecting to PolicyServer.

10. At the **Legacy Agent Service** screen, select the location that legacy Endpoint Encryption agents (version 3.1.3 and below) use to communicate with PolicyServer, then click **Continue**.

11. Click **Yes** to install PolicyServer MMC.

WARNING!

The PolicyServer installer can automatically install a version of PolicyServer MMC that supports the management of the product. PolicyServer 5.0 Patch 3 does not support older versions of PolicyServer MMC. Only click **No** if another endpoint with PolicyServer MMC 5.0 Patch 3 installed manages PolicyServer.

The installation process begins.

12. At the **PolicyServer Installation** message, click **OK**.

13. Click **Finished**.

14. From the PolicyServer Installer window, click **Exit**.

15. Restart the server.

Upgrading Multiple PolicyServer Services Connected to the Same Database

Only one PolicyServer can perform the database upgrade at a time.

Procedure

1. Stop the PolicyServer Windows Service on all PolicyServer instances except the one to upgrade.

   a. Go to **Start** > **Administrative Tools** > **Services**.

   b. Right-click **PolicyServer Windows Service** and then select **Stop**.

2. Perform the upgrade on the active server.

   See *Upgrading PolicyServer on page 4-27*.

3. After the upgrade completes and the database replicates, run the upgrade on the remaining PolicyServer instances.

Upgrading PolicyServer MMC

Note

For improved security measures, legacy versions of the PolicyServer MMC cannot manage PolicyServer 5.0 Patch 3. Upgrading the PolicyServer MMC is required.

Procedure

1. Complete *Uninstalling the PolicyServer MMC on page 4-31*.

2. Complete *Installing PolicyServer MMC on page 4-8*.

Migration to Control Manager

Administrators may manage Endpoint Encryption using only PolicyServer MMC or manage Endpoint Encryption using Control Manager for policy, user and device management and PolicyServer MMC for advanced log management and reporting.

For details, see *Control Manager Integration on page 5-1*.

Uninstallation

The following section explains how to uninstall PolicyServer. A common use case for uninstalling PolicyServer is that incorrect information was specified when PolicyServer was installed.

Uninstalling the PolicyServer MMC

Use **Windows Add or Remove Programs** to uninstall the PolicyServer MMC.

Note

Uninstalling the PolicyServer MMC does not affect the PolicyServer database and services.

Procedure

1. Go to **Start** > **Settings** > **Control Panel** > **Add or Remove Programs**

   The **Add or Remove Programs** window appears.

2. Select PolicyServer from the list of installed programs.
3. Click **Remove**.
4. At the **Add or Remove Programs** message, click **Yes** to confirm.

The uninstall process completes when the program is removed from the list.

Uninstalling PolicyServer

Uninstalling PolicyServer removes all Endpoint Encryption services. The Endpoint Encryption database is not affected by uninstalling PolicyServer.

WARNING!

Although uninstalling PolicyServer does not affect the Endpoint Encryption database, uninstalling PolicyServer removes all Endpoint Encryption services. Endpoint Encryption users are unable to log on to Endpoint Encryption devices until PolicyServer is reinstalled.

Procedure

1. Run `PolicyServerInstaller.exe`

   The PolicyServer Installer opens.

2. At the **Product Legal Notice** screen, read the license agreement and accept the terms by clicking **Accept**.

3. At the **PolicyServer Services** screen, click **Uninstall** at the left.

   The PolicyServer uninstallation begins.

4. Wait for the PolicyServer uninstalling process to remove all services and database settings.

5. Click **Finished**.

6. Restart the server.

7. Optionally, reinstall PolicyServer.

   See *Installing PolicyServer on page 4-3*.

Chapter 5

Control Manager Integration

This chapter explains how to integrate Endpoint Encryption with Trend Micro Control Manager. You may use Control Manager instead of PolicyServer MMC to manage PolicyServer.

Note

For information about the management consoles available to control the Endpoint Encryption implementation, see *Management Consoles on page 2-6*.

Topics include:

- *About Control Manager Integration on page 5-2*
- *Migrating to Control Manager on page 5-3*
- *Adding PolicyServer as a Managed Product to Control Manager on page 5-4*
- *Configuring Groups for Control Manager Policies on page 5-7*
- *Creating a Policy on page 5-8*
- *Changing a PolicyServer Managed Product in Control Manager on page 5-11*
- *Removing a PolicyServer Managed Product from Control Manager on page 5-11*

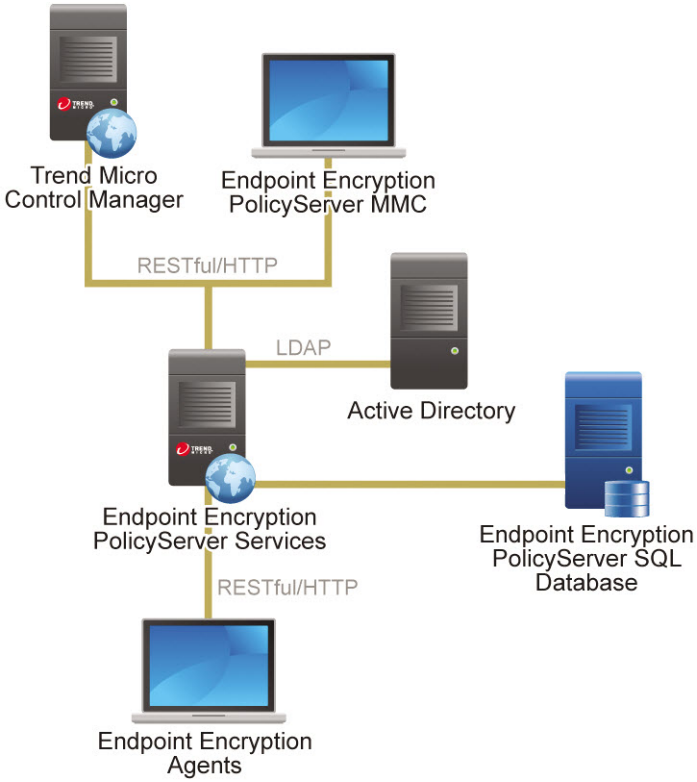
About Control Manager Integration

Flexibly manage Endpoint Encryption using only PolicyServer MMC or manage Endpoint Encryption using Control Manager for policy, user and device management and PolicyServer MMC for advanced log management and reporting.

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

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

The following illustration explains how to deploy Endpoint Encryption for the first time using Control Manager to manage PolicyServer. In a Control Manager deployment, administrators use Control Manager for all Endpoint Encryption policy, user, and device controls, and only use PolicyServer MMC for advanced Enterprise maintenance.



Note

In environments that use Control Manager, changes to PolicyServer policies are always controlled by Control Manager. Any changes made using PolicyServer MMC are overwritten the next time that Control Manager synchronizes policies to the PolicyServer database.

Migrating to Control Manager

Migration to Control Manager is not automated. The following procedure explains manually configuring Control Manager to match the existing configuration.

Procedure

1. Upgrade PolicyServer to version 5.0 Patch 3.

   See *Upgrade Considerations on page 3-22*.

2. Install and configure Control Manager.

   See the supporting documentation:

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

3. Add PolicyServer to Control Manager.

   See *Adding PolicyServer as a Managed Product to Control Manager on page 5-4*.

4. Add all existing users to Control Manager using the Endpoint Encryption Users widget.

5. For each group that currently exists, create a new policy.

   See *Creating a Policy on page 5-8*.

6. In each new policy, specify a policy target for every device that was assigned to the previous group.

   See *Specifying Policy Targets on page 5-9*.

7. Use Control Manager to deploy policies.

   See *Creating a Policy on page 5-8*.

Adding PolicyServer as a Managed Product to Control Manager

Endpoint Encryption allows administrators to use Trend Micro Control Manager to control PolicyServer and manage Endpoint Encryption agent policies or use Trend Micro OfficeScan to deploy Endpoint Encryption agent software on managed endpoints.

To use Control Manager to manage PolicyServer, you must add PolicyServer as a managed product.

Make sure to complete the following tasks before proceeding:

1. Install and configure Control Manager.

   See the supporting documentation at:

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

2. Install and configure PolicyServer.

To configure additional Control Manager procedures, see the *Endpoint Encryption Administrator's Guide*.

Important

Endpoint Encryption supports only one configured PolicyServer instance in Control Manager at a time. It is not possible to add multiple PolicyServer configurations. To configure a different PolicyServer, first remove the previously configured PolicyServer.

Procedure

1. Review all system requirements for compatible product versions.

   See *System Requirements on page 2-1*.

2. Log on to Control Manager.

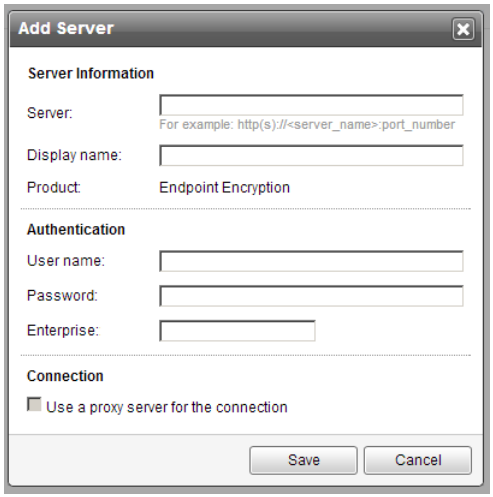
3. Go to **Policies** > **Policy Resources** > **Managed Servers**.

   The **Managed Servers** screen appears.

4. In the **Server Type** drop-down list, select **Endpoint Encryption**.

5. Click **Add**.

The **Add Server** screen appears.



6. Specify **Server Information** options.

   - **Server**: Specify the PolicyServer host name and the port number. Use the following format:

     ```
     http(s)://<server_name>:port_number
     ```

     Note

     Control Manager communicates with PolicyServer Endpoint Encryption Service. The default port number is 8080.

   - **Display name**: Specify how PolicyServer shows in the **Managed Servers** screen

7. Under **Authentication**, specify the user name and password of the Endpoint Encryption Enterprise Administrator account.

8. Under **Connection**, select **Use a proxy server for the connection** if PolicyServer requires a proxy connection.

9. Click **Save**.

Note

Synchronization between Control Manager and PolicyServer may require several minutes to complete.

PolicyServer is added as a new managed product to Control Manager.

Configuring Groups for Control Manager Policies

Control Manager simplifies policy management by merging the group and policy architecture of PolicyServer. Synchronizing the group and policy architecture of PolicyServer to the policy structure of Control Manager is not automated. The following procedure explains the most important information to acquire about the existing configuration before configuring the new Control Manager configuration.

Procedure

1. Log on to PolicyServer MMC.
2. Gather the following information:
   - Total number of groups, their names, and the subgroups
   - All users assigned to each group
   - The policy configuration of each group
3. Log on to Control Manager.
4. For each group in PolicyServer MMC, configure a new policy that matches the corresponding group policy configuration.

Note

Subgroups are no longer supported. Either create a policy for each subgroup, or create one policy for the group that affects the subgroups.

5. Add all users to each new policy.
6. Deploy each policy.

Creating a Policy

The following procedure explains how to configure a Control Manager policy that affects Endpoint Encryption users and devices.

Important

To add a user account to the policy, make sure that the user account already exists.

Note

For information about configuring Active Directory, see *PolicyServer Active Directory Synchronization on page 4-16*.

Procedure

1. Go to **Policies** > **Policy Management**.
2. From the **Product** drop-down list, select **Endpoint Encryption**.
3. Click **Create**.

   The **Create Policy** screen appears.

4. Specify a policy name.
5. Specify policy options.

   See *Specifying Policy Targets on page 5-9*

   Note

   For more information about the available policy options, see the *Endpoint Encryption Administrator's Guide*.

6. Click **Save**.

Specifying Policy Targets

Use the **Specify Target(s)** screen to assign Endpoint Encryption devices to the policy.

Note

The **Specify Target(s)** screen is available when creating a new policy.

For information about creating a policy, see *Creating a Policy on page 5-8*.

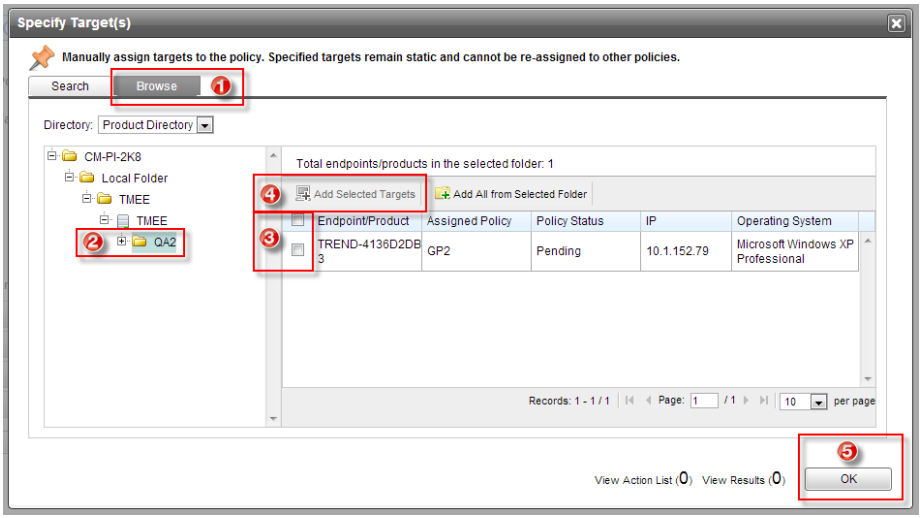


FIGURE 5-1. Specifying Policy Targets

Procedure

1. From the **Specify Target(s)** screen, click the **Browse** tab.
2. From the left pane, expand the tree to select the managed folder.

   Example: **CM-PI-2K8** > **Local Folder** > **TMEE** > **TMEE** > **QA2**
3. Select any appropriate Endpoint Encryption devices, or select the top check box to select all Endpoint Encryption devices listed on the current page.
4. Click **Add Selected Targets**.

> **Note**
>
> To immediately select all devices in the managed folder, click **Add All from Selected Folder**.

"View Action List" and "View Results" update based on the selection.

5. Click **OK**.

Changing a PolicyServer Managed Product in Control Manager

Important

Endpoint Encryption supports only one PolicyServer instance in Control Manager. It is not possible to add multiple PolicyServer instances.

Procedure

1. Remove PolicyServer from Control Manager.

   See *Removing a PolicyServer Managed Product from Control Manager on page 5-11*.

2. Add the new PolicyServer to Control Manager.

   See *Adding PolicyServer as a Managed Product to Control Manager on page 5-4*.

Removing a PolicyServer Managed Product from Control Manager

Procedure

1. Go to **Policies** > **Policy Resources** > **Managed Servers**.

   The **Managed Servers** screen appears.

2. Click the **Delete** icon ( ) in the **Actions** column.

3. At the message, click **OK** to confirm.

The PolicyServer instance is removed from Control Manager. Use PolicyServer MMC to manage policies.

Chapter 6

Endpoint Encryption Agent Deployment

Each Endpoint Encryption agent has unique installation and system requirements. For explanations about configuration and management, see the *Endpoint Encryption Administrator's Guide*.

Topics include:

- *Endpoint Encryption Agents on page 1-18*
- *About Full Disk Encryption on page 6-3*
- *About File Encryption on page 6-4*
- *Installation on page 6-4*
- *Upgrade on page 6-46*
- *Migration on page 6-51*
- *Uninstallation on page 6-59*

Endpoint Encryption Agents

The following table describes the Endpoint Encryption agents available for a variety of environments.

Agent	Description
File Encryption	The Endpoint Encryption agent for file and folder encryption on local drives and removable media. Use File Encryption to protect files and folders located on virtually any device that appears as a drive within the host operating system. For more information, see *About File Encryption on page 6-4*.
Full Disk Encryption	The Endpoint Encryption agent for hardware and software encryption with preboot authentication. Use Full Disk Encryption to secure data files, applications, registry settings, temporary files, swap files, print spoolers, and deleted files on any Windows endpoint. Strong preboot authentication restricts access vulnerabilities until the user is validated. For more information, see *About Full Disk Encryption on page 6-3*.
Encryption Management for Microsoft BitLocker	The Endpoint Encryption Full Disk Encryption agent for Microsoft Windows environments that simply need to enable Microsoft BitLocker on the hosting endpoint. Use the Encryption Management for Microsoft BitLocker agent to secure endpoints with Trend Micro full disk encryption protection in an existing Windows infrastructure. For more information, see *About Full Disk Encryption on page 6-3*.

AGENT	DESCRIPTION
Encryption Management for Apple FileVault	The Endpoint Encryption Full Disk Encryption agent for Mac OS environments that simply need to enable Apple FileVault on the hosting endpoint. Use the Encryption Management for Apple FileVault agent to secure endpoints with Trend Micro full disk encryption protection in an existing Mac OS infrastructure. For more information, see *About Full Disk Encryption on page 6-3*.

Note

Endpoint Encryption 5.0 does not have KeyArmor devices. However, legacy KeyArmor devices are supported.

About Full Disk Encryption

The Full Disk Encryption agent combines a robust AES256 encryption algorithm and mandatory authentication to make data inaccessible without authentication. Full Disk Encryption prevents data loss by encrypting the whole drive, including operating system, program, temporary, and end user files.

Full Disk Encryption allows for the flexibility to use either software-based encrypted hard drives or hardware-based encrypted hard drives as needed. Seagate DriveTrust™, OPAL, OPAL2, and SanDisk™ self-encrypting solid-state drives are supported. While hardware-based encryption is simpler to deploy on new hardware, easier to maintain, and offers a higher level of performance, software-based encryption does not require any hardware and is cheaper to deploy to existing endpoints.

Trend Micro PolicyServer controls policies affecting Full Disk Encryption, ensuring complete endpoint security centrally managed across the Enterprise. Full Disk Encryption is network-aware and updates policies before allowing authentication. You can also remotely lock or wipe data on the endpoint before the operating system or any other sensitive data is accessed.

Trend Micro Endpoint Encryption 5.0 Patch 3 advances Full Disk Encryption by integrating with encryption solutions built into the host operating system through two new Endpoint Encryption agents:

- Encryption Management for Microsoft BitLocker
- Encryption Management for Apple FileVault

About File Encryption

The Trend Micro File Encryption agent uses AES encryption to protect data that is shared between Endpoint Encryption users, stored on removable media, or saved on network resources. File Encryption can also protect different files with different keys, allowing you to set access policies to the File Encryption agent and then create separate policies for access to certain files, which is useful in environments where multiple users access the same endpoint. Encryption is performed after authentication takes place.

You can use Trend Micro PolicyServer to specify which files and folders are encrypted and policies about encrypting removable media.

End users also have the flexibility to locally manage File Encryption by encrypting individual files, folders, or removable media on the fly, safeguarding their data regardless of where it travels.

Installation

The following section explains the prerequisites for fresh Endpoint Encryption agent installations, how to manually install Endpoint Encryption agents, and tools for preparing automated installation scripts.

Before Installing Endpoint Encryption Agents

Before installing the Endpoint Encryption agents, consider the following:

- Make sure that all system requirements are met. For more information, see *System Requirements on page 2-1*

- Copy all agent installation files to the local hard disk
- Tools are available for building automated installation scripts. For more information, see *Automated Deployments on page 6-33*
- The installing account has Local Administrator privileges
- Review *Requirements for Managed Endpoints on page 6-5*

For additional pre-deployment considerations, see *Predeployment Checklist on page 3-2*.

Requirements for Managed Endpoints

After installing any Endpoint Encryption agent, the endpoint registers as a new Endpoint Encryption device to PolicyServer. Authentication, encryption, and remote device actions are centrally controlled by PolicyServer policies. The following are required to install managed endpoints:

- The computer has network access and can communicate with PolicyServer during installation
- For environments using PolicyServer MMC, there is at least one top-level group added
- For environments using Control Manager, there is at least one policy configured
- The Endpoint Encryption user has permission to add devices to the group or policy

Note

It is now possible to use the Enterprise Administrator and Enterprise Authenticator roles to install Endpoint Encryption agents.

- The installing account has Local Administrator privileges.
- If domain authentication/Single Sign-on is enabled, the user name matches the user name in Active Directory. The Active Directory password is used for authentication

Automating Agent Deployment

There are two methods to simplify mass deployment across an enterprise with a large number of endpoints:

- Use OfficeScan: *OfficeScan Integration on page 7-1*
- Create installation scripts and then use automation tools such as Microsoft SCCM or SMS: *Automated Deployments on page 6-33*

Full Disk Encryption Deployment

The following sections describe how to install and configure the three Endpoint Encryption agents that manage full disk encryption:

- Full Disk Encryption
- Encryption Management for Microsoft BitLocker
- Encryption Management for Microsoft BitLocker

Note

It is now possible to use the Enterprise Administrator and Enterprise Authenticator roles to install Endpoint Encryption agents.

Full Disk Encryption Deployment Outline

The following procedure explains how to prepare for and install the following Full Disk Encryption agents:

- Full Disk Encryption
- Encryption Management for Microsoft BitLocker
- Encryption Management for Apple FileVault

Procedure

1. Make changes to the operating system to prepare the endpoint.

See *Endpoint Preparation on page 6-7*.

2. For Windows environments, prepare the hard drive.

   See *Preparing the Hard Disk on page 6-9*.

3. Disable the encryption policy during deployment.

   See *Disable Encryption During Deployment on page 6-11*.

4. Deploy the Endpoint Encryption agent.

   See one of the following topics:

   - *Full Disk Encryption Installation on page 6-11*
   - *Encryption Management for Microsoft BitLocker Installation on page 6-16*
   - *Encryption Management for Apple FileVault Installation on page 6-25*

5. Follow the instructions in the installation task to verify the deployment.

Endpoint Preparation

Before installing Full Disk Encryption agents, prepare the endpoint to prevent data loss. The following topics explain how to prepare the endpoint in Windows and Mac OS environments.

Preparing the Windows Endpoint

Note

- Do not install Full Disk Encryption on endpoints with multiple hard disks. Multiple disk environments are not supported
- RAID and SCSI disks are not supported
- Full Disk Encryption for Windows 8 does not support RAID, SCSI, or eDrive drives

Procedure

1. Disconnect all USB storage devices until after the that agent is installed and the endpoint is restarted.
2. Make sure that the drive with the operating system is not already encrypted and that BitLocker is disabled.
3. Verify that all system requirements are met.

   See *System Requirements on page 2-1*.

4. For Windows 8 endpoints that support UEFI BIOS, change the boot priority to **Legacy First**.
   a. From Windows 8, hold SHIFT and restart the device.

      The device restarts and UEFI BIOS loads.

   b. Click the **Troubleshoot** tile.

      The **Advanced options** screen appears.

   c. Click the **UEFI Firmware Settings** tile.

      If the **UEFI Firmware Setting** tile does not exist, the device does not use UEFI and no change is required.

   d. Set **UEFI/Legacy Boot Priority** to **Legacy First**.
   e. Restart the endpoint.
5. Copy the installation files to the system drive.

Preparing the Mac OS Endpoint

Procedure

1. Remove any existing full disk encryption product.
2. Make sure that Encryption Management for Apple FileVault is currently disabled.

a. Go to **System Preferences** > **Security & Privacy**.

b. Select the **FileVault** tab.

c. If necessary, click the lock icon ( ) to make changes.

d. Specify the user name and password for the endpoint.

e. Click **Turn Off FileVault**.

Preparing the Hard Disk

Full Disk Encryption encrypts every sector on the physical drive. Since many applications, including the operating system, do not utilize the entire physical hard disk space, sectors may be damaged or the drive may be extremely fragmented. Encryption Management for Microsoft BitLocker and Encryption Management for Apple FileVault leverage the encryption solution built into the host operating system. There is no need to prepare the hard disk if using one of these Endpoint Encryption agents.

Note

Trend Micro recommends doing a small pilot of fresh installs and upgrades before deploying the latest Full Disk Encryption build. For more information, see *Endpoint Encryption Pilot Deployment on page C-1*.

Important

The Full Disk Encryption agent can only install on an endpoint with one physical drive. Remove all other drives before installing Full Disk Encryption.

Procedure

1. Run Windows defragment utility on the system drive.

   For information about defragmenting a Windows hard drive, see the following article:

   http://windows.microsoft.com/en-hk/windows-vista/improve-performance-by-defragmenting-your-hard-disk

2. Verify that the system drive has at least 256MB of contiguous free space.

3. Run the Windows disk integrity utility (requires a reboot).

   a. Using a script or command prompt, run `chkdsk /f /r` and schedule to the check disk after the next system restart.

   b. Reboot device.

   c. Replace the drive if `chkdsk` reports multiple bad sectors.

4. Check the disk for a normal Master Boot Record (MBR) and confirm that a normal boot sector is present on the boot partition. For example, a dual boot machine has a modified boot sector.

   Note

   GUID Partition Table (GPT) disks are not currently supported.

Disable Encryption During Deployment

The table below explains how to disable encryption centrally from one of the management consoles. Temporarily disable drive encryption to minimize end user impact and simplify mass deployment. Once device compatibility is confirmed, optionally re-enable encryption.

TABLE 6-1. Disable Device Encryption PolicyServer

CONSOLE	POLICY SETTING
PolicyServer MMC	Go to **Full Disk Encryption** > **PC** > **Encryption** > **Encrypt Device** and select **No**.
Control Manager	Access a new or existing policy (**Policies** > **Policy Management**) and then deselect **Encrypt device** under **Full Disk Encryption**.

Full Disk Encryption Installation

Use Full Disk Encryption to secure data files, applications, registry settings, temporary files, swap files, print spoolers, and deleted files on any Windows endpoint. Strong preboot authentication restricts access vulnerabilities until the user is validated.

Note

Before proceeding, make sure to read the following topics:

- *System Requirements on page 2-1*
- *Before Installing Endpoint Encryption Agents on page 6-4*
- *Requirements for Managed Endpoints on page 6-5*
- *Automated Deployments on page 6-33*

Full Disk Encryption Pre-installation Checklist

The Full Disk Encryption installer automatically checks the target system to make sure that all necessary system requirements are met before installing the agent. If a system incompatibility is discovered, the installer closes and generates the `PreInstallCheckReport.txt` in the same location as the installer.

Use the pre-installation checklist to determine which system requirements are not met. The checklist file is located in the same folder as the Full Disk Encryption installer.

TABLE 6-2. Conditions Checked by the Installer

SPECIFICATION	REQUIREMENT	DESCRIPTION
Supported OS	Not all operating systems are supported	Full Disk Encryption cannot be installed on certain versions of Windows.
Encryption Management for Microsoft BitLocker is already installed	No other full disk encryption product can be installed	Encryption Management for Microsoft BitLocker must not be installed. Uninstall Encryption Management for Microsoft BitLocker to install Full Disk Encryption or use Encryption Management for Microsoft BitLocker instead.
Fixed media	Internal hard drive	Full Disk Encryption cannot be installed on removable drives running Windows.
Multiple hard disks	Only one hard disk is allowed.	The endpoint must only have one hard disk. Multiple disk environments are not supported.
Free space	256 MB minimum	
Memory	512 MB minimum 1 GB recommended	
Partition count	Fewer than 25 partitions	Partitions with extended MBRs are not available.
Partition type	Only MBR is supported	GUID partition table (necessary for disks larger that 2 TB) is not currently supported.

Specification	Requirement	Description
Physical drive is bootable	A bootable partition is required	Full Disk Encryption must be installed on a bootable table.
SCSI disk	ATA, AHCI or IRRT drive controller. SCSI is not supported	• Check only provides a warning; Windows may report a SATA drive as SCSI • If the disk is not a true SCSI, Full Disk Encryption can be installed. If unsure, physically check the drive
Microsoft .Net Framework	.Net 2.0 SP1 or newer required for Windows XP or earlier	Skipped for Windows Vista or newer operating systems.
SED hardware compatibility	Hardware encryption is enabled if present	Full Disk Encryption currently supports the following: • Seagate DriveTrust drives • Seagate OPAL and OPAL 2 drives • SanDisk self-encrypting solid-state drives
BitLocker is enabled	BitLocker must be disabled	Full Disk Encryption and BitLocker cannot simultaneously provide full disk encryption.

Note

If the pre-installation check fails for any of these reasons, contact Trend Micro for assistance.

Installing the Full Disk Encryption Agent

After the agent is installed, the endpoint restarts for software-based encryption or shuts down for hardware-based encryption.

Policies are synchronized with PolicyServer after the endpoint restarts.

Note

- Do not install Full Disk Encryption on endpoints with multiple hard disks. Multiple disk environments are not supported
- RAID and SCSI disks are not supported
- Full Disk Encryption for Windows 8 does not support RAID, SCSI, or eDrive drives

Note

For information about the Endpoint Encryption services used by Endpoint Encryption agents, see *Endpoint Encryption Services on page D-1*.

Procedure

1. Copy the installation package to the local hard drive.
2. Run `TMFDEInstall.exe`.

   Note

   If the **User Account Control** windows displays, click **Yes** to allow the installer to make changes to the Endpoint Encryption device.

3. Wait for the installer to load.

FIGURE 6-1. Installation Loading Badge

After a moment, the installation welcome screen appears.

4. Select **Managed installation** and then click **Next**.

   Managed Installation screen displays.

5. Specify the PolicyServer information.

OPTION	DESCRIPTION
Server name	Specify the PolicyServer IP address or host name, and include the port number assigned to that configuration.
Enterprise	Specify the Enterprise. Only one Enterprise is supported.
User name	Specify the user name of an account with permission to add devices to the Enterprise.
Password	Specify the password for the user name.

6. At the **Installation Complete** screen, click **Close**.

7. At the dialog box, click **Yes** to restart or shutdown the endpoint.

   Full Disk Encryption installation is complete once Preboot displays. Disk encryption begins after Windows starts.

What to do next

When Full Disk Encryption Preboot loads, the user must log on before gaining access to Windows. Depending on the policy configuration, the user may be required to change the password after logging on the endpoint.

Note

For information about understanding and managing the Endpoint Encryption agent, see the *Endpoint Encryption Administrator's Guide*.

Encryption Management for Microsoft BitLocker Installation

Use the Encryption Management for Microsoft BitLocker agent to secure endpoints with Trend Micro full disk encryption protection in an existing Windows infrastructure.

Before proceeding, make sure to read the following topics:

- *System Requirements on page 2-1*
- *Before Installing Endpoint Encryption Agents on page 6-4*
- *Requirements for Managed Endpoints on page 6-5*
- *Automated Deployments on page 6-33*

In addition to the other requirements, Encryption Management for Microsoft Bitlocker requires two partitions: a boot partition and a system partition on the local endpoint. On Microsoft Windows 7 and later versions, a system partition and a boot partition are both typically created during the installation process. If you attempt to install or upgrade Encryption Management for Microsoft Bitlocker and receive an error regarding system and boot partitions, create a system partition and try again.

For more information, see *Creating a System Partition with Microsoft BitLocker on page 6-18*.

Once installed, the Endpoint Encryption agent is inactive until the policy to encrypt the Endpoint Encryption device is enabled. The Endpoint Encryption agent becomes inactive again if encryption is disabled at a later time.

Installing the Encryption Management for Microsoft BitLocker Agent

After the agent is installed, the endpoint restarts for software-based encryption or shuts down for hardware-based encryption.

Note

For information about the Endpoint Encryption services used by Endpoint Encryption agents, see *Endpoint Encryption Services on page D-1*.

Procedure

1. Copy the installation package to the local hard drive.
2. Run `TMFDEInstall_BL.exe`.

   Note

   If the **User Account Control** windows displays, click **Yes** to allow the installer to make changes to the Endpoint Encryption device.

3. Wait for the installer to load.

FIGURE 6-2. Installation Loading Badge

After a moment, the installation welcome screen appears.

4. Specify the PolicyServer information.

OPTION	DESCRIPTION
Server name	Specify the PolicyServer IP address or host name, and include the port number assigned to that configuration.
Enterprise	Specify the Enterprise. Only one Enterprise is supported.
User name	Specify the user name of an account with permission to add devices to the Enterprise.

Option	Description
Password	Specify the password for the user name.

5. Click **Install**.

   Encryption Management for Microsoft BitLocker installation begins. After a moment, the installation completes and the installer closes.

6. Go to the system tray and click the icon to open the Encryption Management for Microsoft BitLocker agent.

Note

For information about understanding and managing the Endpoint Encryption agent, see the *Endpoint Encryption Administrator's Guide*.

Creating a System Partition with Microsoft BitLocker

Encryption Management for Microsoft Bitlocker requires separate boot and system partitions on the local endpoint. On Microsoft Windows 7 and later versions, a system partition and a boot partition are both typically created during the installation process. If you attempt to install or upgrade Encryption Management for Microsoft Bitlocker and receive an error regarding system and boot partitions, you may need to create a system partition. Perform the following procedure to check whether the endpoint has separate boot and system partitions. If the endpoint does not have separate partitions, use BitLocker Drive Encryption to create a system partition.

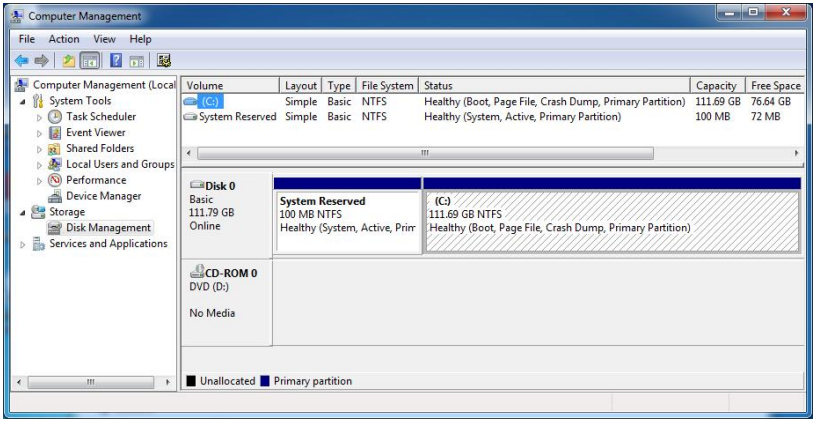
Procedure

1. Verify whether your endpoint has separate system and boot partitions.

   a. Open the Windows **Start** menu.

   b. Type `diskmgmt.msc` to open the **Computer Management** window.

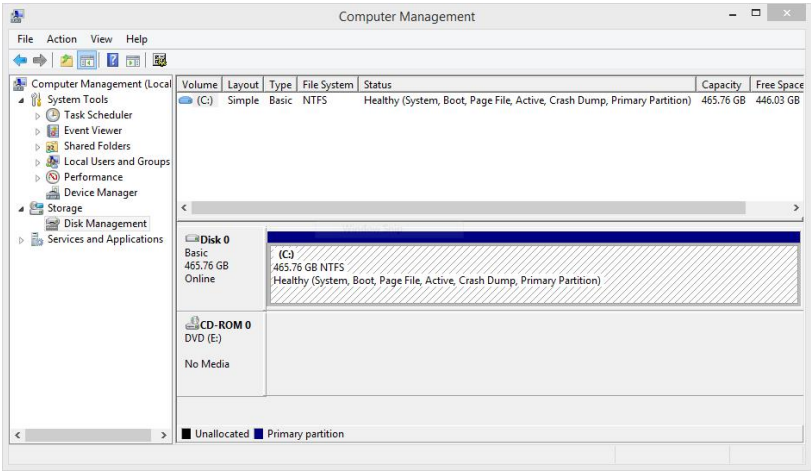
The following is an example of an endpoint that contains separate system and boot partitions:



WARNING!

If you attempted to install or upgrade Encryption Management for Microsoft Bitlocker and received an error regarding system and boot partitions, check **Computer Management**. If you find that you already have separate system and boot partitions, do not continue this task. Contact Trend Micro Support.

The following is an example of an endpoint that contains a combined system and boot partition:



If your system and boot partitions are both in the same disk, continue the rest of this procedure.

2. If you already have an Encryption Management for Microsoft BitLocker agent on your endpoint, uninstall the agent.

   This step is only necessary if you were attempting to upgrade Encryption Management for Microsoft BitLocker to a newer version.

3. Back up critical files in your primary drive.

Important

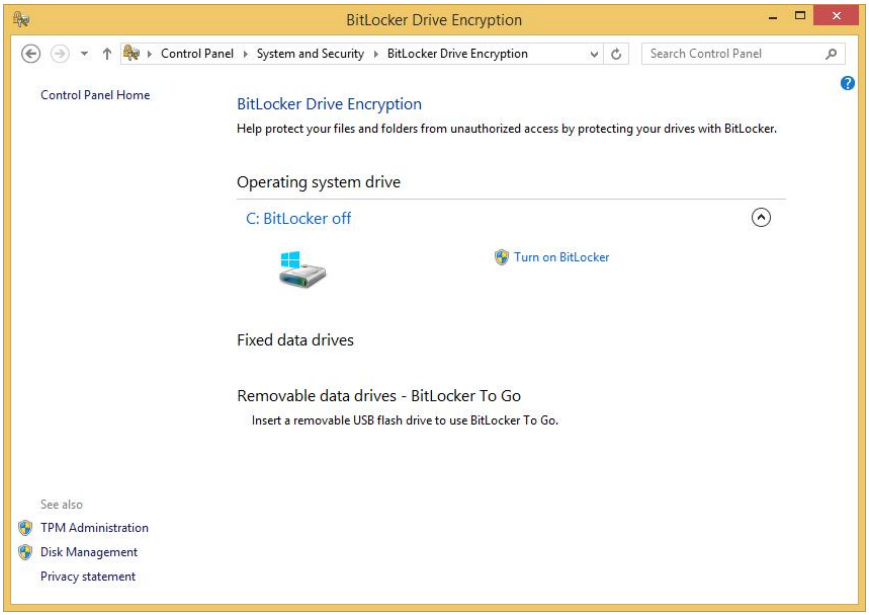
The following steps include using BitLocker to change the structure of your primary drive. Any changes to system structure may result in errors. Trend Micro strongly recommends saving important files to a removeable device before continuing.

---

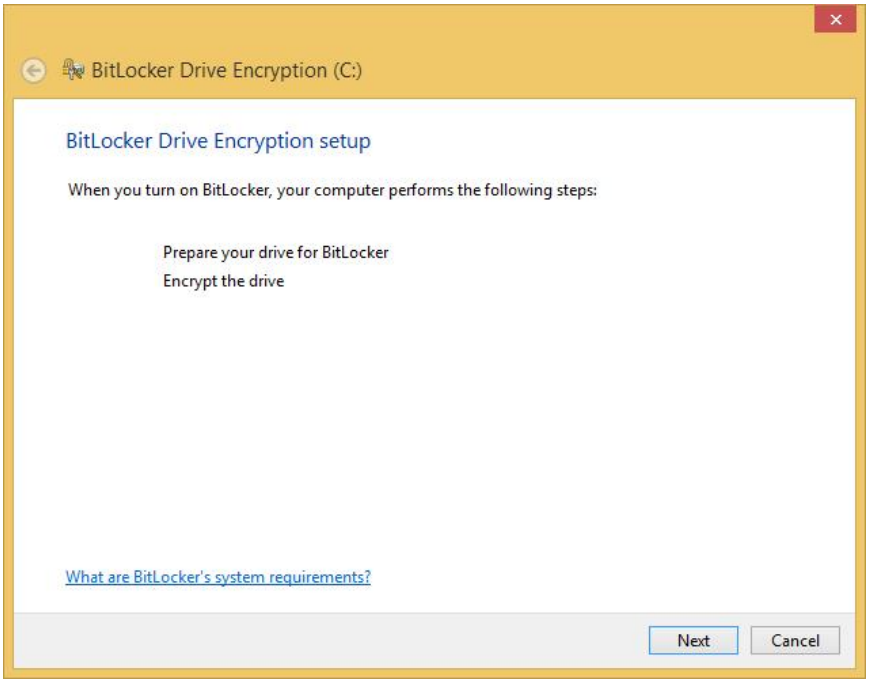
4. Turn on BitLocker.

   a. From the Windows **Start** menu, go to **Control Panel** > **System and Security** > **BitLocker Drive Encryption**.

b. Click **Turn on BitLocker**.



The **BitLocker Drive Encryption** window appears.

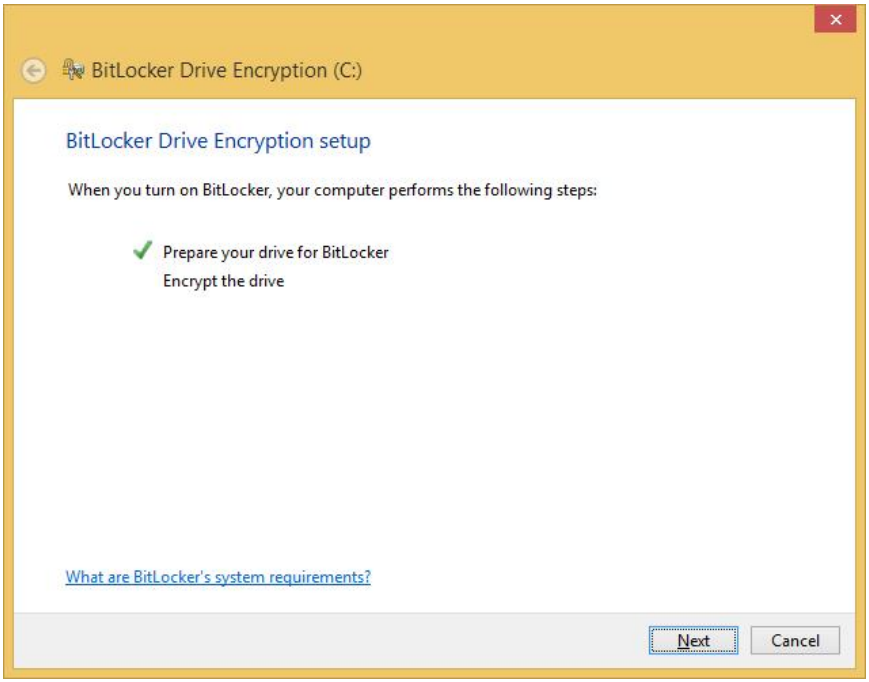


5. To create the system partition, follow the on-screen instructions in the **BitLocker Drive Encryption** window.

   Creating the system partition may take a long time depending upon the drive size.

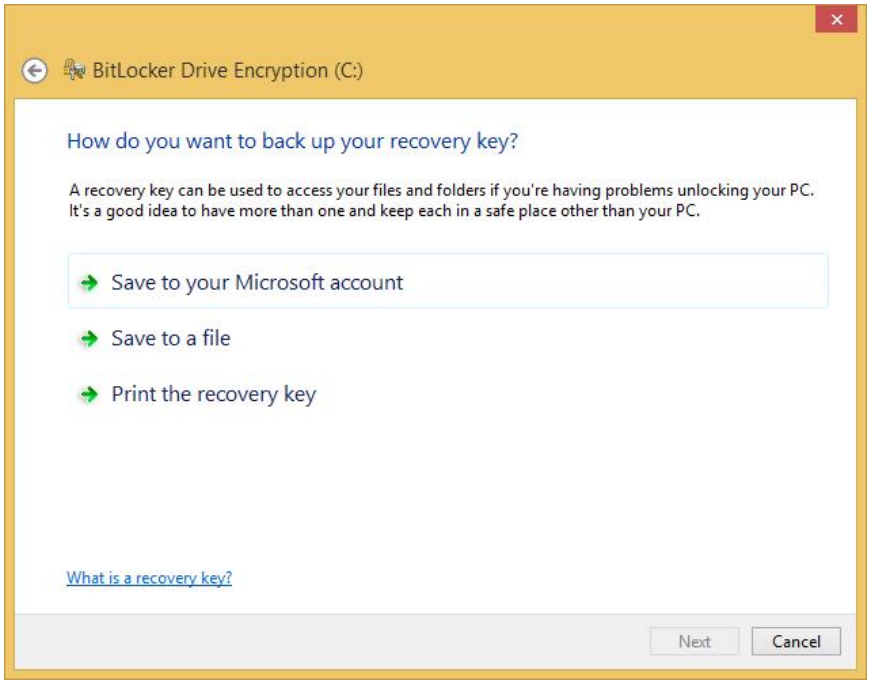
6. Restart your endpoint.

After restarting your endpoint, BitLocker will display the following screen:



7. Click **Next**.

BitLocker will request that you back up your recovery key.



Endpoint Encryption will create a recovery key during the encryption process, so backing up the recovery key at this point is unnecessary.

8. Click **Cancel** to close **BitLocker Drive Encryption**.

   The system partition has been created.

9. Install the Encryption Management for Microsoft BitLocker agent.

   See *Installing the Encryption Management for Microsoft BitLocker Agent on page 6-16*.

Encryption Management for Apple FileVault Installation

Use the Encryption Management for Apple FileVault agent to secure endpoints with Trend Micro full disk encryption protection in an existing Mac OS infrastructure.

Before proceeding, make sure to read the following topics:

- *System Requirements on page 2-1*
- *Before Installing Endpoint Encryption Agents on page 6-4*
- *Requirements for Managed Endpoints on page 6-5*
- *Automated Deployments on page 6-33*

Installing the Encryption Management for Apple FileVault Agent

Encryption Management for Apple FileVault can be installed by PolicyServer Group Administrator, Authenticator, or standard user accounts.

Note

For information about the Endpoint Encryption services used by Endpoint Encryption agents, see *Endpoint Encryption Services on page D-1*.

Procedure

1. Run `TMFDEInstall_FV.exe`.

   The Trend Micro Full Disk Encryption disk image appears.

2. Double-click `Trend Micro Full Disk Encryption.pkg` to begin the installation.

   The Encryption Management for Apple FileVault Setup Wizard to begin the File Encryption installation process

3. From the **Welcome** screen, click **Continue**.

   The Installer checks that the system requirements are met.

4. If the system requirements are met, click **Install**.

5. Select the hard disk to install that agent.

6. Specify the user name and password of an account with permission to install applications on the endpoint, and click **Install Agent**

   The installation begins.

7. Specify the PolicyServer information.

Option	Description
Server name	Specify the PolicyServer IP address or host name, and include the port number assigned to that configuration.
Enterprise	Specify the Enterprise. Only one Enterprise is supported.
User name	Specify the user name of an account with permission to add devices to the Enterprise.
Password	Specify the password for the user name.

8. Click **Continue**.

   After a moment, the Encryption Management for Apple FileVault installation begins.

9. After the installation completes, click **Close** to restart the endpoint.

   The Encryption Management for Apple FileVault agent initiates immediately after the endpoint restarts.

10. Go to the menu bar ( ) to open the Encryption Management for Apple FileVault agent.

Note

For information about understanding and managing the Endpoint Encryption agent, see the *Endpoint Encryption Administrator's Guide*.

Creating a Mobile Account for Active Directory on Mac OS

Mac OS local accounts or mobile accounts are able to initiate encryption on Mac OS X Mountain Lion or above. Other Mac OS user account types will be unable to initiate encryption.

If a Mac OS account other than a local account or mobile account attemps to initate encryption, the following notification appears:

The following task shows how to create a mobile account for your Mac OS account to bypass this issue.

Procedure

1. Go to **System Preferences...** in the Apple menu.

   The **System Preferences** window appears.

2. Select **User Groups** under the **System** section.

3. Click the lock icon in the lower left corner.

4. Click **Create...** next to **Mobile account**.

5. On the following screens, select any personal settings, and click **Create** to proceed from one screen to the next.

6. When prompted, enter your Active Directory password and click **OK**.

Your mobile account has been created. You may now use this mobile account to initate encryption.

File Encryption Deployment

This section describe how to install the File Encryption agent. Use File Encryption to protect files and folders located on virtually any device that appears as a drive within the host operating system.

Note

It is now possible to use the Enterprise Administrator and Enterprise Authenticator roles to install Endpoint Encryption agents.

File Encryption Deployment Outline

Procedure

1. Enable File Encryption in PolicyServer MMC.
2. Configure File Encryption Policies:
   a. Encryption Key Used
   b. Folders to Encrypt
   c. Use of Removable Media
   d. Authentication Method
3. Set up groups and users.
4. Create and test the installation package in a pilot program.

   See *Endpoint Encryption Pilot Deployment on page C-1*
5. Verify policy settings are enforced as defined.
   a. Set the encrypted folder.

      See *File Encryption Encrypted Folder on page 6-30*.
   b. Set the encryption key.

      See *File Encryption Encryption Key on page 6-30*.
   c. Set the storage device policies.

      See *File Encryption Storage Device Protection on page 6-31*.
6. Prepare end user communications.

   See *End User Communication on page B-11*.

File Encryption Encrypted Folder

File Encryption can automatically created encrypted folders on endpoints with the File Encryption agent installed . Files copied to a secure folder are automatically encrypted. By default, a File Encryption encrypted folder is created on the desktop.

The following table explains the policies requirements to configure File Encryption Encrypted Folder. Depending on the management console used, the policy configuration is slightly different.

TABLE 6-3. Encrypted Folder Policy Configuration

CONSOLE	POLICY SETTING
Control Manager	Access a new or existing policy (**Policies** > **Policy Management**), and expand **File Encryption**. Use **Folder to Encrypt** to create secure folders on endpoint.
PolicyServer MMC	• Use **File Encryption** > **Encryption** > **Specify Folders To Encrypt** to create secure folders on the endpoint. • Use **File Encryption** > **Encryption** > **Removable Media** > **Folders To Encrypt On Removable Media** to create secure folders on a USB storage device.

File Encryption Encryption Key

The File Encryption Encryption Key sets the level of access to the File Encryption encrypted folder.

- User key: Only the user can access the encrypted content.
- Group key: Only users within the same policy (Control Manager) or the same group (PolicyServer MMC) can access the content.
- Enterprise key: All Endpoint Encryption users can access the content.

TABLE 6-4. Encryption Key Policy Configurations

CONSOLE	POLICY SETTING
Control Manager	Access a new or existing policy (**Policies** > **Policy Management**), and expand **File Encryption**. Use **Encryption Key Used** to set the key.
PolicyServer MMC	• Use **File Encryption** > **Encryption** > **Encryption Method Allowed** to set which keys are available • Use **File Encryption** > **Encryption** > **Encryption Key Used** to set the key

File Encryption Storage Device Protection

File Encryption can protect files on removable media. The following options are available:

- **Removable Media**: Enables USB storage device protection.
- **Allowed USB Devices**: Permit any USB storage device or only KeyArmor devices to be used.
- **Fully Encrypt Device**: Automatically encrypt all files copied to the USB storage device.
- **Disable USB Drive**: Set to Always, Logged Out or Never.

TABLE 6-5. Storage Device Policy Configurations

CONSOLE	POLICY SETTING
Control Manager	Access a new or existing policy (**Policies** > **Policy Management**), and expand **File Encryption**. Set policies under the **Storage Devices** section.
PolicyServer MMC	Go to **File Encryption** > **Encryption**.

File Encryption Installation

Use File Encryption to protect files and folders located on virtually any device that appears as a drive within the host operating system.

Note

Before proceeding, make sure to read the following topics:

- *System Requirements on page 2-1*
- *Before Installing Endpoint Encryption Agents on page 6-4*
- *Requirements for Managed Endpoints on page 6-5*
- *Automated Deployments on page 6-33*

Installing the File Encryption Agent

The File Encryption installation process involves running an installer on the endpoint and following the step-by-step instructions.

Note

For information about the Endpoint Encryption services used by Endpoint Encryption agents, see *Endpoint Encryption Services on page D-1*.

Procedure

1. Run `FileEncryptionIns.exe`

   The File Encryption Setup Wizard appears.

2. Click **Next**.

   Note

   If prompted by User Account Control, click **Yes**.

   The File Encryption installer initiates and automatically installs the agent.

3. Wait for the File Encryption agent to install.
4. When the installation completes, click **Close**.
5. Click **Yes** to restart Windows.

The endpoint restarts and File Encryption is installed. Two File Encryption icons display: one shortcut on the desktop and one tray icon. After the desktop loads, it may take a moment for the agent to initiate.

6. From the File Encryption **Login** screen, set the following parameters.

Option	Description
User name	Specify the user name of an account with permission to add devices to the Enterprise.
Password	Specify the password for the user name.
Server name	Specify the PolicyServer IP address or host name, and include the port number assigned to that configuration.
Enterprise	Specify the Enterprise. Only one Enterprise is supported.

7. Click **OK**.

Note

For information about understanding and managing the Endpoint Encryption agent, see the *Endpoint Encryption Administrator's Guide*.

Automated Deployments

Scripting installations is most common for large deployments using automated tools such as Microsoft SMS or Active Directory. The Command Line Installer Helper (see *Command Line Installer Helper on page 6-40* for more details) is a tool used to create scripts. The arguments available allow for completely silent or partially silent installations.

WARNING!

Insufficient system setup or hard disk drive preparation may result in irreversible data loss.

Endpoint Encryption Agent Deployment using OfficeScan

For environments using OfficeScan, the most efficient deployment method is with the Endpoint Encryption Deployment Tool plug-in. For information about using the plug-in, see *OfficeScan Integration on page 7-1*.

Requirements for Scripted Deployments

- Use the Command Line Helper or Command Line Installer Helper to build the script
- Run the script from the endpoint, not a network share or USB device
- System management software: Tivoli, SCCM/SMS or LANDesk
- Run installation scripts using a Local Administrator account
- Recommendation: test installation scripts in a pilot program before mass deployment. For pilot program recommendations, see *Endpoint Encryption Pilot Deployment on page C-1*

Encryption Management for Apple FileVault Automated Deployment

The following is the process for setting up command line scripts to automate Encryption Management for Apple FileVault deployments. This procedure assumes that you have received the following files:

- `Installer.sh`
- `InstallPreCheck`
- `Trend Micro Full Disk Encryption.pkg`

The following is an example of the intended installation command script built using this procedure:

```
$ sudo /var/tmp/Installer.sh /var/tmp
```

The following is an example of the intended agent registration command script built using this procedure:

```
$ sudo"/Library/Application Support/TrendMicro/FDEMM/
RegisterDevice
HOST=10.1.152.58 ENTERPRISE=MyCompany USERNAME=User
ePASSWORD==5mih67uKdy7TlVaN2ISWGQQ=
```

Procedure

1. Place the installation files into the the same directory.

   `Installer.sh`, `InstallPreCheck`, and `Trend Micro Full Disk Encryption.pkg` must be in the same directory for automated deployment to run successfully. This procedure assumes those files have been placed in the directory `/var/tmp` for later example command scripts.

2. In a command line interface, run `Installer.sh` with the directory of the installation files as the first parameter.

   An example command script is as follows:

   ```
   $ sudo /var/tmp/Installer.sh /var/tmp
   ```

   `Installer.sh` will call `InstallPreCheck` to check your environment for potential issues that could hinder deployment or agent use. If any issues are found, the return code of the issue will be returned. If no issues are found, `Installer.sh` will execute `Trend Micro Full Disk Encryption.pkg` to perform installation.

   For potential error codes and limitations of Encryption Management for Apple FileVault deployment, see *Encryption Management for Apple FileVault Preinstallation Return Codes on page 6-37*.

3. If `Installer.sh` returns code `106`, check the version of a currently installed Encryption Management for Apple FileVault agent.

   Return code `106` means that Encryption Management for Apple FileVault is already installed.

   To check the currently installed version, run the following command script:

   ```
   $ defaults read "/Applications/Encryption Management for
   Apple FileVault.app/Contents/Info.plist"
   CFBundleShortVersionString
   ```

To check the version of the intended agent deployment package, run the following command script:

```
$ /var/tmp/InstallPreCheck version
```

If the intended version is later than the currently installed version, upgrade Encryption Management for Apple FileVault instead of continuing deployment. See *Upgrading Encryption Management for Apple FileVault on page 6-50*.

4. If installation of Encryption Management for Apple FileVault proceeded successfully, run the `RegisterDevice` executable with your enterprise credentials as parameters to register the agent to PolicyServer.

   The `RegisterDevice` executable is located in the agent directory. The default `RegisterDevice` path is `/Library/Application Support/TrendMicro/FDEMM/RegisterDevice`.

   In order, add the `HOST`, `ENTERPRISE`, `USERNAME`, and `PASSWORD` arguments as parameters. Encryption Management for Apple FileVault supports encrypted values of these arguments by adding `e` before the argument name. For example, an encrypted argument of `PASSWORD` is `ePASSWORD`.

   See the following links for help creating the `RegisterDevice` command script:

   - *Script Arguments on page 6-38*
   - *Creating Agent Installation Scripts on page 6-40*

   The following is an example of the intended agent registration command script:

```
$ sudo"/Library/Application Support/TrendMicro/FDEMM/
RegisterDevice
HOST=10.1.152.58 ENTERPRISE=MyCompany USERNAME=User
ePASSWORD==5mih67uKdy7TlVaN2ISWGQQ=
```

   After agent registration, the Encryption Management for Apple FileVault agent deployment is complete.

Encryption Management for Apple FileVault Preinstallation Return Codes

Before performing an Encryption Management for Apple FileVault automated deployment, run `Installer.sh` to check your environment for potential issues that could hinder deployment or agent use. The following is a list of the potential codes that `Installer.sh` will return.

Note

Do not perform Encryption Management for Apple FileVault agent deployment unless `Installer.sh` returns code `0`.

TABLE 6-6. Return Codes

RETURN CODE	DESCRIPTION
`0`	The endpoint is ready for Encryption Management for Apple FileVault agent deployment.
`101`	The operating system is not supported. Encryption Management for Apple FileVault requires Mac OS X Mountain Lion (10.7) or later.
`102`	The endpoint does not have sufficient disk space. Encryption Management for Apple FileVault requires at least 400 MB of free disk space.
`103`	Apple FileVault is enabled. Disable Apple FileVault, restart the endpoint, and try again.
`104`	Encryption Management for Apple FileVault does not support Apple Fusion Drive. Set a hard drive without Apple Fusion Drive as the root drive and try again.
`105`	Encryption Management for Apple FileVault requires Mono Framework version 2.10.11. Unistall the currently installed version and try again.

Return Code	Description

106	Encryption Management for Apple FileVault is already installed.
	
	To check the currently installed version, run the following command script:
	
	`$ defaults read "/Applications/Encryption Management for Apple FileVault.app/Contents/Info.plist" CFBundleShortVersionString`
	
	To check the version of the intended agent deployment package, run the following command script:
	
	`$ <directory>/InstallPreCheck version`

107	Encryption Management for Apple FileVault deployment requires administrator privileges. Use the `sudo` parameter when running the command script.
108	The syntax of the command script is incorrect. Specify the directory of `Installer.sh` in the first parameter position and try again. For example: `$ /var/tmp/Installer.sh /var/tmp`
109	`Installer.sh` is unable to find or run `InstallPreCheck`. Check that `InstallPreCheck` is in the same directory as `Installer.sh` and that you have privileges to run executable files and try again.
110	`Installer.sh` is unable to find `Trend Micro Full Disk Encryption.pkg`. Check that `Trend Micro Full Disk Encryption.pkg` is in the same directory as `Installer.sh` and try again.
111	`Trend Micro Full Disk Encryption.pkg` is unable to execute. Check that you have privileges to run executable files and try again.

Script Arguments

The table below explains the arguments available for building scripts to automatically install agents.

TABLE 6-7. Full Disk Encryption Script Arguments

ARGUMENT	VALUE	NOTES
ENTERPRISE	Enterprise name	The name of the organization.
HOST	DNS hostname or IP address	The name or location of PolicyServer
USERNAME	• Group Administrator • Group Authenticator • Group User (if the allow install policy is enabled)	Enterprise Administrator or Authenticator account cannot be used to install Full Disk Encryption
PASSWORD	Password for specified user name	The fixed password configured in PolicyServer for the user, or a domain password

Note

Encryption Management for Microsoft BitLocker uses the same script as Full Disk Encryption.

TABLE 6-8. File Encryption Script Arguments

ARGUMENT	VALUE	NOTES
PSENTERPRISE	Enterprise name	The name of the organization.
PSHOST	DNS hostname or IP address	The name or location of PolicyServer.
FAUSERNAME	• Group Administrator • Group Authenticator • Group User (if the allow install policy is enabled)	Enterprise Administrator or Authenticator account cannot be used to install File Encryption
FAPASSWORD	Password for specified user name	The fixed password configured in PolicyServer for the user, or a domain password

Command Line Installer Helper

Full Disk Encryption and File Encryption are compliant with automated software distribution tools, such as SMS, SCCM, Tivoli, GPO, and LANDesk. Use the Command Line Installer Helper to generate scripts used to install any Endpoint Encryption product. Options allow for encrypting and hiding installation account information, and selecting various prompt options. Script results are easily copied to the clipboard for export.

Note

Command line installation of PolicyServer is supported in versions 3.1.2 and higher.

When using the Command Line Installer Helper:

- Only run installation scripts on an endpoint, not from the network
- Run scripts with a Local Administrator account
- Test installation scripts in a pilot program before mass deployment
- Review all Full Disk Encryption, File Encryption, Encryption Management for Microsoft BitLocker, or Encryption Management for Apple FileVault pre-installation checklist items before executing any mass distribution of software

Creating Agent Installation Scripts

The following information is required to generate a silent install script: PolicyServer host name or IP address, the Enterprise name, user name, password, and the path and version number of the endpoint client installer. The Command Line Installer Helper is available in the **Tools** folder of the installation directory.

Procedure

1. Double-click `CommandLineInstallerHelper.exe`.

The **Command Builder** screen appears.

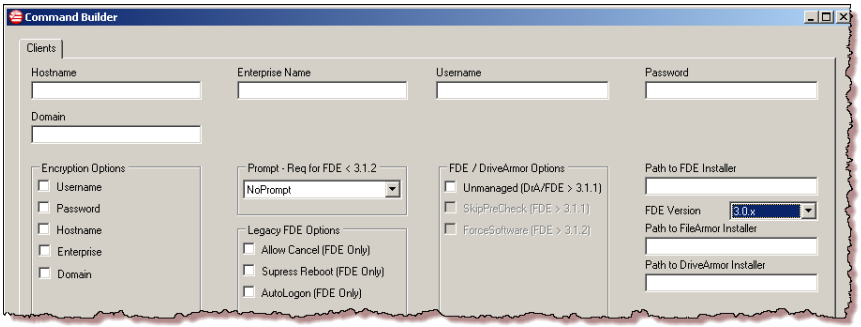


FIGURE 6-3. Command Line Helper Installer

2. Specify the required PolicyServer server name (hostname), Enterprise, and Enterprise Administrator user name and password.

OPTION	DESCRIPTION
Server name	Specify the PolicyServer IP address or host name, and include the port number assigned to that configuration.
Enterprise	Specify the Enterprise. Only one Enterprise is supported.
User name	Specify the user name of an account with permission to add devices to the Enterprise.
Password	Specify the password for the user name.

3. Select the encryption options.
   - User name
   - Password
   - Hostname
   - Enterprise
   - Domain
4. Select whether to prompt the end user, or to do a silent installation.

5. Specify legacy options that affect only older versions of Full Disk Encryption agent.
   - **Allow Cancel**: The end user may cancel the installation
   - **Suppress Reboot**: The endpoint does not restart after installation
   - **Autologon**: The user is automatically logged on the Full Disk Encryption preboot logon after installing the Full Disk Encryption agent and restarting the endpoint
6. Specify the path to the installation files.
7. Click **Generate Command**.

   The script generates.
8. Click the appropriate button to copy the command.

   The resulting script is copied to the clipboard.
9. Paste the command into the installation script.

Command Line Helper

The Command Line Helper is used to create encrypted values that can then be used to secure credentials when you are scripting an install for deployment or using DAAutoLogin. The Command Line Helper tool is located in the `Tools` folder.

Note

The Command Line Helper can only run on systems with Trend Micro Endpoint Encryption products installed as it makes use of the MobileArmor cryptographic.

The Command Line Helper tool accepts a single string as an argument and returns an encrypted value for in the installation script. The leading and trailing "=" signs are included as part of the complete encrypted string and must be included on the command line. If the value is encrypted and does not return a leading = sign, then an equal sign must be added to the script.

Options allow encrypting and hiding installation account information, and selecting various prompt options. Script results are easily copied to the clipboard for export.

TABLE 6-9. Arguments for Command Line Helper

FUNCTION	ARGUMENTS		
	FULL DISK ENCRYPTION	FULL DISK ENCRYPTION ENCRYPTED	FILE ENCRYPTION
Enterprise	**ENTERPRISE**	**eENTERPRISE**	
PolicyServer	**HOST**	**eHOST**	**PSHOST**
User name	**USERNAME**	**eUSERNAME**	**FAUSERNAME**
Password	**PASSWORD**	**ePASSWORD**	**FAPASSWORD**

Note

The File Encryption Installer automatically handles encrypted values.

Full Disk Encryption Script Example

Only one value can be passed to Command Line Helper. However, it can be run as many times as required to gather all needed encrypted values.

```
Software location = C:\Program Files\Trend Micro\Full Disk
Encryption\TMFDEInstaller.exe

ENTERPRISE = MyCompany

HOST = PolicyServer.mycompany.com

eUSERNAME = GroupAdministrator

ePASSWORD = 123456
```

Note

In this example, both the user name and the password are encrypted.

Output to install Full Disk Encryption:

```
C:\Program Files\Trend Micro\
Full Disk Encryption\TMFDEInstaller.exe
ENTERPRISE=MyCompany HOST= PolicyServer.mycompany.com
eUSERNAME==jJUJC/Lu4C/Uj7yYwxubYhAuCrY4f7AbVFp5hKo2PR4O
ePASSWORD==5mih67uKdy7T1VaN2ISWGQQ=
```

File Encryption Script Example

This is an example of an installation script to install File Encryption.

```
Software location = C:\Program Files\Trend Micro\File
Encryption\FileEncryptionIns.exe

PSEnterprise = MyCompany

PSHost = PolicyServer.mycompany.com

FAUser = GroupAdministrator

FAPassword = 123456
```

Note

In this example, both user name and password will be encrypted.

Output to install File Encryption:

```
C:\Program Files\Trend Micro\
File Encryption\FileEncryptionIns.exe
PSEnterprise=MyCompany PSHost= PolicyServer.mycompany.com
FAUser==jJUJC/Lu4C/Uj7yYwxubYhAuCrY4f7AbVFp5hKo2PR4O=
FAPassword==5mih67uKdy7T1VaN2ISWGQQ=
```

Encryption Management for Apple FileVault Script Example

This is an example of an installation script to install Encryption Management for Apple FileVault.

```
Software location = /Library/Application Support/TrendMicro/
FDEMM/RegisterDevice

ENTERPRISE = MyCompany

HOST = 10.1.152.58

USERNAME = User

ePASSWORD = 5mih67uKdy7TlVaN2ISWGQQ
```

Note

In this example the password is encrypted.

Output to install Encryption Management for Apple FileVault:

```
$ sudo "/Library/Application Support/TrendMicro/FDEMM/
RegisterDevice"
HOST=10.1.152.58 ENTERPRISE=MyCompany USERNAME=User
ePASSWORD==5mih67uKdy7TlVaN2ISWGQQ=
```

Using Command Line Helper

Adminstrators can use the Command Line Helper and DAAutoLogin together for seamless Full Disk Encryption patch management. Command Line Helper enables encrypted values to pass via the installation script to the Full Disk Encryption preboot. `DAAutoLogin` grants a one-time bypass of the Full Disk Encryption preboot.

Procedure

1. Copy `CommandLineHelper.exe` locally to Full Disk Encryption device.

   Example: Copy `CommandLineHelper.exe` to the `C:\` drive.

2. Open command prompt and type `C:\CommandLineHelper.exe`, then specify the user name or password.

   For example, use the following command if the user name is SMSUser:

   ```
   C:\CommandLineHelper.exe SMSUser
   ```

3. Press ENTER to display the encrypted value.
4. Run Command Line Helper again for the second encrypted value. If the first time was the user name, run it again to encrypt the password.

Upgrade

To gain access to new product features or to upgrade older agent software for improved endpoint security, administrators may need to upgrade the Endpoint Encryption PolicyServer and all managed endpoints running any Endpoint Encryption agent. For policy synchronization and information security, make sure to always upgrade PolicyServer before the Endpoint Encryption agents.

This section explains how to safely upgrade Endpoint Encryption, including PolicyServer, PolicyServer MMC, and the Endpoint Encryption agent software to the most current versions.

WARNING!

Before upgrading the agent, make sure to first upgrade PolicyServer to version 5.0 Patch 3. Endpoint Encryption 5.0 Patch 3 agents cannot communicate with PolicyServer 3.1.3 or earlier.

Upgrading the Endpoint to Windows 8

Endpoint Encryption does not support upgrading to Windows 8. If an upgrade is required, Trend Micro recommends following this procedure to prevent data loss when Full Disk Encryption or File Encryption is already installed on the agent.

Procedure

1. Decrypt the endpoint.

   For more information, see appropriate section for that agent in the *Endpoint Encryption Administrator's Guide*.

2. Uninstall the agent.

- To use OfficeScan, see *Using OfficeScan to Uninstall Endpoint Encryption Agents on page 6-64*.
- To manually uninstall Full Disk Encryption, see *Uninstalling Full Disk Encryption on page 6-59*.
- To manually uninstall File Encryption, see *Uninstalling File Encryption on page 6-63*.
- To manually uninstall Encryption Management for Microsoft BitLocker, see *Uninstalling Encryption Management for Microsoft BitLocker on page 6-62*.

3. Install the Windows 8 operating system.

Note

This documentation does not explain how to install Windows 8. For instructions, see the associated user documentation from Microsoft.

4. Verify that the Windows 8 environment is stable and that the upgrade was successful.
5. Re-install agent applications:
   - For information about installing Full Disk Encryption, see *Full Disk Encryption Deployment on page 6-6*.
   - For information about installing File Encryption, see *File Encryption Deployment on page 6-28*.

Upgrading Full Disk Encryption

Before you begin

- Verify *Full Disk Encryption System Requirements on page 2-9*
- Review *Upgrade Paths on page 3-23*

Use the Full Disk Encryption installer to upgrade the agent from Full Disk Encryption 3.1.3 SP1 to Full Disk Encryption 5.0 Patch 3. For previous versions of Full Disk Encryption, see the associated documentation available at:

http://docs.trendmicro.com/en-us/enterprise/endpoint-encryption.aspx

Procedure

1. Copy the installation package to the local hard drive.
2. Run `TMFDEInstall.exe`.

   Note

   If the **User Account Control** windows displays, click **Yes** to allow the installer to make changes to the Endpoint Encryption device.

   The following message appears above the system tray.

3. Wait for the upgrade to finish.
4. At the confirmation dialog box, click **Yes** to reboot the endpoint.

Important Notes for the MobileArmor Full Disk Encryption Product Service Pack 7 and earlier

When upgrading from the MobileArmor Full Disk Encryption product Service Pack 7 and earlier:

- In the BIOS verify the disk controller is set to ATA or AHCI mode.
- For laptops that use a multi-bay, only install the agent while not docked.

Intel™ Rapid Recovery Technology (IRRT):

- Some newer systems support IRRT in the BIOS.
- If the BIOS disk controller is set to IRRT mode, it will need to be changed to AHCI mode prior to Full Disk Encryption installation.
- IRRT must be supported by the OS.

Intel™ Matrix Manager software:

- By default Window XP does not have Intel Matrix Manager software installed. Settings must be made in BIOS without an OS rebuild.
- Windows Vista has Intel Matrix Manager software by default.

Note

If the SATA Operation setting in Windows Vista is changed and Full Disk Encryption is installed, then Windows will not boot. Change back to IRRT and Vista will load normally.

Upgrading File Encryption

Before you begin

- Verify *File Encryption System Requirements on page 2-13*
- Review *Upgrade Paths on page 3-23*

Use `FileEncryptionIns.exe` to upgrade the agent from a previous version.

Note

`FileEncryptionIns.exe` overrides the Allow User to Uninstall policy and upgrades whether the policy is set to **Yes** or **No**.

Procedure

1. Run `FileEncryptionIns.exe`.

Windows installer uninstalls the older File Encryption agent (FileArmor) and then installs File Encryption 5.0 Patch 3.

2. Wait for the endpoint to restart.

3. After Windows loads, log on and check the new File Encryption folder. Encrypted files and folders are maintained.

Upgrading Encryption Management for Apple FileVault

The process for upgrading is the same as it is for installation. Make sure to have the PolicyServer information available.

Procedure

- Complete *Installing the Encryption Management for Apple FileVault Agent on page 6-25*.

Upgrading Encryption Management for Microsoft BitLocker

Procedure

1. Complete *Uninstalling Encryption Management for Microsoft BitLocker on page 6-62*.

2. Wait for endpoint decryption to complete. The user can use the endpoint as usual.

3. Complete Encryption Management for Microsoft BitLocker at *Installing the Encryption Management for Microsoft BitLocker Agent on page 6-16*.

Migration

Administrators may need to migrate Endpoint Encryption devices when employees move to a different department or office location. One PolicyServer instance may have multiple Enterprise configurations that each represent a business unit or department.

Moving to a new Enterprise removes the Endpoint Encryption device from the old Enterprise and adds the Endpoint Encryption device to the new Enterprise within the same PolicyServer instance.

Moving to a new PolicyServer does not remove the Endpoint Encryption device from the old PolicyServer, but changes the network configuration in the Endpoint Encryption agent to point to the new PolicyServer instance.

Replacing a Previously Installed Encryption Product

Full Disk Encryption can be installed on a device that was previously encrypted with a different full disk encryption product. As most encryption software modifies every sector on a hard drive, it is critical to test the disk preparation process and deployment strategy. Depending on the time required to decrypt a device and encrypt with Full Disk Encryption, it may be as simple as backing up user data and re-imaging the endpoint before installing Full Disk Encryption.

Option 1: Remove Previous Encryption Product

Procedure

1. Decrypt the disk using the defined method as provided by the software vendor.
2. Uninstall the previously installed vendor's software (or verify BitLocker is disabled).
3. Reboot the device.
4. Run `chkdsk` and defragment the drive.
5. Check each device for a Normal Master Boot Record (MBR) and confirm that a Normal Boot Sector is present on the boot partition.

Note

The device cannot be a dual-boot machine.

6. Back up user files.
7. Install Full Disk Encryption. For more information, see *Full Disk Encryption Installation on page 6-11*.

Option 2: Back Up and Re-image the Endpoint

Procedure

1. Backup user files.
2. Re-image the drive:
   a. From a command prompt, run `DiskPart Clean All`.
   b. Create a partition.
   c. Format the drive.
   d. Image the drive.
3. Install Full Disk Encryption and encrypt the endpoint.
4. Restore user files.

Full Disk Encryption PolicyServer Settings

Full Disk Encryption PolicyServer settings are configurable by going to the Recovery Console from the Full Disk Encryption preboot or by running `C:\Program Files\Trend Micro\Full Disk Encryption\RecoveryConsole.exe`.

Recovery Console Requirement

Use the Full Disk Encryption Recovery Console to change PolicyServer settings.

Accessing Recovery Console from Full Disk Encryption Preboot

Only Enterprise or Group Administrator and Authenticator accounts can access Recovery Console.

Procedure

1. To allow users to access Recovery Console, enable the following policy:

   Full Disk Encryption > **Agent** > **Allow User Recovery**

2. Reboot the endpoint.

   The Full Disk Encryption preboot appears.

3. Select the **Recovery Console** check box.

4. Specify Endpoint Encryption user account credentials.

5. Click **Login**.

   Recovery Console opens.

Accessing Recovery Console from Windows

Procedure

1. In Windows, go to the Full Disk Encryption installation directory.

   The default location is `C:\Program Files\Trend Micro\Full Disk Encryption\`.

2. Open `RecoveryConsole.exe`.

   The **Recovery Console** window appears.

3. Specify the Endpoint Encryption user name and password, then click **Login**.

Recovery Console opens to the **Decrypt Disk** page.

Migrating Full Disk Encryption to a New Enterprise

One PolicyServer instance may have multiple Enterprise configurations that each represent a business unit or department. Moving to a new Enterprise removes the Endpoint Encryption device from the old Enterprise and adds the Endpoint Encryption device to the new Enterprise within the same PolicyServer instance. The Full Disk Encryption agent may need to move to a new Enterprise when the employee moves to a different department or office location.

Note

For information about changing the PolicyServer that manages the Full Disk Encryption agent, see *Changing the Full Disk Encryption PolicyServer on page 6-56*.

Changing the Enterprise requires access to Full Disk Encryption Recovery Console. For more information, see *Full Disk Encryption PolicyServer Settings on page 6-52*.

WARNING!

Changing the Enterprise requires configuring policies again, recreating groups, and deletes all cached passwords, password history, and audit logs.

Procedure

1. Click **Network Setup**.
2. Select the **PolicyServer** tab.
3. Click **Change Enterprise**.

The **Change Enterprise** screen appears.

FIGURE 6-4. Recovery Console Change Enterprise

4. Configure the following options:

OPTION	DESCRIPTION
New Server User	Specify an Enterprise Administrator account user name, or the user name of an account with permission to install to the Enterprise or group in the new PolicyServer.
New User Password	Specify the password for the Enterprise Administrator account.
New Server Address	Specify the new PolicyServer IP address or host name.
New Enterprise	Specify the new PolicyServer Enterprise.

5. Click **Save**.

Full Disk Encryption validates the new PolicyServer information.

6. At the confirmation message, click **OK**.

Migrating Endpoints to a New PolicyServer

This section explains how to change the PolicyServer that controls Endpoint Encryption agent policies. The Endpoint Encryption agent may need to migrate to a different PolicyServer if the endpoint moves to another department that is managed by a different PolicyServer instance or when there are network factors that required PolicyServer to change its IP address or host name. After migrating to the new PolicyServer, the endpoint registers as a new Endpoint Encryption device in the new PolicyServer database and the previously registered Endpoint Encryption device is removed from the old PolicyServer database.

Changing the Full Disk Encryption PolicyServer

Note

Changing the PolicyServer requires access to Full Disk Encryption Recovery Console. For more information, see *Full Disk Encryption PolicyServer Settings on page 6-52*.

Procedure

1. From the Full Disk Encryption Recovery Console, click the **PolicyServer** tab.
2. Click **Change Server**.
3. At the warning message, click **Yes**.
4. Specify the new server address.
5. Click **Save**.

Changing the Encryption Management for Apple FileVault PolicyServer

For information about why Endpoint Encryption agents may need to change the PolicyServer that manages policies, see *Migrating Endpoints to a New PolicyServer on page 6-56*.

Procedure

1. Uninstall the Encryption Management for Apple FileVault agent.

   See *Uninstalling Encryption Management for Apple FileVault on page 6-61*.

2. Wait for the hard drive decryption to complete. The user can use the endpoint as usual.

3. Remove the device from the old PolicyServer.

   a. Log on to PolicyServer MMC.

   b. Right-click the Endpoint Encryption device, and then select **Remove Device**.

   c. Click **Yes** to confirm.

   For more information about removing Endpoint Encryption devices, see the *Endpoint Encryption Administrator's Guide*.

4. Follow the fresh install instructions to reinstall Encryption Management for Apple FileVault at *Installing the Encryption Management for Apple FileVault Agent on page 6-25*. Make sure to specify the new PolicyServer credentials.

5. To confirm the migration, go to either the Control Manager Endpoint Encryption Devices widgets or log on the PolicyServer MMC that manages the new PolicyServer.

Changing the Encryption Management for Microsoft BitLocker PolicyServer

For information about why Endpoint Encryption agents may need to change the PolicyServer that manages policies, see *Migrating Endpoints to a New PolicyServer on page 6-56*.

Procedure

1. Uninstall the Encryption Management for Microsoft BitLocker agent.

   See *Uninstalling Encryption Management for Microsoft BitLocker on page 6-62*.

2. Wait for the hard drive decryption to complete. The user can use the endpoint as usual.

3. Remove the device from the old PolicyServer.

   a. Log on to PolicyServer MMC.

   b. Right-click the Endpoint Encryption device, and then select **Remove Device**.

   c. Click **Yes** to confirm.

   For more information about removing Endpoint Encryption devices, see the *Endpoint Encryption Administrator's Guide*.

4. Follow the fresh install instructions to reinstall Encryption Management for Microsoft BitLocker at *Installing the Encryption Management for Microsoft BitLocker Agent on page 6-16*. Make sure to specify the new PolicyServer credentials.

5. To confirm the migration, go to either the Control Manager Endpoint Encryption Devices widgets or log on the PolicyServer MMC that manages the new PolicyServer.

Changing the File Encryption PolicyServer

For information about why Endpoint Encryption agents may need to change the PolicyServer that manages policies, see *Migrating Endpoints to a New PolicyServer on page 6-56*.

Procedure

1. Right-click the File Encryption tray icon and select **About File Encryption**.
2. Click **Edit PolicyServer**.
3. Specify the new PolicyServer IP address or host name and then click **OK**.

Uninstallation

During an upgrade, some Endpoint Encryption agents require first manually uninstalling the old Endpoint Encryption agent software. If the Endpoint Encryption agent software is malfunctioning in some way, uninstalling and reinstalling the Endpoint Encryption agent software may solve the problem.

The following section explains how to manually uninstall the Endpoint Encryption agent software or use OfficeScan to deploy the uninstallation command simultaneously to multiple managed endpoints.

Manually Uninstalling Endpoint Encryption Agents

The following section explains how to manually uninstall Endpoint Encryption agents using the program installer. Uninstalling the Endpoint Encryption agent software may be a necessary step to resolve a problem or to upgrade the Endpoint Encryption agent software.

Uninstalling Full Disk Encryption

During an upgrade, some Endpoint Encryption agents require first manually uninstalling the old Endpoint Encryption agent software. If the Endpoint Encryption agent software

is malfunctioning in some way, uninstalling and reinstalling the Endpoint Encryption agent software may solve the problem.

Note

To uninstall Endpoint Encryption agents, the user account must have uninstall rights within the group or policy that the Endpoint Encryption devices are registered to and have local administrator rights.

Tip

Any User or Group Authenticator can run the uninstaller in Windows if the policy **Full Disk Encryption** > **Agent** > **Allow User to Uninstall** = **Yes**.

Procedure

1. Log on to the Full Disk Encryption preboot and then Windows.
2. From Windows, go to `C:\Program Files\Trend Micro\Full Disk Encryption` and run TMFDEUninstall.exe.

   Note

   If prompted by **User Account Control**, click **Yes**.

   The **Full Disk Encryption Uninstall** window opens.
3. Click **Next**.

   Full Disk Encryption begins to uninstall.
4. Click **OK** to confirm hard drive decryption.

   Note

   To view decryption status, open Full Disk Encryption from the system tray.
5. When decryption completes, click **OK**.
6. Run `TMFDEUninstall.exe` again to finish the uninstall.

7. Reboot the device.

> **Note**
> The device record is not automatically removed and must be manually removed from PolicyServer.

Uninstalling Encryption Management for Apple FileVault

Uninstalling the Encryption Management for Apple FileVault agent requires access to the Mac OS X Terminal application.

For information about installing Encryption Management for Apple FileVault, see *Encryption Management for Apple FileVault Installation on page 6-25*.

To uninstall Endpoint Encryption agents, the user account must have uninstall rights within the group or policy that the Endpoint Encryption devices are registered to and have local administrator rights.

> **Tip**
> Any User or Group Authenticator can run the uninstaller if the policy **Full Disk Encryption** > **Agent** > **Allow User to Uninstall** = **Yes**.

Procedure

1. Go to **Applications** > **Utilities** and double-click **Terminal**.

   The Terminal window appears.

2. Type `cd /Library/Application Support/TrendMicro/FDEMM`

3. Type `sudo ./Uninstaller`

   During automated uninstallations on Mac OS X Yosemite, the user must confirm that they want to restart the endpoint if the the device requires decryption before uninstallation. To automate this confirmation, users can append the parameter `RebootWithoutConfirm`.

   The following is an example command that automates restart confirmation:

```
sudo ./Uninstaller RebootWithoutConfirm
```

The agent uninstalls in the background.

4. Restart the endpoint to complete the uninstallation.

Uninstalling Encryption Management for Microsoft BitLocker

Use **Windows Add or Remove Programs** to uninstall Encryption Management for Microsoft BitLocker.

Note

To uninstall Endpoint Encryption agents, the user account must have uninstall rights within the group or policy that the Endpoint Encryption devices are registered to and have local administrator rights.

Tip

Any User or Group Authenticator can run the uninstaller in Windows if the policy **Full Disk Encryption** > **Agent** > **Allow User to Uninstall** = **Yes**.

Procedure

1. Go to **Start** > **Settings** > **Control Panel** > **Add or Remove Programs**

   The **Add or Remove Programs** window appears.

2. Select Encryption Management for Microsoft BitLocker from the list of installed programs.

3. Click **Remove**.

4. At the **Add or Remove Programs** message, click **Yes** to confirm.

The uninstall process completes when the program is removed from the list.

Uninstalling File Encryption

Use **Windows Add or Remove Programs** to uninstall File Encryption.

Note

To uninstall Endpoint Encryption agents, the user account must have uninstall rights within the group or policy that the Endpoint Encryption devices are registered to and have local administrator rights.

Tip

Any User or Group Authenticator can run the uninstaller in Windows if the policy **Full Disk Encryption** > **Agent** > **Allow User to Uninstall** = **Yes**.

Note

- Set the **Policies** > **File Encryption** > **Computer** > **Allow User to Uninstall** to **Yes** to allow any User or Group Authenticator to run the uninstaller in Windows.
- Save and close all documents before starting the uninstall process. A reboot is required when the uninstaller completes.

WARNING!

Decrypt all encrypted files before uninstalling File Encryption. Otherwise, they will become unreadable.

Procedure

1. Log on to File Encryption with an account that has permission to uninstall File Encryption.
2. Open the **Windows Start Menu** and go to **Control Panel** > **Programs** > **Uninstall a Program**.
3. Select File Encryption from the list and then click **Uninstall**.

Using OfficeScan to Uninstall Endpoint Encryption Agents

During an upgrade, some Endpoint Encryption agents require first manually uninstalling the old Endpoint Encryption agent software. If the Endpoint Encryption agent software is malfunctioning in some way, uninstalling and reinstalling the Endpoint Encryption agent software may solve the problem.

During an upgrade, some Endpoint Encryption agents require first manually uninstalling the old Endpoint Encryption agent software. If the Endpoint Encryption agent software is malfunctioning in some way, uninstalling and reinstalling the Endpoint Encryption agent software may solve the problem.

This procedure explains how to uninstall Endpoint Encryption agents using the OfficeScan Endpoint Encryption Deployment Tool plug-in.

Procedure

1. Select the Endpoint Encryption device.

   Note

   To select multiple Endpoint Encryption devices, hold SHIFT and select applicable endpoints.

2. Click **Uninstall** and select the appropriate Endpoint Encryption agent from the drop-down list.
3. Click **OK** to confirm the deployment.

   The Endpoint Encryption agent uninstall command is deployed.

4. The Endpoint Encryption agent uninstallation is complete when OfficeScan displays the confirmation message.

Note

All future deployment commands fail if the Endpoint Encryption device is not restarted after the uninstall command is initiated and completes.

If the uninstall cannot complete, follow the manual uninstallation process at *Uninstallation on page 6-59*.

When uninstallation completes, the Endpoint Encryption agent is removed and the product folder is deleted from the endpoint.

Chapter 7

OfficeScan Integration

The following content explains how to use the Endpoint Encryption Deployment Tool OfficeScan plug-in to deploy Endpoint Encryption across an enterprise with endpoints managed by OfficeScan.

Topics include:

- *About Trend Micro OfficeScan Integration on page 3-8*
- *Installing OfficeScan on page 7-3*
- *About Plug-in Manager on page 7-4*
- *Endpoint Encryption Deployment Tool Installation on page 7-5*
- *Plug-in Program Management on page 7-6*
- *Using Plug-in Programs on page 7-7*
- *Managing the Agent Tree on page 7-9*
- *Endpoint Encryption Agent Deployment on page 7-12*

About Trend Micro OfficeScan Integration

OfficeScan protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks. An integrated solution, OfficeScan consists of an agent that resides at the endpoint and a server program that manages all agents.

The agent guards the endpoint and reports its security status to the server. The server, through the web-based management console, makes it easy to set coordinated security policies and deploy updates to every agent.

Note

For information about OfficeScan, see the supporting documentation at:

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

Use the OfficeScan Endpoint Encryption Deployment Tool plug-in to deploy Endpoint Encryption agents to OfficeScan managed endpoints. You can select endpoints based on specific criteria and see the status of the deployment. After the Endpoint Encryption Deployment Tool plug-in deploys the Endpoint Encryption agent software, the Endpoint Encryption agent synchronizes to PolicyServer using the settings specified in the plug-in. OfficeScan does not manage Endpoint Encryption policies. The OfficeScan agent and the Endpoint Encryption agent are independent on the same endpoint.

The following illustration explains how to deploy Endpoint Encryption for the first time on OfficeScan managed endpoints. In OfficeScan deployments, administrators can use either Control Manager or PolicyServer MMC to manage PolicyServer.

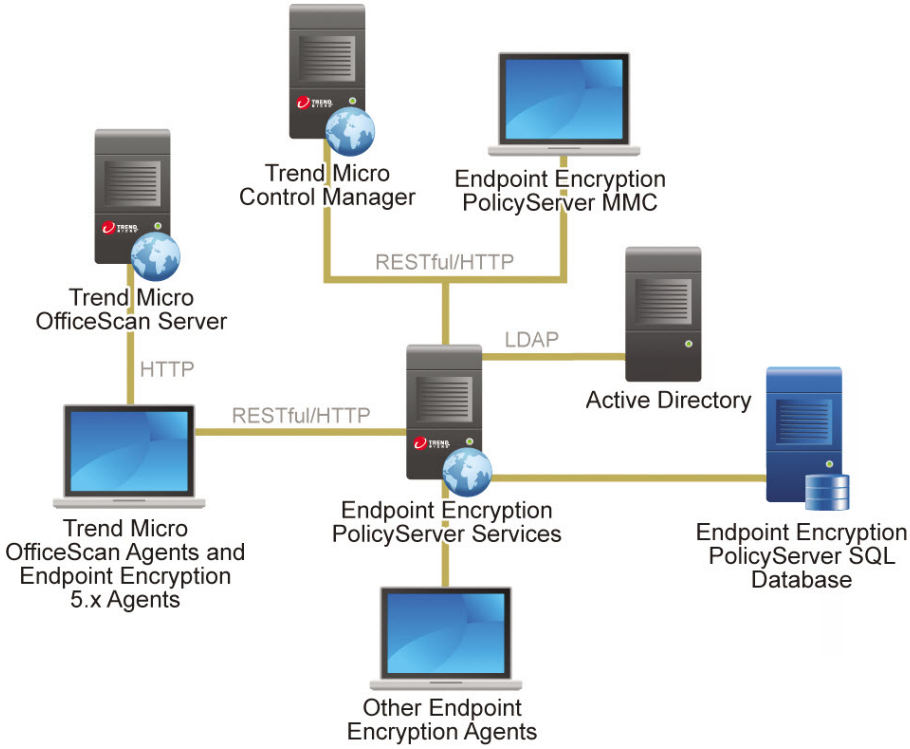


FIGURE 7-1. OfficeScan integration deployment

Installing OfficeScan

For information about installing and configuring OfficeScan, see the documentation available at:

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

For information about installing and configuring the OfficeScan Endpoint Encryption Deployment Tool before deploying Endpoint Encryption agents, see the *Endpoint Encryption Installation and Migration Guide* for installation and configuration options.

About Plug-in Manager

OfficeScan includes a framework called Plug-in Manager that integrates new solutions into the existing OfficeScan environment. To help ease the management of these solutions, Plug-in Manager provides at-a-glance data for the solutions in the form of widgets.

Note

None of the plug-in solutions currently support IPv6. The server can download these solutions but is not able to deploy the solutions to pure IPv6 Endpoint Encryption agents or pure IPv6 hosts.

Plug-in Manager delivers two types of solutions:

- **Native Product Features**

  Some native OfficeScan features are licensed separately and activated through Plug-in Manager. In this release, two features fall under this category, namely, **Trend Micro Virtual Desktop Support** and **OfficeScan Data Protection**.

- **Plug-in programs**

  Plug-in programs are not part of the OfficeScan program. The plug-in programs have separate licenses and management consoles. Access the management consoles from within the OfficeScan web console. Examples of plug-in programs are **Intrusion Defense Firewall**, **Trend Micro Security (for Mac)**, and **Trend Micro Mobile Security**.

This document provides a general overview of plug-in program installation and management and discusses plug-in program data available in widgets. Refer to specific plug-in program documentation for details on configuring and managing the program.

Endpoint Encryption Deployment Tool Installation

Plug-in programs display on the **Plug-in Manager** console. Use the console to download, install, and manage the programs. Plug-in Manager downloads the installation package for the plug-in program from the Trend Micro ActiveUpdate server or from a custom update source, if one has been properly set up. An Internet connection is necessary to download the package from the ActiveUpdate server.

When Plug-in Manager downloads an installation package or starts the installation, Plug-in Manager temporarily disables other plug-in program functions such as downloads, installations, and upgrades.

Plug-in Manager does not support plug-in program installation or management from Trend Micro Control Manager's single sign-on function.

Installing Endpoint Encryption Deployment Tool

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.
2. On the **Plug-in Manager** screen, go to the plug-in program section and click **Download**.

   The size of the plug-in program package displays beside the **Download** button. .

   Monitor the progress or navigate away from the screen during the download.

   Note

   If OfficeScan encounters problems downloading or installing the package, check the server update logs on the OfficeScan web console. On the main menu, click **Logs** > **Server Update**.

3. Click **Install Now** or **Install Later**.
   - After clicking **Install Now**, the installation begins and an installation progress screen appears.

- After clicking **Install Later**, the **Plug-in Manager** screen appears.

  Install the plug-in program by clicking the **Install** button located in the plug-in program's section on the **Plug-in Manager** screen.

The **Trend Micro End User License Agreement** screen appears.

> **Note**
>
> Not all plug-in programs require this screen. If this screen does not appear, the plug-in program installation begins.

4. Click **Agree** to install the plug-in program.

   Monitor the progress or navigate away from the screen during the installation.

> **Note**
>
> If OfficeScan encounters problems downloading or installing the package, check the server update logs on the OfficeScan web console. On the main menu, click **Logs** > **Server Update**.

After the installation, the current plug-in program version displays on the **Plug-in Manager** screen.

Plug-in Program Management

Configure settings and perform program-related tasks from the plug-in program's management console, which is accessible from the OfficeScan web console. Tasks include activating the program and possibly deploying the plug-in program agent to endpoints. Consult the documentation for the specific plug-in program for details on configuring and managing the program.

Managing Endpoint Encryption Deployment Tool

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.
2. On the **Plug-in Manager** screen, go to the plug-in program section and click **Manage Program**.

Using Plug-in Programs

This section describes how to install and manage the OfficeScan Endpoint Encryption Deployment Tool plug-in program.

Plug-in Program Management

Configure settings and perform program-related tasks from the plug-in program's management console, which is accessible from the OfficeScan web console. Tasks include activating the program and possibly deploying the plug-in program agent to endpoints. Consult the documentation for the specific plug-in program for details on configuring and managing the program.

Managing Endpoint Encryption Deployment Tool

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.
2. On the **Plug-in Manager** screen, go to the plug-in program section and click **Manage Program**.

Endpoint Encryption Deployment Tool Upgrades

A new version of an installed plug-in program displays on the Plug-in Manager console. Download the package and upgrade the plug-in program on the console. Plug-in Manager downloads the package from the Trend Micro ActiveUpdate server or a custom update source, if one has been properly set up. An Internet connection is necessary to download the package from the ActiveUpdate server.

When Plug-in Manager downloads an installation package or starts an upgrade, Plug-in Manager temporarily disables other plug-in program functions such as downloads, installations, and upgrades.

Plug-in Manager does not support plug-in program upgrading using the Trend Micro Control Manager single sign-on function.

Upgrading Endpoint Encryption Deployment Tool

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.
2. On the **Plug-in Manager** screen, go to the plug-in program section and click **Download**.

   The size of the upgrade package displays beside the **Download** button.
3. Monitor the download progress.

   Navigating away from the screen during the download does not affect the upgrade.

   Note

   If OfficeScan encounters problems downloading or installing the package, check the server update logs on the OfficeScan web console. On the main menu, click **Logs** > **Server Update**.
4. After Plug-in Manager downloads the package, a new screen displays.

After the upgrade, the Plug-in Manager service may need to restart, causing the **Plug-in Manager** screen to be temporarily unavailable. When the screen becomes available, the current plug-in program version displays.

Endpoint Encryption Deployment Tool Uninstallation

Uninstall a plug-in program in the following ways:

- Uninstall the plug-in program from the Plug-in Manager console.
- Uninstall the OfficeScan server, which uninstalls Plug-in Manager and all installed plug-in programs. For instructions on uninstalling the OfficeScan server, see the *OfficeScan Installation and Upgrade Guide*.

Uninstalling Endpoint Encryption Deployment Tool from the Plug-in Manager Console

Procedure

1. Open the OfficeScan web console and click **Plug-in Manager** in the main menu.
2. On the **Plug-in Manager** screen, go to the plug-in program section and click **Uninstall**.
3. Monitor the uninstallation progress or navigate away from the screen during the uninstallation.
4. Refresh the **Plug-in Manager** screen after the uninstallation.

   The plug-in program is again available for installation.

Managing the Agent Tree

The OfficeScan Agent Tree

The OfficeScan agent tree displays all the agents grouped into domains that the server currently manages. Agents are grouped into domains so you can simultaneously configure, manage, and apply the same configuration to all domain members.

Agent Tree Specific Tasks

The agent tree displays when you access certain screens on the web console. Above the agent tree are menu items specific to the screen you have accessed. These menu items allow you to perform specific tasks, such as configuring agent settings or initiating agent tasks. To perform any of the tasks, first select the task target and then select a menu item.

The agent tree provides access to the following functions:

- **Search for endpoints**: Locate specific endpoints by typing search criteria in the text box.
- **Synchronize with OfficeScan**: Synchronize the plug-in program's agent tree with the OfficeScan server's agent tree. For details, see *Synchronizing the Agent Tree on page 7-10*.
- **Deploy Server Settings**: Displays the **Deploy Server Settings** screen. For details, see *Deploying Server Settings on page 7-11*.

Administrators can also manually search the agent tree to locate endpoints or domains. Specific computer information displays in the table on the right.

Synchronizing the Agent Tree

Before the plug-in program can deploy settings to agents, administrators need to synchronize the agent tree with the OfficeScan server.

Procedure

1. Open the plug-in console.
2. On the **Client Management** screen, click **Synchronize with OfficeScan**.

A confirmation message screen appears.

3. Allow a few moments for the synchronization to complete.

4. Click **Close** to return to the **Client Management** screen.

Deploying Server Settings

Configure and deploy the PolicyServer settings to ensure communication between the agents and PolicyServer.

Procedure

1. Open the plug-in program console.

2. Click the **PolicyServer Settings** tab.

3. Specify the following details:

OPTION	DESCRIPTION
Server name	Specify the PolicyServer IP address or host name.
Port	Specify the port number assigned to the PolicyServer instance.
Enterprise	Specify the PolicyServer Enterprise. Only one Enterprise is supported.
User name	Specify the Enterprise Administrator user name.
Password	Specify the Enterprise Administrator password.

4. Click **Save**.

   A confirmation message appears. Allow some time to establish a server connection.

Endpoint Encryption Agent Deployment

This section describes how to use the Endpoint Encryption Deployment Tool Plug-in to initiate agent installation and uninstallation commands.

The following illustration shows the Endpoint Encryption Deployment Tool **Client Management** screen.

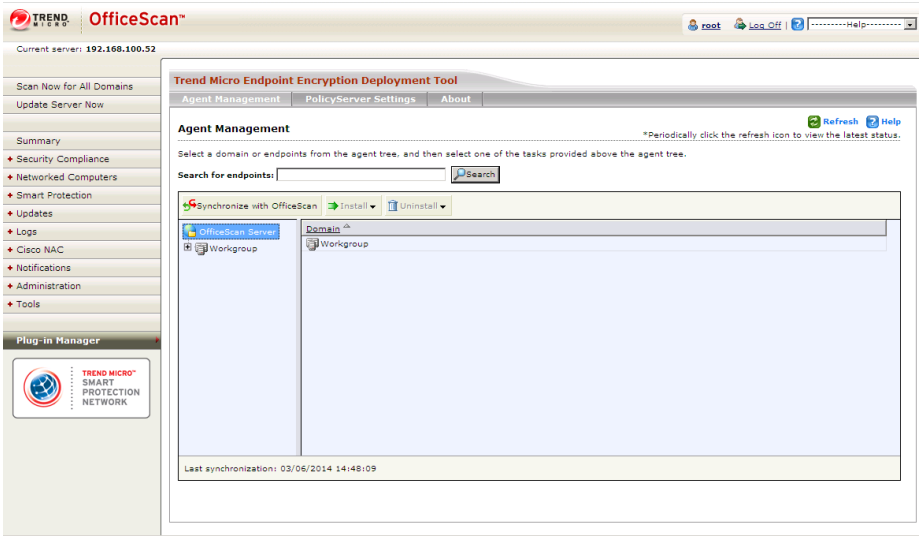


FIGURE 7-2. Endpoint Encryption Deployment Tool

Deploying the Agent with OfficeScan

Before deploying agents, make sure that the endpoints meet the minimum system requirements.

For more information, see *System Requirements on page 2-1*.

Procedure

1. Select the endpoint from the client tree.

Note

To select multiple endpoints, hold CTRL and select applicable endpoints.

2. Click **Install**, then select one of the following options:

Option	Description
Full Disk Encryption	Select the appropriate Full Disk Encryption agents. • Select the Full Disk Encryption agent to deploy all features, including preboot authentication, all policies, notifications, and device actions. • Select the Encryption Management for Microsoft BitLocker agent to enable Microsoft BitLocker full disk encryption, deploying only limited policies and device actions. **Note** It is not possible to deploy the Encryption Management for Apple FileVault agent using the Endpoint Encryption Deployment Tool plug-in.
File Encryption	Deploy the File Encryption agent, which includes all features and policies.

3. Click **Deploy**.
4. At the message, click **OK** to confirm the deployment.

   The agent deployment command is initiated. If successful, any selected endpoint is prompted to restart.

Confirming Agent Deployment

This task explains how to confirm that the Endpoint Encryption agent install initiates correctly on the endpoint.

Procedure

1. Complete *Deploying the Agent with OfficeScan on page 7-12*.

2. Log on to the selected Endpoint Encryption device.
3. Do one of the following:
   - To view the deployment status, open the log files at:

Client endpoint	`C:\TMEE_Deploy_Client.log`
Server endpoint	`C:\TMEE_Deploy_Server_Inst.log`

   - Run Task Manager and search one of the services at *Endpoint Encryption Agent Services on page 7-14*.
4. When the Endpoint Encryption agent deployment completes, reboot the endpoint to complete the installation.

Endpoint Encryption Agent Services

The following table explains the services running when the Endpoint Encryption agent initiates on the endpoint. Use it to verify that the agent has been successfully installed and is correctly functioning.

Note

For more information about Endpoint Encryption services, see *Endpoint Encryption Services on page D-1*.

SERVICE	STATUS
`FEService.exe`	The File Encryption agent is running.
`TMFDE.exe`	The Full Disk Encryption agent is running.
`TMFDEForBitLocker.exe`	The Encryption Management for Microsoft BitLocker agent is running.

Endpoint Encryption Agent Deployment Statuses

The following table explains the OfficeScan statuses that appear in the Endpoint Encryption Deployment Tool plug-in console after initiating a deployment command.

Use it to understand if there was a problem during the agent installation or uninstallation.

TABLE 7-1. Agent Installation Statuses

STATUS	MESSAGE	DESCRIPTION
In progress	In progress: agent deployment	OfficeScan is attempting to communicate with the managed endpoint, install the Endpoint Encryption agent, then establish a connection with PolicyServer.
Successful	Successful agent deployment	The Endpoint Encryption agent installed successfully, and has established communication with both OfficeScan and PolicyServer.
Unsuccessful	Unsuccessful agent deployment	The Endpoint Encryption agent deployment could not finish. Review the logs to find out why the managed endpoint could not update with the selected Endpoint Encryption agent.
Restart required	Successful agent deployment. Shutdown/Restart required.	For the Full Disk Encryption agent, a restart is required to complete the installation. The status is not updated until after the user has logged on the PolicyServer preboot.
Timeout	Timed out: agent deployment	The timeout period is 30 minutes. After a timeout, initiate a new deployment command.

TABLE 7-2. Agent Uninstallation Statuses

STATUS	MESSAGE	DESCRIPTION
In progress	Request in progress: agent deployment	OfficeScan is attempting to communicate with the managed endpoint and uninstall the agent software. The managed endpoint must reply to the deployment command before the uninstallation can start.
Successful	Successful agent uninstallation	The Endpoint Encryption agent uninstalled successfully and has established communication with OfficeScan and PolicyServer. After uninstallation, the Endpoint Encryption device is removed from PolicyServer.
Unsuccessful	Unsuccessful agent uninstallation	The Endpoint Encryption agent uninstallation request could not establish a connection. Review the logs to find out why the managed endpoint could not uninstall the Endpoint Encryption.
Restart required	Successful agent uninstallation. Shutdown/ Restart required.	For some Endpoint Encryption agents, a restart is required to complete the uninstallation.
Timeout	Request timeout: agent uninstallation	The timeout period is 30 minutes. After a timeout, initiate a new uninstallation request.

Endpoint Encryption Agent Installation Error Codes

The following table describes the error codes for Endpoint Encryption agent installation errors. Use it to understand the problem and resolution for a specific installation error.

Note

Make sure that the endpoint meets the minimum system requirements before deploying Endpoint Encryption agents. Microsoft .Net Framework 2.0 SP1 or above is required. For information about system requirements, see the *Endpoint Encryption Installation and Migration Guide*.

TABLE 7-3. Installation Error Codes

AGENT	ERROR CODE	PROBLEM AND RESOLUTION
File Encryption	1603	Unable to install the Endpoint Encryption agent. A required resource may be unavailable. Restart the endpoint and try the installation again. If the problem persists, contact Trend Micro Support.
	1641	Unable to install the Endpoint Encryption agent. The system may require a restart to complete a previous uninstallation. Restart the endpoint and try the installation again. If the problem persists, contact Trend Micro Support.
Full Disk Encryption	-3	The user name or password is invalid. Verify the credentials and try to log on to PolicyServer again.
	-6	Unable to install the Endpoint Encryption agent. A required resource may be unavailable. Restart the endpoint and try the installation again. If the problem persists, contact Trend Micro Support.

Agent	Error Code	Problem and Resolution
	-13	The endpoint does not meet the minimum system requirements. Upgrade the RAM or disk space and try to install the agent again.
Encryption Management for Microsoft BitLocker	1603	Unable to install the Endpoint Encryption agent. A required resource may be unavailable. Restart the endpoint and try the installation again. If the problem persists, contact Trend Micro Support.
	-13	Unable to install the Endpoint Encryption agent. Microsoft BitLocker requires Trusted Platform Module (TPM). The endpoint either does not support TPM, TPM is not enabled in BIOS, or TPM is locked by another logged on user. Enable TPM in BIOS or contact the system administrator for assistance.
	-14	Unable to install the Endpoint Encryption agent. The operating system is not supported. Install one of the following supported operating systems and then try again: • Windows 7 32-bit or 64-bit, Ultimate or Enterprise edition

Agent	Error Code	Problem and Resolution
		• Windows 8 32-bit or 64-bit, Professional or Enterprise edition • Windows 8.1 32-bit or 64-bit, Professional or Enterprise edition
	-15	Full Disk Encryption is already installed.
	-16	Unable to install the Endpoint Encryption agent. The endpoint is already encrypted.

Using OfficeScan to Uninstall Endpoint Encryption Agents

During an upgrade, some Endpoint Encryption agents require first manually uninstalling the old Endpoint Encryption agent software. If the Endpoint Encryption agent software is malfunctioning in some way, uninstalling and reinstalling the Endpoint Encryption agent software may solve the problem.

During an upgrade, some Endpoint Encryption agents require first manually uninstalling the old Endpoint Encryption agent software. If the Endpoint Encryption agent software is malfunctioning in some way, uninstalling and reinstalling the Endpoint Encryption agent software may solve the problem.

This procedure explains how to uninstall Endpoint Encryption agents using the OfficeScan Endpoint Encryption Deployment Tool plug-in.

Procedure

1. Select the Endpoint Encryption device.

Note

To select multiple Endpoint Encryption devices, hold SHIFT and select applicable endpoints.

2. Click **Uninstall** and select the appropriate Endpoint Encryption agent from the drop-down list.
3. Click **OK** to confirm the deployment.

   The Endpoint Encryption agent uninstall command is deployed.
4. The Endpoint Encryption agent uninstallation is complete when OfficeScan displays the confirmation message.

Note

All future deployment commands fail if the Endpoint Encryption device is not restarted after the uninstall command is initiated and completes.

If the uninstall cannot complete, follow the manual uninstallation process at *Uninstallation on page 6-59*.

When uninstallation completes, the Endpoint Encryption agent is removed and the product folder is deleted from the endpoint.

Chapter 8

Maintenance and Technical Support

The following topics describe how to understand the Maintenance Agreement, find solutions online, use the Support Portal, contact Trend Micro, and find additional resources.

Topics include:

- *Maintenance Agreement on page 8-2*
- *Troubleshooting Resources on page 8-5*
- *Contacting Trend Micro on page 8-7*
- *Other Resources on page 8-8*

Maintenance Agreement

A Maintenance Agreement is a contract between your organization and Trend Micro, regarding your right to receive technical support and product updates in consideration for the payment of applicable fees. When you purchase a Trend Micro product, the License Agreement you receive with the product describes the terms of the Maintenance Agreement for that product.

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

If the Maintenance Agreement expires, scanning can still occur, but the product cannot be updated, even manually. Also, you will not be entitled to receive technical support from Trend Micro.

Typically, ninety (90) days before the Maintenance Agreement expires, you will be alerted of the pending discontinuance. You can update your Maintenance Agreement by purchasing renewal maintenance from your reseller, Trend Micro sales, or on the Trend Micro Online Registration URL:

Online Registration System

Renewing the Maintenance Agreement

Trend Micro or an authorized reseller provides technical support, downloads, and program updates for one (1) year to all registered users, after which renewal maintenance must be purchased.

If the Maintenance Agreement expires, basic operations are maintained; however, new users and devices cannot be added to PolicyServer, either through the PolicyServer MMC, agent installations, or Control Manager. To prevent this, renew the Maintenance Agreement as soon as possible.

For customers upgrading, the existing license is accepted until the expiration.

Procedure

1. To renew the Maintenance Agreement, do one of the following:
   - To purchase renewal maintenance, contact the same vendor from whom the product was purchased. A Maintenance Agreement extending protection for another year will be sent by post to the primary company contact listed in your Registration Profile.
   - To view or modify the company's Registration Profile, log on at the Trend Micro online registration website: https://olr.trendmicro.com/registration/
2. To view the Registration Profile, specify the Logon ID and password created when the product was first registered with Trend Micro (as a new customer), and then click **Login**.
3. To update the environment with the new Activation Code, see *Activating the New Product License on page 8-3*.

Trial License

You can install and evaluate Endpoint Encryption for a limited 30-day trial period. During PolicyServer installation, the Enterprise database and Enterprise Administrator account are created. PolicyServer functions normally with all client applications, unlimited devices, and up to 100 users for the 30-day trial period. After 30 days, contact Trend Micro Technical Sales to receive a license file. Endpoint Encryption user accounts and devices function normally after the trial period expires.

Activating the New Product License

A free 30-day trial license is available to install and evaluate Endpoint Encryption. If activating from the trial license, make sure to upgrade to the full version before the license expires.

Procedure

1. Log on to the server where PolicyServer is currently installed.

2. Go to the folder containing the PolicyServer program files and open the `Tools` folder.
3. Run `TMEE_License_Renewal.exe`.

   The **License Renewal Tool** opens.
4. Under **Renew License**, click **Renew Online** to access the Trend Micro registration website.

   After completing the registration, Trend Micro sends an email message containing the Activation Code.
5. Specify the new Activation Code for the product.
6. Click **Activate**.
7. At the confirmation message, click **OK** to continue.
8. Click **Exit**.

The updated Endpoint Encryption product license is immediately available.

Viewing the Product License

Use PolicyServer MMC to view the current license status.

Procedure

1. Log on to PolicyServer MMC.
2. Right-click the Enterprise and select **Activation/License**.

   The **Registration Information** screen appears.
3. Review the following options.

OPTION	DESCRIPTION
Activation Code	For a full licence, the Activation Code appears. For other license types, the name of the license appears.

Option	Description
Start Date	The date that the license was activated.
Expiration Date	The date that the license must be renewed. After a license expires, existing Endpoint Encryption users can still log on to Endpoint Encryption devices, but no new Endpoint Encryption devices or users can be added to the Enterprise.
Number of Devices	The number of Endpoint Encryption devices allowed in the license.
Number of Installed Devices	The number of Endpoint Encryption devices currently configured in the Enterprise.
Number of Users	The total number of Endpoint Encryption users allowed in the license.
Number of Created Users	The number of Endpoint Encryption users currently added to the Enterprise.
Activation Period in Days	The number of days left until the license expires.

4. Click **Close**.

Product Maintenance

From time to time, Trend Micro might release a patch for a reported known issue or an upgrade that applies to the product. To find out whether there are any patches available, visit: http://downloadcenter.trendmicro.com

Patches are dated. If there are available patches, open the readme file to determine whether the patch is applicable. If so, follow the upgrade instructions in the readme.

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Trend Community

To get help, share experiences, ask questions, and discuss security concerns with other users, enthusiasts, and security experts, go to:

http://community.trendmicro.com/

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to http://esupport.trendmicro.com.
2. Select a product or service from the appropriate drop-down list and specify any other related information.

   The **Technical Support** product page appears.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Submit a Support Case** from the left navigation and add any relevant details, or submit a support case here:

   http://esupport.trendmicro.com/srf/SRFMain.aspx

   A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Security Intelligence Community

Trend Micro cybersecurity experts are an elite security intelligence team specializing in threat detection and analysis, cloud and virtualization security, and data encryption.

Go to http://www.trendmicro.com/us/security-intelligence/index.html to learn about:

- Trend Micro blogs, Twitter, Facebook, YouTube, and other social media

- Threat reports, research papers, and spotlight articles
- Solutions, podcasts, and newsletters from global security insiders
- Free tools, apps, and widgets.

Threat Encyclopedia

Most malware today consists of "blended threats" - two or more technologies combined to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to http://www.trendmicro.com/vinfo to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports.

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone, fax, or email:

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

Email address	support@trendmicro.com

- Worldwide support offices:

  http://www.trendmicro.com/us/about-us/contact/index.html

- Trend Micro product documentation:

  http://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional hardware connected to the endpoint
- Amount of memory and free hard disk space
- Operating system and service pack version
- Endpoint client version
- Serial number or activation code
- Detailed description of install environment
- Exact text of any error message received.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

TrendEdge

Find information about unsupported, innovative techniques, tools, and best practices for Trend Micro products and services. The TrendEdge database contains numerous documents covering a wide range of topics for Trend Micro partners, employees, and other interested parties.

See the latest information added to TrendEdge at:

http://trendedge.trendmicro.com/

Download Center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

http://www.trendmicro.com/download/

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

TrendLabs

TrendLabs℠ is a global network of research, development, and action centers committed to 24x7 threat surveillance, attack prevention, and timely and seamless solutions delivery. Serving as the backbone of the Trend Micro service infrastructure, TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services.

TrendLabs monitors the worldwide threat landscape to deliver effective security measures designed to detect, preempt, and eliminate attacks. The daily culmination of these efforts is shared with customers through frequent virus pattern file updates and scan engine refinements.

Learn more about TrendLabs at:

http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs

Appendices

Appendices

Appendix A

Introducing Trend Micro™ Control Manager™

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

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

This chapter contains the following topics:

- *Control Manager Standard and Advanced on page A-3*
- *Introducing Control Manager Features on page A-3*
- *Control Manager Architecture on page A-5*
- *Registering Endpoint Encryption to Control Manager on page A-8*

- *Understanding User Access on page A-9*
- *Understanding the Product Directory on page A-15*
- *Downloading and Deploying New Components on page A-38*
- *Using Logs on page A-65*
- *Understanding Reports on page A-68*

Control Manager Standard and Advanced

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

Note

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

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

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

For a complete list of all features Standard and Advanced Control Manager servers support see the *Trend Micro Control Manager* documentation.

Introducing Control Manager Features

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

TABLE A-1. Control Manager Features

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

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

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

Control Manager Architecture

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

TABLE A-2. Control Manager Components

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

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

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

Registering Endpoint Encryption to Control Manager

Before registering the Endpoint Encryption server to a Control Manager server, you must ensure that both the server and the Control Manager server belong to the same network segment.

Procedure

1. Click **Administration** > **Control Manager Settings**.

   Note

   Control Manager uses the name specified in the Host name field to identify the Endpoint Encryption server. The Host name appears in the Product Directory of Control Manager.

   The **Control Manager Settings** screen displays.

2. Under **Connection settings**, type the name of the Endpoint Encryption server in the **Entity display name** field.

3. Under **Control Manager Server Settings** specify the following:

   a. Type the Control Manager server IP address or host name in the Server FQDN or IP address field.

   b. Type the port number that the MCP agent uses to communicate with Control Manager.

   c. If you have Control Manager security set to medium (HTTPS and HTTP communication is allowed between Control Manager and the MCP agent of managed products), select **Connect through HTTPS**.

d. If your network requires authentication, type the user name and password for your IIS server in the **Username** and **Password** fields.

e. If you use a NAT device, select **Enable two-way communication port forwarding** and type the NAT device's IP address and port number in **IP address** and **port number**.

Refer to the *Trend Micro Control Manager Administrator's Guide* for more information about managing products in Control Manager.

4. From the Control Manager management console, click **Products**.

   The **Product Directory** screen appears.

5. The Endpoint Encryption server appears in the Product Directory tree.

Understanding User Access

Control Manager access control consists of the following four sections.

TABLE A-3. Control Manager User Access Options

SECTION	DESCRIPTION
My Account	The **My Account** screen contains all the account information that Control Manager has for a specific user. The information on the **My Account** screen varies from user to user.

Section	Description
User Accounts	The **User Accounts** screen displays all Control Manager users. The screen also provides the options for users to create and maintain Control Manager user accounts. Use these functions to define clear areas of responsibility for users by restricting access rights to certain managed products and limiting what actions users can perform on the managed products. The functions are: • Execute • Configure • Edit Directory
User Roles	The **User Roles** screen displays all Control Manager user roles. The screen also provides the options for users to create and maintain Control Manager user roles. User roles define which areas of the Control Manager web console a user can access.
User Groups	The **User Groups** screen contains Control Manager groups and provides options for creating groups. Control Manager uses groups as an easy method to send notifications to a number of users without having to select the users individually. Control Manager groups do not allow administrators to create a group that shares the same access rights.

Note

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

Control Manager User Access with Endpoint Encryption User Access

Endpoint Encryption user access is similar to Control Manager user access. Administrators can control which parts of the Endpoint Encryption web console users can access (Power User, Operator, or Administrator).

All user accounts created in Control Manager have administrator access to any managed product to which the user has access. This creates a problem if an administrator wants to restrict a user's access to Power User on the Endpoint Encryption server while allowing access to Control Manager.

MCP Heartbeat

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

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

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

The MCP heartbeats implement in the following ways:

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

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

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

Using the Schedule Bar

Use the schedule bar on the **Agent Communication Schedule** screen to display and set Communicator schedules. The bar has 24 slots, each representing the hours in a day.

The slots with clock icons denote working status or the hours that the Agent/ Communicator sends information to the Control Manager server. White slots indicate idle time. Define working or idle hours by toggling specific slots.

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

FIGURE A-1. Schedule bar

The active periods specified by the bar are from 0:00 to 7:00, 8:00 to 4:00 PM, and from 6:00 P.M. to midnight.

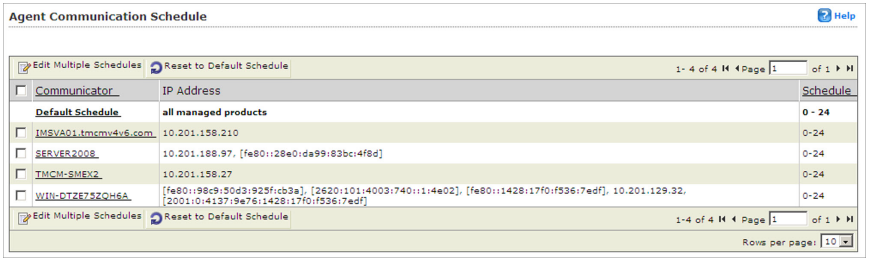
Setting an Agent Communication Schedule for a Managed Product

Procedure

1. Open the Control Manager console.

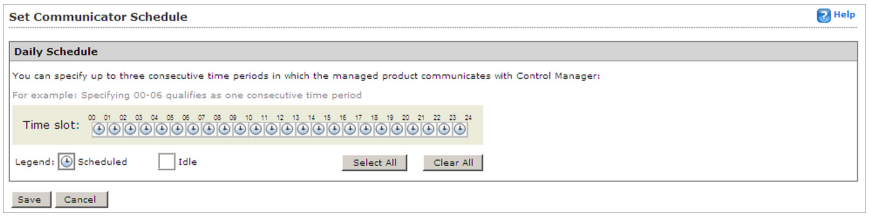
2. Navigate to **Administration** > **Settings** > **Agent Communication Schedule**.

   The **Agent Communication Schedule** screen appears.



3. Select the managed product schedule to modify.

   The **Set Communicator Schedule** screen appears.



4. Define the schedule. Specify a new time or use the default setting:

   - To specify a new setting, change the appropriate time slots in the schedule bar and then click **Save**

   - To use the default setting, return to the **Agent Communication Schedule** screen. Select the schedule to apply and click **Reset to Default Schedule**

Determining the Right Heartbeat Setting

When choosing a heartbeat setting, balance between the need to display the latest managed product status information and the need to manage system resources. The default setting is satisfactory for most situations, however consider the following points when you customize the heartbeat setting:

TABLE A-4. Heartbeat Recommendations

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

Configuring the Agent Communicator Heartbeat

Use the **Communication Time-out** screen to define the frequency and maximum delay times (in minutes) for the Control Manager server and agent communication.

Note

The agent/communicator heartbeat setting only applies to Communicators for managed products directly controlled by the Control Manager server. Child Control Manager server agent/communicators use pre-defined values:

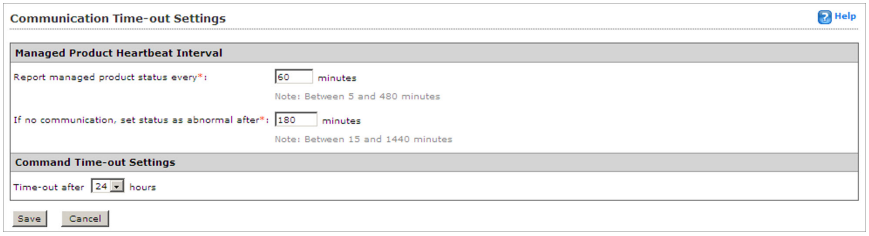
Frequency: 3 minutes

Maximum delay: 5 minutes

Procedure

1. Open the Control Manager console.
2. Navigate to **Administration** > **Settings** > **Communication Time-out Settings**.

   The **Communication Time-out** screen appears.



3. On the working area, leave the default values or specify new settings for the following:
   - **Report managed product status every**: Defines how often the managed product responds to Control Manager server messages. Valid values are between 5 to 480 minutes
   - **If no communication, set status as abnormal after**: Specifies how long Control Manager waits for a response from the managed product before changing its web console status to (inactive). Valid values are between 15 and 1440 minutes.

   Note

   The **If no communication, set status as abnormal after** value must be at least triple the **Report managed product status every** value.

4. Click **Save**.

Understanding the Product Directory

A managed product is a representation of an antivirus, content security, or web protection product in the Product Directory. Managed products display as icons (for

example, (SMEX) or (PW)) in the Control Manager web console Product Directory section. These icons represent Trend Micro antivirus, content security, and web protection products. Control Manager supports dynamic icons, which change with the status of the managed product. See your managed product's documentation for more information on the icons and associated statuses for your managed product.

Indirectly administer the managed products either individually or by groups through the Product Directory. The following table lists the menu items and buttons on the Product Directory screen.

TABLE A-5. Product Directory Options

MENU ITEM	DESCRIPTION
Advanced Search	Click this menu item to specify search criteria to perform a search for one or more managed products.
Configure	After selecting a managed product/ directory, move the cursor over this menu item and select a task, to log on to a web-based console using SSO or to configure a managed product.
Tasks	After selecting a managed product/ directory, move the cursor over this menu item and select a task, to perform a specific function (such as deploying the latest components) to a specific managed product or child server or groups of managed products or child servers. Initiate a task from a directory and Control Manager sends requests to all managed products belonging to that directory.
Directory Management	Click this button to open the **Directory Management** screen. From the screen, move entities/directories (by dragging and dropping them) or create new directories.
Buttons	

Menu Item	Description
Search	Click this button, after typing a managed product's name, to perform a search for the specified managed product.
Status	Click this button, after selecting a managed product/directory, to obtain status summaries about the managed product or managed products found in the directory.
Folder	Click this button, after selecting a directory, to obtain status summaries about the managed products and the managed product endpoints found in the directory.

Note

Managed products belonging to child Control Manager servers cannot have tasks issued to them by the parent Control Manager server.

Product Directory Structure Recommendations

Trend Micro recommends the following when planning your Product Directory structure for managed products and child servers:

Table A-6. Considerations when Grouping Managed Products or Child Servers

Structure	Description
Company network and security policies	If different access and sharing rights apply to the company network, group managed products and child servers according to company network and security policies.
Organization and function	Group managed products and child servers according to the company's organizational and functional division. For example, have two Control Manager servers that manage the production and testing groups.

Structure	Description
Geographical location	Use geographical location as a grouping criterion if the location of the managed products and child servers affects the communication between the Control Manager server and its managed products or child servers.
Administrative responsibility	Group managed products and child servers according to system or security personnel assigned to them. This allows group configuration.

The Product Directory provides a user-specified grouping of managed products which allows you to perform the following for administering managed products:

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

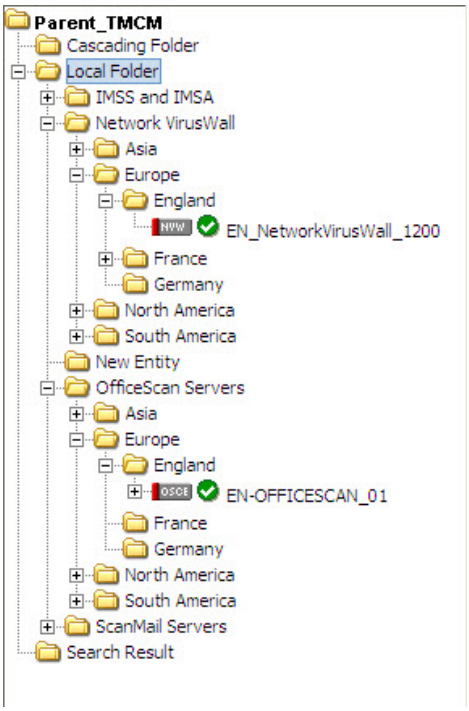
Plan this structure carefully, because the structure also affects the following:

Table A-7. Considerations for the Structure

Consider	Effect
User access	When creating user accounts, Control Manager prompts for the segment of the Product Directory that the user can access. For example, granting access to the root segment grants access to the entire directory. Granting access to a specific managed product only grants access to that specific product.

CONSIDER	EFFECT
Deployment planning	Control Manager deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.
Outbreak Prevention Policy (OPP) and Damage Control Template (DCT) deployments	OPP and DCT deployments depend on Deployment Plans for efficient distribution of Outbreak Prevention Policy and cleanup tasks.

A sample Product Directory appears below:



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

Note

All newly registered managed products usually appear in the New Entity folder regardless of the agent type.

TABLE A-8. Managed Product Icons

ICON	DESCRIPTION
EMAN	InterScan eManager
OSCE	OfficeScan Corporate Edition
SPNT	ServerProtect Information Server
	ServerProtect Domain
NT	ServerProtect for Windows (Normal Server)

Icon	Description
	ServerProtect for NetWare (Normal Server)
	InterScan Messaging Security Suite
	InterScan Web Security Suite
	InterScan VirusWall for Windows
	InterScan VirusWall for UNIX
	ScanMail for Microsoft Exchange
	ScanMail for Lotus Notes
	Network VirusWall
	NetScreen Global PRO Firewall
	Managed Product connection status icon

Arrange the Product Directory using the Directory Manager. Use descriptive folder names to group your managed products according to their protection type or the Control Manager network administration model.

Accessing the Product Directory

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

Note

Viewing and accessing the folders in the Product Directory depends on the Account Type and user account access rights.

Procedure

- Click **Products** from the main menu.

The **Product Directory** screen appears.

Manually Deploying Components Using the Product Directory

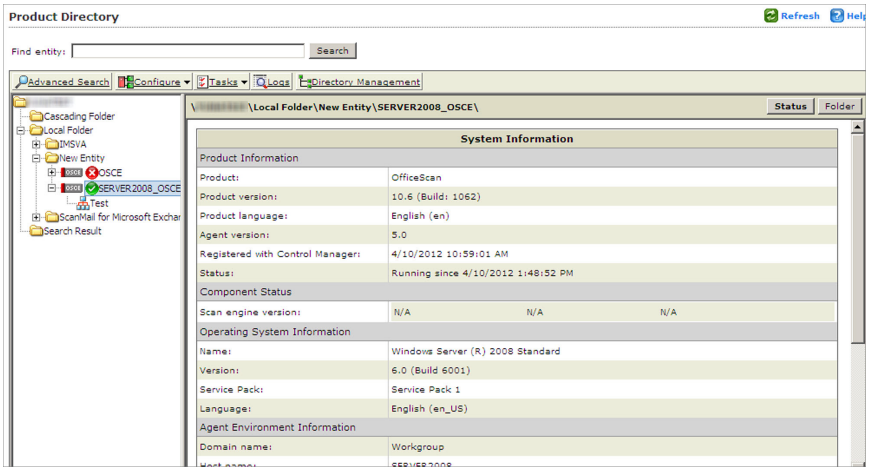
Manual deployments allow you to update the virus patterns, spam rules, and scan engines of your managed products on demand. Use this method of updating components during virus outbreaks.

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

Procedure

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

   The **Product Directory** screen appears.



2. Select a managed product or directory from the Product Directory.

   The managed product or directory highlights.

3. Move the cursor over **Tasks** from the Product Directory menu.

4. Select **Deploy <component>** from the drop-down menu.
5. Click **Deploy Now** to start the manual deployment of new components.
6. Monitor the progress through the **Command Tracking** screen.
7. Click the Command Details link on the **Command Tracking** screen to view details for the Deploy Now task.

Viewing Status Summaries for Managed Products

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

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

- Through the dashboard using the Threat Detection Results widget (found on the Summary tab)
- Through the Product Directory

Accessing Through the Dashboard

Procedure

- Upon opening the Control Manager web console, the **Summary** tab on the Dashboard displays the summary of the entire Control Manager network. This summary is identical to the summary provided by the Product Status tab in the Product Directory Root folder.

Accessing Through the Product Directory

Procedure

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

   The **Product Directory** screen appears.

2. From the Product Directory tree, select the desired folder or managed product.
   - If you click a managed product, the Product Status tab displays the managed product's summary.
   - If you click the Root folder, New entity, or other user-defined folder, the Product Status tab displays Antivirus, Content Security, and Web Security summaries.

Note

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

Configuring Managed Products

Depending on the product and agent version you can configure the managed product from the managed product's web console or through a Control Manager-generated console.

Procedure

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

   The **Product Directory** screen appears.

2. Select the desired managed product from the Product Directory tree.

   The product status appears in the right-hand area of the screen.

3. Move the cursor over **Configure** in the Product Directory menu.
4. Select one of the following:
   - **Configuration Replication**: The **Configuration Settings** screen appears.

   a. Select the folder to which the selected managed product's settings replicate from the Product Directory tree.

   b. Click **Replicate**.

The selected managed product's settings replicate to the target managed products.

- **<Managed Product Name> Single Sign On**: The managed product's web console or Control Manager-generated console appears.

a. Configure the managed product from the web console.

Note

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

Issuing Tasks to Managed Products

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

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

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

Procedure

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

   The **Product Directory** screen appears.

2. Select the managed product or directory to issue a task.

3. Move the cursor over **Tasks**.
4. Click a task from the list. Monitor the progress through Command Tracking. Click the **Command Details** link at the response screen to view command information.

Querying and Viewing Managed Product Logs

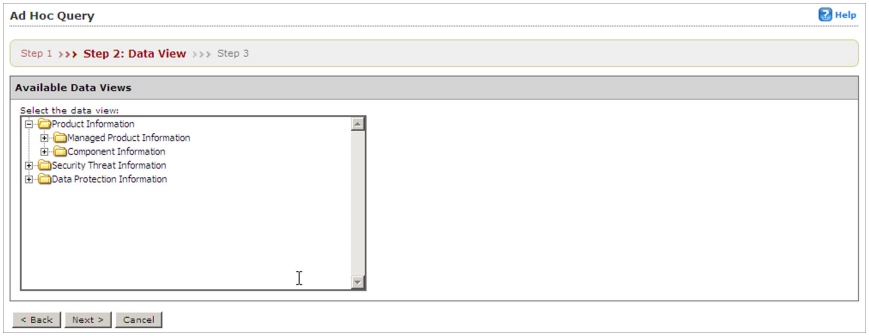
Use the Logs tab to query and view logs for a group or a specific managed product.

Procedure

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

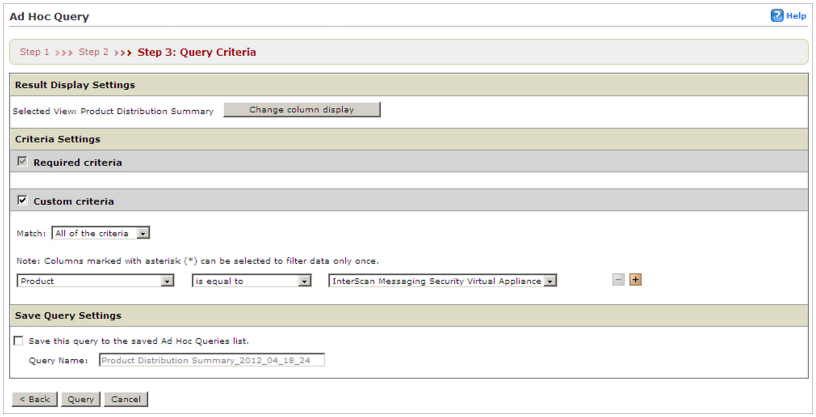
   The **Product Directory** screen appears.
2. Select the desired managed product or folder from the Product Directory.
3. Move the cursor over **Logs** in the Product Directory menu.
4. Click **Logs** from the drop-down menu.

   The **Ad Hoc Query > Step 2: Select Data View** screen appears.



5. Specify the data view for the log:
   a. Select the data to query from the Available Data Views area.
   b. Click **Next**.

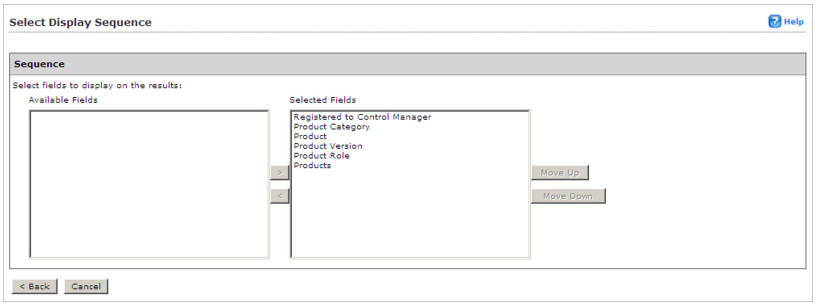
The **Ad Hoc Query > Step 3: Query Criteria** screen appears.



6. Specify the data to appear in the log and the order in which the data appears. Items appearing at the top of the Selected Fields list appear as the left most column of the table. Removing a field from Selected Fields list removes the corresponding column from the Ad Hoc Query returned table.

   a. Click **Change column display**.

      The **Select Display Sequence** screen appears.



   b. Select a query column from the Available Fields list. Select multiple items using the **Shift** or **Ctrl** keys.

   c. Click **>** to add items to the Selected Fields list.

d. Specify the order in which the data displays by selecting the item and clicking **Move up** or **Move down**.

e. Click **Back** when the sequence fits your requirements.

7. Specify the filtering criteria for the data:

> **Note**
>
> When querying for summary data, users must specify the items under Required criteria.

- Required criteria:
  - Specify a Summary Time for the data or whether you want COOKIES to appear in your reports.
- Custom criteria:

  a. Specify the criteria filtering rules for the data categories:
     - **All of the criteria**: This selection acts as a logical AND function. Data appearing in the report must meet all the filtering criteria.
     - **Any of the criteria**: This selection acts as a logical OR function. Data appearing in the report must meet any of the filtering criteria.

  b. Specify the filtering criteria for the data. Control Manager supports specifying up to 20 criteria for filtering data.

> **Tip**
>
> If you do not specify any filtering criteria, the Ad Hoc Query returns all results for the applicable columns. Trend Micro recommends specifying filtering criteria to simplify data analysis after the information for the query returns.

8. Save the query:

   a. Click **Save this query to the saved Ad Hoc Queries list**.

   b. Type a name for the saved query in the **Query Name** field.

9. Click **Query**.

   The **Results** screen appears.

10. Save the report as a CSV file:

    a. Click **Export to CSV**.

    b. Click **Download**.

    c. Specify the location to save the file.

    d. Click **Save**.

11. Save the report as an XML file:

    a. Click **Export to XML**.

    b. Click **Download**.

    c. Specify the location to save the file.

    d. Click **Save**.

> **Tip**
>
> To query more results on a single screen, select a different value in Rows per page. A single screen can display 10, 15, 30, or 50 query results per page.

12. Save the settings for the query:

    a. Click **Save query settings**.

    b. Type a name for the saved query in the **Query Name** field.

    c. Click **OK**.

    The saved query appears on the **Saved Ad Hoc Queries** screen.

About Recovering Managed Products Removed From the Product Directory

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

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

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

- Replacing the corrupted Control Manager database with another database of the same name

- Accidentally deleting the managed product from Directory Management

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

MCP agents do not re-register automatically. Administrators must manually re-register managed products using MCP agents.

Recovering Managed Products Removed From the Product Directory

---

Procedure

- Restart the Trend Micro Control Manager service on the managed product server. For more information, see *Stopping and Restarting Control Manager Services on page A-31*.

- Wait for the Agent to re-register itself: By default, the older Control Manager agents verify their connection to the server every eight (8) hours. If the agent detects that its record has been deleted, it will re-register itself automatically.

- Manually re-register to Control Manager: MCP agents do not re-register automatically and need to be manually re-registered to the Control Manager server.

Stopping and Restarting Control Manager Services

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

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

Note

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

Procedure

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

Searching for Managed Products, Product Directory Folders, or Computers

Use the **Search** button to quickly locate a specific managed product in the Product Directory.

Searching for a Folder or Managed Product

Procedure

1. Access the Product Directory.

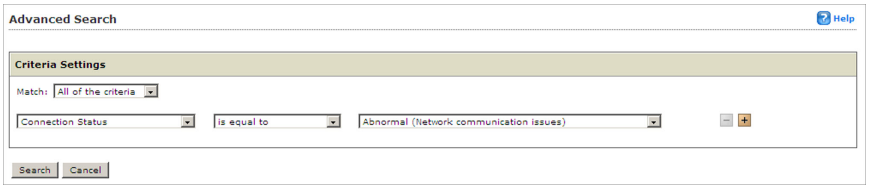
2. Type the display name of the managed product in the **Find entity** field.
3. Click **Search**.

Performing an Advanced Search

Procedure

1. Access the Product Directory.
2. Click **Advanced Search**.

   The **Advanced Search** screen appears.



3. Specify your filtering criteria for the product. Control Manager supports up to 20 filtering criteria for searches.
4. Click **Search** to start searching.

   Search results appear in the **Search Result** folder of the Product Directory.

Refreshing the Product Directory

Procedure

- On the **Product Directory** screen, click the **Refresh** icon on the upper right corner of the screen.

Understanding the Directory Management Screen

After registering to Control Manager, the managed product appears in the Product Directory under the default folder.

Use the Directory Management screen to customize the Product Directory organization to suit your administration needs. For example, you can group products by location or product type (messaging security, web security, file storage protection).

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

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

- Product Directory
- User Accounts
- Deployment Plans
- Ad Hoc Query
- Control Manager reports

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

TABLE A-9. Product Grouping Comparison

GROUPING TYPE	ADVANTAGES	DISADVANTAGES
Geographical or Administrative	Clear structure	No group configuration for identical products
Product type	Group configuration and status is available	Access rights may not match

Grouping Type	Advantages	Disadvantages
Combination of both	Group configuration and access right management	Complex structure, may not be easy to manage

Using the Directory Management Screen Options

Use these options to manipulate and organize managed products in your Control Manager network.

The **Directory Management** screen provides several options:

- Add directories to the Product Directory
- Rename directories in the Product Directory
- Move managed products or directories in the Product Directory
- Remove managed products or directories from the Product Directory

Note

The keep permissions check box allows a folder to keep its source permission when moved.

Using the Directory Management Screen

Procedure

- Select a managed product or directory and click **Rename** to rename a managed product or directory
- Click **+** or the folder to display the managed products belonging to a folder
- Drag managed products or directories to move the managed products or directories in the Product Directory
- Click **Add Folder** to add a directory to the Product Directory

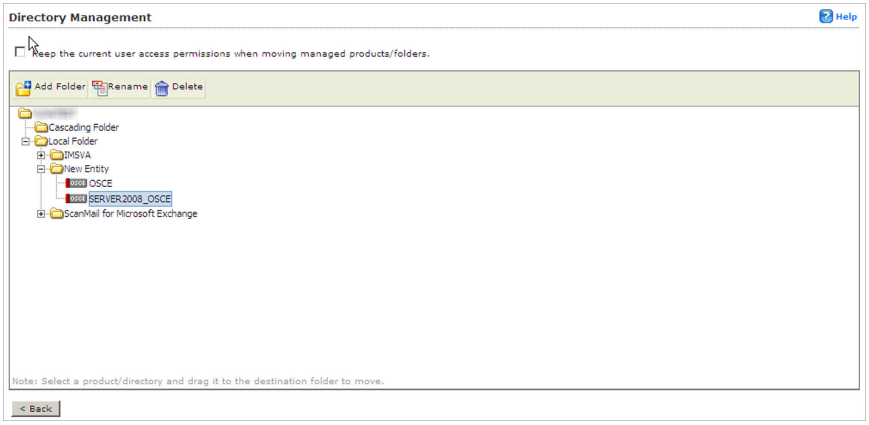
Accessing the Directory Management Screen

Use the **Directory Management** screen to group managed products together.

Procedure

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

   The **Product Directory** screen appears.



2. Click **Directory Management** from the Product Directory menu.

   The **Directory Management** screen appears.

Creating Folders

Group managed products into different folders to suit your organization's Control Manager network administration model.

Procedure

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

   The **Product Directory** screen appears.

2. Click **Directory Management** from the Product Directory menu.

   The **Directory Management** screen appears.

3. Select **Local Folder**.

4. Click **Add Folder**.

   The **Add Directory** screen appears.

5. Type a name for the new directory in the **Directory name** field.

6. Click **Save**.

Note

Except for the **New Entity** folder, Control Manager lists all other folders in ascending order, starting from special characters (!, #, $, %, (,), *, +, -, comma, period, +, ?, @, [,], ^, _, {, |, }, and ~), numbers (0 to 9), or alphabetic characters (a/A to z/Z).

Renaming Folders or Managed Products

Rename directories and managed products on the **Directory Management** screen.

Note

Renaming a managed product only changes the name stored in the Control Manager database; there are no effects to the managed product.

Procedure

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

   The **Product Directory** screen appears.

2. Click **Directory Management** from the Product Directory menu.

   The **Directory Management** screen appears.

3. Select the managed product or directory to rename.

4. Click **Rename**.

   The **Rename Directory** screen appears.

5. Type a name for the managed product or directory in the **Directory name** field.

6. Click **Save**.

7. Click **OK**.

   The managed product or directory displays in the Product Directory with the new name.

Moving Folders or Managed Products

When moving folders pay special attention to the **Keep the current user access permissions when moving managed products/folders** check box. If you select this check box and move a managed product or folder, the managed product or folder keeps the permissions from its source folder. If you clear the keep permissions check box, and then move a managed product or folder, the managed product or folder assumes the access permissions from its new parent folder.

Procedure

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

   The **Product Directory** screen appears.

2. Click **Directory Management** from the Product Directory menu.

   The **Directory Management** screen appears.

3. On the working area, select the folder or managed product to move.

4. Drag the folder or managed product to the target new location.

5. Click **Save**.

Deleting User-Defined Folders

Take caution when deleting user-defined folders on the **Directory Management** screen. You may accidentally delete a managed product which causes it to unregister from the Control Manager server.

Note

You cannot delete the **New Entity** folder.

Procedure

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

   The **Product Directory** screen appears.

2. Click **Directory Management** from the Product Directory menu.

   The **Directory Management** screen appears.

3. Select the managed product or directory to delete.

4. Click **Delete**.

   A confirmation dialog box appears.

5. Click **OK**.

6. Click **Save**.

Downloading and Deploying New Components

Trend Micro recommends updating the antivirus and content security components to remain protected against the latest virus and malware threats.

By default, Control Manager enables download only on components belonging to managed products registered to the Control Manager server. Control Manager enables virus pattern download even if no managed products are registered to the Control Manager server.

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

TABLE A-10. Available Components

COMPONENT	DESCRIPTION
Pattern files/Cleanup templates	Pattern files/Cleanup templates contain hundreds of malware signatures (for example, viruses or Trojans) and determine the managed product's ability to detect and clean malicious file infections
Antispam rules	Antispam rules are the Trend Micro-provided files used for antispam and content filtering
Engines	Engines refer to virus/malware scan engines, Damage Cleanup engine, VirusWall engines, the Spyware/Grayware engine and so on. These components perform the actual scanning and cleaning functions.

Component	Description
OfficeScan Plug-in Programs	OfficeScan Plug-in Programs (for example, Trend Micro Security for Mac). **Note** The OfficeScan web console displays all available Plug-in Programs. You can specify to download any of them from Control Manager. However, Control Manager may not have the downloaded the Plug-in Program. Which means that OfficeScan cannot download the specified Plug-in Program from Control Manager. Before specifying a Plug-in Program for download, from Control Manager to OfficeScan, verify that Control Manager has already downloaded the Plug-in Program.
Product programs and widget pool	Product-specific components (for example, Service Pack releases) and the Control Manager widget pool

Note

Only registered users are eligible for components update.

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

The **Component List** screen presents a full list of all components that Control Manager has available for managed products. The list also matches components with managed

products that use the component. Click **Updates** > **Component List** to open the **Component List** screen.

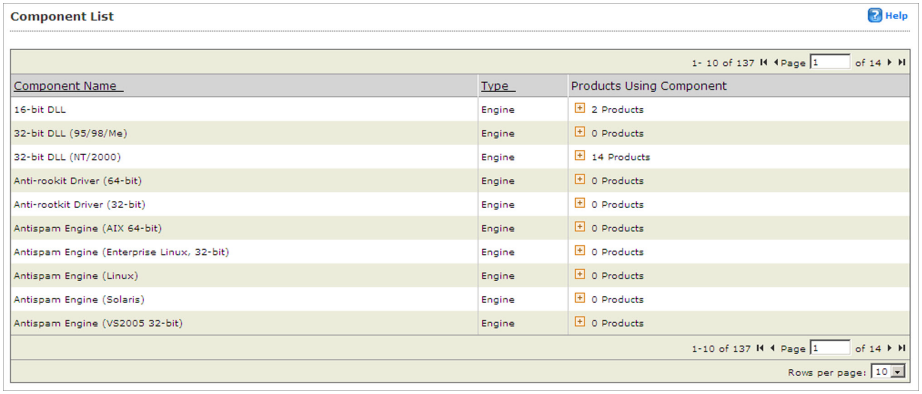


FIGURE A-2. The Component List screen

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

Tip

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

Manually Downloading Components

Manually download component updates when you initially install Control Manager, when your network is under attack, or when you want to test new components before deploying the components to your network.

Trend Micro recommends the following method to configure manual downloads. Manually downloading components requires multiple steps:

Tip

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

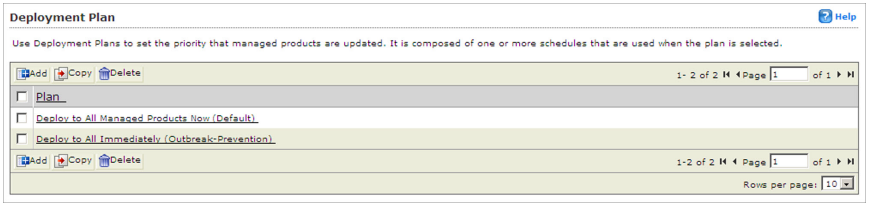
- Step 1: Configure a deployment plan for your components
- Step 2: Configure your proxy settings, if you use a proxy server
- Step 3: Select the components to update
- Step 4: Configure the download settings
- Step 5: Configure the automatic deployment settings
- Step 6: Complete the manual download

Step 1: Configure a Deployment Plan for Your Components

Procedure

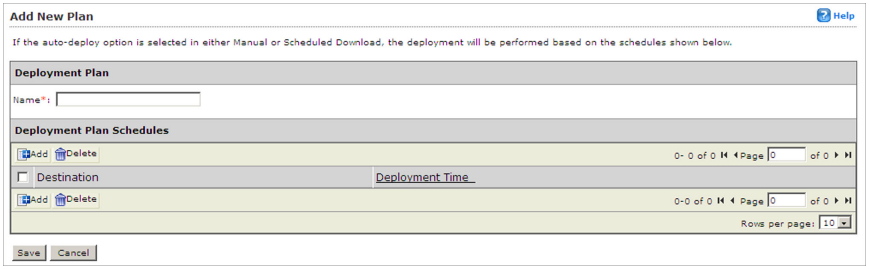
1. Navigate to **Updates** > **Deployment Plan**.

   The **Deployment Plan** screen appears.



2. Click **Add**.

   The **Add New Plan** screen appears.



3. Type a deployment plan name in the **Name** field.

4. Click **Add** to provide deployment plan details.

   The **Add New Schedule** screen appears.

5. On the **Add New Schedule** screen, choose a deployment time schedule by selecting one the following options:

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

     Use the menus to designate the time in hours and minutes.

   - **Delay**: after Control Manager downloads the update components, Control Manager delays the deployment according to the interval that you specify.

     Use the menus to indicate the duration, in terms of hours and minutes.

6. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.

7. Click **Save**.

The **Add New Plan** screen appears.

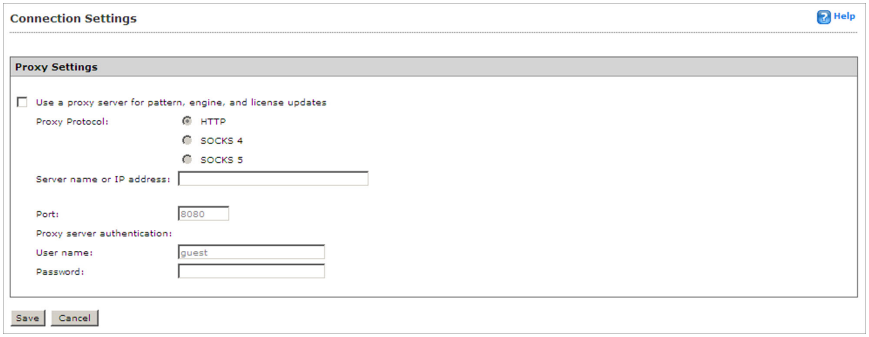
8. Click **Save** to apply the new deployment plan.

Step 2: Configure Your Proxy Settings (If You Use a Proxy Server)

Procedure

1. Navigate to **Administration** > **Settings** > **Proxy Settings**.

   The **Connection Settings** screen appears.



2. Select **Use a proxy server for pattern, engine, and license updates**.
3. Select the protocol:
   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**
4. Type the host name or IP address of the server in the **Server name or IP address** field.
5. Type a port number in the **Port** field.
6. Type a log on name and password if your server requires authentication.

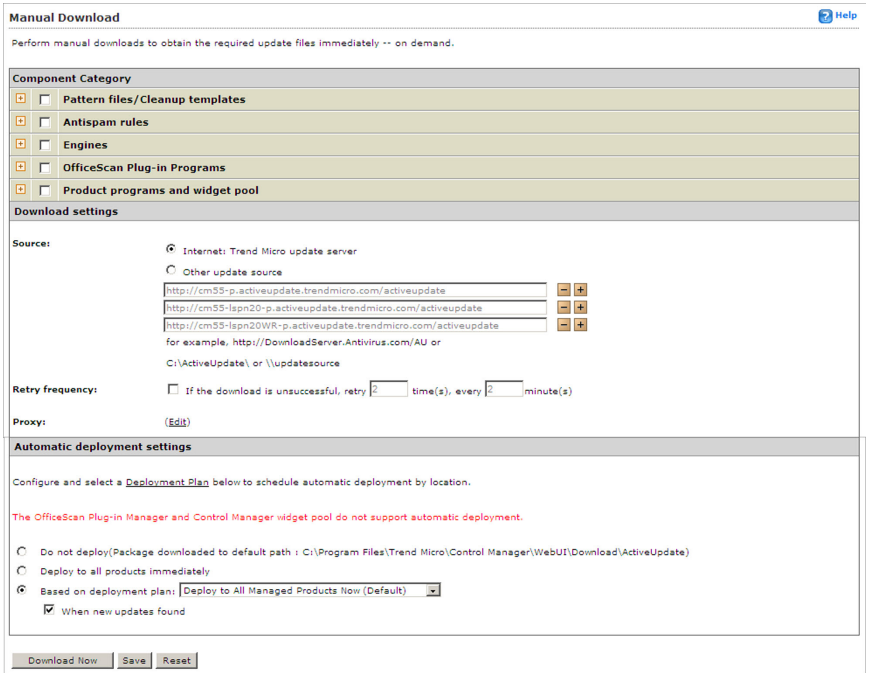
7. Click **Save**.

Step 3: Select the Components to Update

Procedure

1. Navigate to **Updates** > **Manual Download**.

   The **Manual Download** screen appears.



2. From the Component Category area select the components to download.

   a. Click the + icon to expand the component list for each component group.

   b. Select the components to download. To select all components for a group, select:

- Pattern files/Cleanup templates
- Antispam rules
- Engines
- OfficeScan Plug-in Programs
- Product programs and widget pool

Step 4: Configure the Download Settings

Procedure

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

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

   Tip

   Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.
3. If you use an HTTP proxy server on the network (that is, if the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings on the **Connection Settings** screen.

Step 5: Configure the Automatic Deployment Settings

Procedure

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

Tip

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

Step 6: Complete the Manual Download

Procedure

1. Click **Download Now** and then click **OK** to confirm.

   The download response screen appears. The progress bar displays the download status.

2. Click **Command Details** to view details from the **Command Details** screen.

3. Click **OK** to return to the **Manual Download** screen.

Understanding Scheduled Download Exceptions

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

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

Note

Daily scheduled exceptions apply to the selected days, while hourly scheduled exceptions apply to every day of the week.

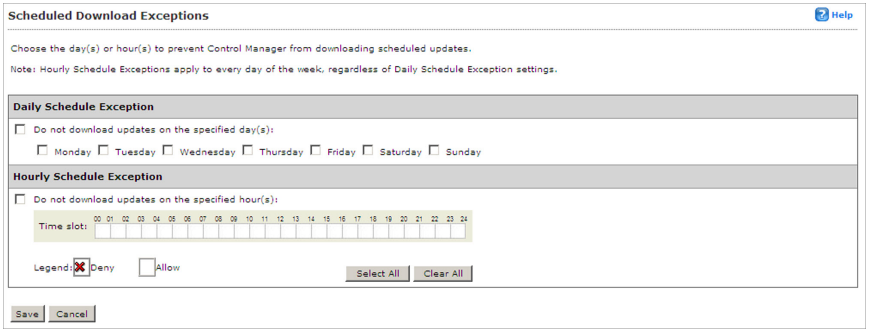
Example: The administrator decides that they do not want Control Manager to download components on weekends or after working hours throughout the week. The administrator enables **Daily Schedule Exception** and selects **Saturday** and **Sunday**. The administrator then enables **Hourly Schedule Exception** and specifies the hours of **00:00 to 9:00** and **18:00 to 24:00**.

Configuring Scheduled Download Exceptions

Procedure

1. Navigate to **Updates** > **Scheduled Download Exceptions**.

   The **Scheduled Download Exceptions** screen appears.



2. Do one or more of the following:

   - To schedule a daily exception, under Daily Schedule Exception, select the day(s) to prevent downloads, and then select **Do not download updates on the specified day(s)**. Every week, Control Manager blocks all downloads during the selected day(s).

   - To schedule an hourly exception, under Hourly Schedule Exception, select the hour(s) to prevent downloads, and then select **Do not download updates on the specified hour(s)**. Every day, Control Manager blocks all downloads during the selected hours.

3. Click **Save**.

Configuring Scheduled Downloads

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

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

- **Frequency**: Shows how often the component updates
- **Enabled**: Indicates if the schedule for the component is enabled or disabled

- **Update Source**: Displays the URL or path of the update source

Configuring scheduled component downloads requires multiple steps:

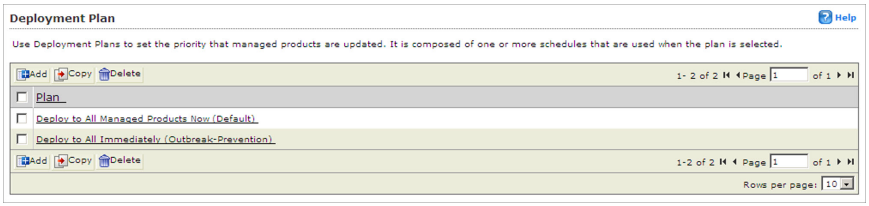
- Step 1: Configure a Deployment Plan for your components
- Step 2: Configure your proxy settings, if you use a proxy server
- Step 3: Select the components to update
- Step 4: Configure the download schedule
- Step 5: Configure the download settings
- Step 6: Configure the automatic deployment settings
- Step 7: Enable the schedule and save settings

Step 1: Configure a Deployment Plan for Your Components

Procedure

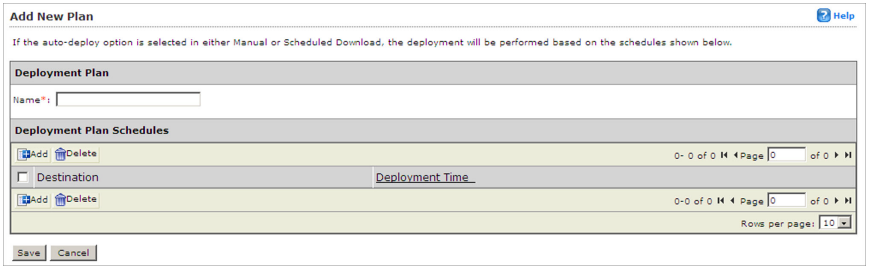
1. Navigate to **Updates** > **Deployment Plan**.

   The **Deployment Plan** screen appears.



2. Click **Add**.

   The **Add New Plan** screen appears.



3. Type a deployment plan name in the **Name** field.

4. Click **Add** to provide deployment plan details.

   The **Add New Schedule** screen appears.

5. Choose a deployment time schedule by selecting one the following options:

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

     Use the menus to designate the time in hours and minutes.

   - **Delay**: after Control Manager downloads the update components, Control Manager delays the deployment according to the interval that you specify.

     Use the menus to indicate the duration, in terms of hours and minutes.

6. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.

7. Click **Save**.

   The **Add New Plan** screen appears.

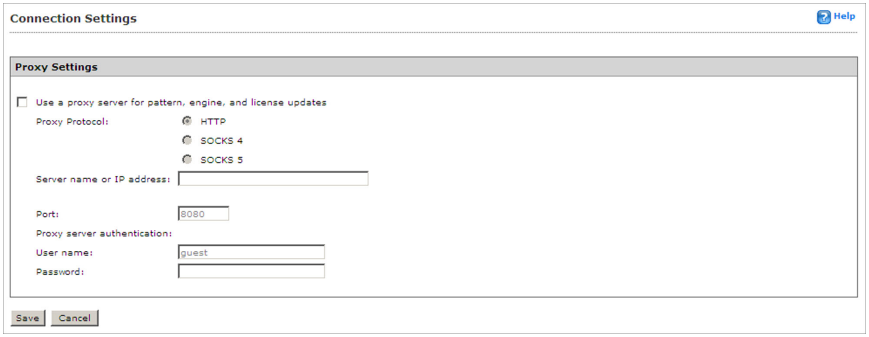
8. Click **Save** to apply the new deployment plan.

Step 2: Configure Your Proxy Settings (If You Use a Proxy Server)

Procedure

1. Navigate to **Administration** > **Settings** > **Proxy Settings**.

   The **Connection Settings** screen appears.



2. Select **Use a proxy server for pattern, engine, and license updates**.
3. Select the protocol:
   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**
4. Type the host name or IP address of the server in the **Server name or IP** address field.
5. Type a port number for the proxy server in the **Port** field.
6. Type a logon name and password if your server requires authentication.

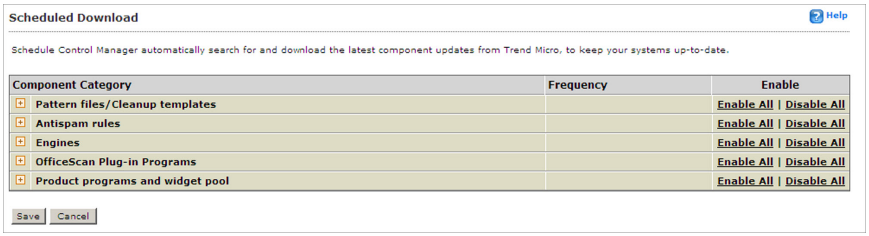
7. Click **Save**.

Step 3: Select the Components to Update

Procedure

1. Navigate to **Updates** > **Scheduled Download**.

   The **Scheduled Download** screen appears.



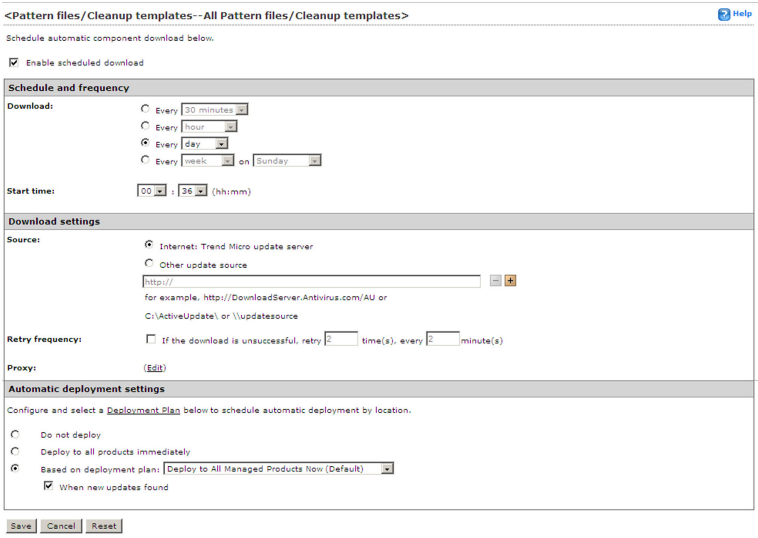
2. From the Component Category area select the components to download.

   a. Click the + icon to expand the component list for each component group.

   b. Select the components to download. To select all components for a group, select:

      - **All Pattern files/Cleanup templates**
      - **All Antispam rules**
      - **All Engines**
      - **OfficeScan Plug-in Programs**
      - **Product programs and widget pool**

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



Step 4: Configure the Download Schedule

Procedure

1. Select the **Enable scheduled download** check box to enable scheduled download for the component.
2. Define the download schedule. Select a frequency, and use the appropriate drop down menu to specify the desired schedule. You may schedule a download by minutes, hours, days, or weeks.
3. Use the **Start time** menus to specify the date and time the schedule starts to take effect.

Step 5: Configure the Download Settings

Procedure

1. Select the update source:

   - **Internet**: **Trend Micro update server**: Download components from the official Trend Micro ActiveUpdate server.

   - **Other update source**: Type the URL of the update source in the accompanying field.

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

2. Select **Retry frequency** and specify the number of retries and duration between retries for downloading components.

   Note

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

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

Step 6: Configure the Automatic Deployment Settings

Procedure

1. Select when to deploy downloaded components from the Automatic deployment settings area. The options are:

   - **Do not deploy**: Components download to Control Manager, but do not deploy to managed products. Use this option under the following conditions:

     - Deploying to the managed products individually

- Testing the updated components before deployment

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

Note

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

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

Step 7: Enable the Schedule and Save Settings

Procedure

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

Configuring Scheduled Download Schedule and Frequency

Specify how often Control Manager obtains component updates at the Schedule and Frequency group.

Procedure

1. Navigate to **Updates** > **Scheduled Download**.

The **Scheduled Download** screen appears.

2. From the Component Category area select the components to download.

   a. Click the **+** icon to expand the component list for each component group.

   b. Select the components to download. To select all components for a group, select:

      - **All Pattern files/Cleanup templates**
      - **All Antispam rules**
      - **All Engines**
      - **OfficeScan Plug-in Programs**
      - **Product programs and widget pool**

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

3. Under Schedule and frequency:

   a. Define the download schedule. Select a frequency, and use the appropriate drop down menu to specify the desired schedule. You may schedule a download every minutes, hours, days, or weeks.

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

4. Click **Save**.

Configuring Scheduled Download Settings

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

Procedure

1. Navigate to **Updates** > **Scheduled Download**.

The **Scheduled Download** screen appears.

2. From the Component Category area select the components to download.

   a. Click the **+** icon to expand the component list for each component group.

   b. Select the components to download. To select all components for a group, select:

      - **All Pattern files/Cleanup templates**
      - **All Antispam rules**
      - **All Engines**
      - **OfficeScan Plug-in Programs**
      - **Product programs and widget pool**

      The Component Name> screen appears. Where Component Name> represents the name of the selected component.

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

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

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

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

Note

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

---

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

6. Click **Save**.

Configuring Scheduled Download Automatic Deployment Settings

Use the Automatic deployment settings group to set how Control Manager deploys updates.

Procedure

1. Navigate to **Updates** > **Scheduled Download**.

   The **Scheduled Download** screen appears.

2. From the Component Category area select the components to download.

   a. Click the + icon to expand the component list for each component group.

   b. Select the components to download. To select all components for a group, select:

      - **All Pattern files/Cleanup templates**
      - **All Antispam rules**
      - **All Engines**
      - **OfficeScan Plug-in Programs**
      - **Product programs and widget pool**

        The Component Name> screen appears. Where Component Name> represents the name of the selected component.

3. Select when to deploy downloaded components from the Automatic deployment settings area. The options are:

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

Note

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

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

Note

The settings in Automatic deployment settings only apply to components used by managed products.

Understanding Deployment Plans

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

The Control Manager installation creates two deployment plans:

- Deploy to All Managed Products Now (Default): default plan used during component updates
- Deploy to All Immediately (Outbreak-Prevention): default plan for the Outbreak Prevention Services Prevention Stage

By default, these plans deploy updates to all products in the Product Directory immediately.

Select or create plans from the Manual and Scheduled download screens. Customize these plans, or create new ones, as required by your network. For example, create deployment plans according to the nature of the outbreak:

- Email-borne virus
- File-sharing virus

Deploying updates to the Product Directory is separate from the download process.

Control Manager downloads the components and follows the deployment plan according to manual or scheduled download settings.

When creating or implementing a deployment plan, consider the following points:

- Assign deployment schedules to folders, not to specific products.

  Planning the contents of the Product Directory folders, therefore, becomes very important.

- You can only include one folder for each deployment plan schedule.

  However, you can specify more than one schedule per deployment plan.

- Control Manager bases the deployment plan delays on the completion time of the download, and these delays are independent of each other.

  For example, if you have three folders to update at 5 minute intervals, you can assign the first folder a delay of 5 minutes, and then set delays of 10 and 15 minutes for the two remaining folders.

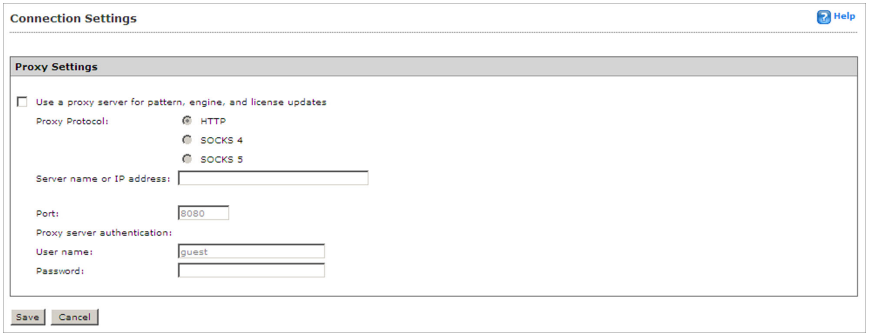
Configuring Proxy Settings

Configure the proxy server connection for component downloads and for license updates.

Procedure

1. Navigate to **Administration** > **Settings** > **Proxy Settings**.

   The **Connection Settings** screen appears.



2. Select **Use a proxy server for pattern, engine, and license updates**.
3. Select the protocol:
   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**
4. Type the host name or IP address of the server in the **Server name or IP address** field.
5. Type a port number in the **Port** field.
6. Type a log on name and password if your server requires authentication.
7. Click **Save**.

Configuring Update/Deployment Settings

Using HTTPS to download components from the Trend Micro ActiveUpdate server (the default download source) or other update source provides a more secure method for retrieving components.

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

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

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

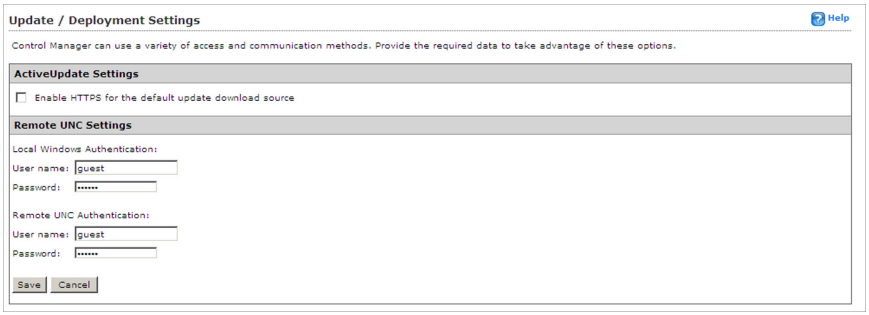
The **remote UNC authentication** feature uses a user account from the component source server that has permission to share a folder to which Control Manager will download updates.

Enabling HTTPS Download

Procedure

1. Navigate to **Updates** > **Update/Deployment Settings**.

   The **Update/Deployment Settings** screen appears.



2. Select **Enable HTTPS for the default update download source**.

3. Click **Save**.
4. Navigate to the **Manual Download** or **Scheduled Download** screen.
5. On the working area under **Download settings**, select **Internet: Trend Micro update server** or specify your organization's component source server in the **Other update source** field.
6. Click **Save**.

Enabling UNC Download

Procedure

1. Navigate to **Updates** > **Update/Deployment Settings**.

   The **Update/Deployment Settings** screen appears.
2. Type the **Local Windows Authentication** and **Remote UNC Authentication** user names and passwords.
3. Click **Save**.
4. Navigate to the **Manual Download** or **Scheduled Download** screen.
5. On the working area under **Download settings**, select **Other update source** and then specify the shared network folder.
6. Click **Save**.

Setting "Log on as batch job" Policy

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

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

Procedure

1. Click **Start** > **Settings** > **Control Panel**.
2. Click **Administrative Tools**.
3. Open **Local Security Policy**. The Local Security Settings screen appears.
4. Click **Local Policies** > **User Rights Assignment**.
5. Double-click **Log on as a batch job**.

   The **Log on as a batch job Properties** dialog box appears.
6. Add the user if they do not appear on the list.

Using Logs

Although Control Manager receives data from various log types, Control Manager allows users to query the log data directly from the Control Manager database. Users can then specify filtering criteria to gather only the data they need.

Control Manager also introduces log aggregation. Log aggregation can improve query performance and reduce the network bandwidth managed products require when sending logs to Control Manager. However, this comes at a cost of lost data through aggregation. Control Manager cannot query data that does not exist in the Control Manager database.

Understanding Managed Product Logs

Managed product logs contain information about the performance of your managed products. You can obtain information for specific products or groups of products administered by the parent or child server. With Control Manager's data query on logs and data filtering capabilities, administrators can focus on the information they need.

Note

More logs mean abundant information about the Control Manager network. However, these logs occupy disk space. You must balance the need for information with your available system resources.

Managed products generate different kinds of logs depending on their function.

TABLE A-11. Managed Product Logs

LOG CATEGORY	DESCRIPTION
Product Information	Product information logs provide information on subjects ranging from user access and events on managed products to component deployment and update status. • Managed Product Information • Component Information
Security Threat Information	Security threat logs provide information on known and potential security threats detected on your network. • Virus/Malware Information • Spyware/Grayware Information • Content Violation Information • Spam Violation Information • Policy/Rule Violation Information • Web Violation/Reputation Information • Suspicious Threat Information • Overall Threat Information
Data Protection Information	Data Protection logs provide information on DLP incidents, template matches, and incident sources. • Data Loss Prevention Information

Querying Log Data

Ad Hoc Queries provide administrators with a quick method to pull information directly from the Control Manager database. The database contains all information collected from all products registered to the Control Manager server (log aggregation can affect the data available to query). Ad Hoc Queries provide a very powerful tool for administrators.

While querying data, administrators can filter the query criteria so only the data they need returns. Administrators can then export the data to CSV or XML format for further analysis or save the query for future use. Control Manager also supports sharing saved queries with other users so others can benefit from useful queries.

Completing an Ad Hoc query consists of the following process:

- Step 1: Select the managed product or current Control Manager server for the query
- Step 2: Select the data view to query
- Step 3: Specify filtering criteria and the specific information that displays
- Step 4: Save and complete the query
- Step 5: Export the data to a CSV or XML file

Note

Control Manager supports sharing saved Ad Hoc Queries with other users. Saved and shared queries appear on the **Saved Ad Hoc Queries** screen.

Understanding Data Views

A data view is a table consisting of clusters of related data cells. Data views provide the foundation on which users perform Ad Hoc Queries to the Control Manager database.

Control Manager allows direct queries to the Control Manager database. Data views are available to Control Manager 5 report templates and to Ad Hoc Query requests.

Data views are tables filled with information. Each heading in a data view acts as a column in a table. For example, the Virus/Malware Action/Result Summary data view has the following headings:

- Action Result
- Action Taken
- Unique Endpoints
- Unique Sources
- Detections

As a table, a data view takes the following form with potential subheadings under each heading:

TABLE A-12. Sample Data View

ACTION RESULT	ACTION TAKEN	UNIQUE ENDPOINTS	UNIQUE SOURCES	DETECTIONS

This information is important to remember when specifying how data displays in a report template.

Control Manager separates data views into two major categories: Product Information and Security Threat Information. See the appendix for more information about data views. The major categories separate further into several subcategories, with the subcategories separated into summary information and detailed information.

Understanding Reports

Control Manager reports consist of two parts: report templates and report profiles. Where a report template determines the look and feel of the report, the report profile specifies the origin of the report data, the schedule/time period, and the recipients of the report.

Control Manager 5.0 introduced radical changes over previous Control Manager versions by introducing customized reports for Control Manager administrators. Control

Manager 6.0 continues to support report templates from previous Control Manager versions, however Control Manager 6.0 allows administrators to design their own custom report templates.

Understanding Control Manager Report Templates

A report template outlines the look and feel of Control Manager reports. Control Manager categorizes report templates according to the following types:

- Control Manager 5 templates: User-defined customized report templates that use direct database queries (database views) and report template elements (charts and tables). Users have greater flexibility specifying the data that appears in their reports compared to report templates from previous Control Manager versions.
- Control Manager 3 templates: Includes pre-defined templates.

Understanding Control Manager 5 Templates

Control Manager 5 report templates use database views as the information foundation for reports. For more information on data views, see *Understanding Data Views on page A-67*. The look and feel of generated reports falls to the report elements. Report elements consist of the following.

TABLE A-13. Control Manager 5 Report Template Elements

TEMPLATE ELEMENT	DESCRIPTION
Page break	Inserts a page break for a report. Each report page supports up to three report template elements.
Static text	Provides a user-defined description or explanation for the report. Static text content can contain up to 4096 characters.
Bar chart	Inserts a bar chart into a report template.
Line chart	Inserts a line graph into a report template.
Pie chart	Inserts a pie chart into a report template.
Dynamic table	Inserts a dynamic table/pivot table into a report template.

Template Element	Description
Grid table	Inserts a table into a report template. The information in a grid table will be the same as the information that displays in an Ad Hoc Query.

Each Control Manager 5 template can contain up to 100 report template elements. Each page in the report template can contain up to three report template elements. Use page breaks to create report template pages.

To better understand Control Manager 5 report templates, Trend Micro provides the following pre-defined report templates.

Note

Access the **Report Templates** screen to view the Trend Micro pre-defined templates.

Table A-14. Control Manager 5 Pre-defined Templates

Template	Description
TM-Content Violation Detection Summary	Provides the following information: • Content Violation Detection Grouped by Day (Line chart) • Policy in Violation Count Grouped by Day (Line chart) • Sender/Users in Violation Count Grouped by Day (Line chart) • Recipient Count Grouped by Day (Line chart) • Top 25 Policies in Violation (Bar chart) • Content Violation Policy Summary (Grid table) • Top 25 Senders/Users in Violation (Bar chart) • Content Violation Senders/Users in Violation Summary (Grid table) • Action Result Summary (Pie chart)

Template	Description
TM-Managed Product Connection/Component Status	Provides the following information: • Server/Appliance Connection Status (Pie chart) • Client Connection Status (Pie chart) • Server/Appliance Pattern File/Rule Update Status (Pie chart) • Client Pattern File/Rule Update Status (Pie chart) • Server/Appliance Scan Engine Update Status (Pie chart) • Client Scan Engine Update Status (Pie chart) • Pattern File/Rule Summary for Servers/Appliances (Grid table) • Pattern File/Rule Summary for Clients (Grid table) • Scan Engine Summary for Servers/Appliances (Grid table) • Scan Engine Summary for Clients (Grid table)
TM-Overall Threat Summary	Provides the following information: • Complete Network Security Risk Analysis Summary (Grid table) • Network Protection Boundary Summary (Grid table) • Security Risk Entry Point Analysis Information (Grid table) • Security Risk Destination Analysis Information (Grid table) • Security Risk Source Analysis Information (Grid table)

Template	Description
TM-Spam Detection Summary	Provides the following information: • Spam Detection Grouped by Day (Line chart) • Recipient Domain Count Grouped by Day (Line chart) • Recipient Count Grouped by Day (Line chart) • Top 25 Recipient Domains (Bar chart) • Overall Spam Violation Summary (Grid table) • Top 25 Spam Recipients (Bar chart) • Spam Recipient Summary (Grid table)
TM-Spyware/Grayware Detection Summary	Provides the following information: • Spyware/Grayware Detection Grouped by Day (Line chart) • Unique Spyware/Grayware Count Grouped by Day (Line chart) • Spyware/Grayware Source Count Grouped by Day (Line chart) • Spyware/Grayware Destination Count Grouped by Day (Line chart) • Top 25 Spyware/Grayware (Bar chart) • Overall Spyware/Grayware Summary (Grid table) • Top 25 Spyware/Grayware Sources (Bar chart) • Spyware/Grayware Source Summary (Grid table) • Top 25 Spyware/Grayware Destinations (Bar chart) • Spyware/Grayware Destination Summary (Grid table) • Action Result Summary (Pie Chart) • Spyware/Grayware Action/Result Summary (Grid table)

Template	Description
TM-Suspicious Threat Detection Summary	Provides the following information: • Suspicious Threat Detection Grouped by Day (Line chart) • Rule in Violation Count Grouped by Day (Line chart) • Sender Count Grouped by Day (Line chart) • Recipient Count Grouped by Day (Line chart) • Source IP Address Count Grouped by Day (Line chart) • Destination IP Address Count Grouped by Day (Line chart) • Top 25 Senders (Bar chart) • Top 25 Recipients (Bar chart) • Suspicious Threat Sender Summary (Grid table) • Suspicious Threat Riskiest Recipient Summary (Grid table) • Top 25 Source IP Addresses (Bar chart) • Top 25 Destination IP Addresses (Bar chart) • Suspicious Threat Source Summary (Grid table) • Suspicious Threat Riskiest Destination Summary (Grid table) • Top 25 Protocol Names (Bar chart) • Suspicious Threat Protocol Detection Summary (Grid table) • Overall Suspicious Threat Summary (Grid table)

Template	Description
TM-Virus/Malware Detection Summary	Provides the following information: • Virus/Malware Detection Grouped by Day (Line chart) • Unique Virus/Malware Count Grouped by Day (Line chart) • Infection Destination Count Grouped by Day (Line chart) • Top 25 Virus/Malware (Bar chart) • Overall Virus/Malware Summary (Grid table) • Top 25 Infection Sources (Bar chart) • Virus/Malware Infection Source Summary (Grid table) • Top 25 Infection Destinations (Bar chart) • Virus/Malware Infection Destination Summary (Grid table) • Action Result Summary (Pie chart) • Virus/Malware Action/Result Summary (Grid table)
TM-Web Violation Detection Summary	Provides the following information: • Web Violation Detection Grouped by Day (Line chart) • Policy in Violation Count Grouped by Day (Line chart) • Client in Violation Count Grouped by Day (Line chart) • URL in Violation Count Grouped by Day (Line chart) • Top 25 Policies in Violation (Bar chart) • Overall Web Violation Summary (Grid table) • Top 25 Clients in Violation (Bar chart) • Web Violation Client IP Address Summary (Grid table) • Top 25 URLs in Violation (Bar chart) • Web Violation URL Summary (Grid table) • Filter/Blocking Type Summary (Pie chart)

Understanding Control Manager 3 Templates

Control Manager added 87 pre-generated report templates divided into six categories: Executive Summary, Gateway, Mail Server, Server, Desktop, Network Products, and Data Loss Prevention.

Note

In Control Manager 3.5, spyware/grayware were no longer considered viruses. This change affects the virus count in all original virus-related reports.

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

Use the Report Category list on the Control Manager screen to peruse the six categories of reports listed below:

TABLE A-15. Executive Summary Reports and Report Types

EXECUTIVE SUMMARY REPORTS	REPORT TYPES
Spyware/Grayware Detection Reports	• Spyware/Grayware detected • Most commonly detected Spyware/ Grayware (10, 25, 50, 100) • Detected Spyware/Grayware list for all entities
Virus Detection Reports	• Viruses detected • Most commonly detected viruses (10, 25, 50, 100) • Virus infection list for all entities

Executive Summary Reports	Report Types
Comparative Reports	• Spyware/Grayware, grouped by (Day, Week, Month) • Viruses, grouped by (Day, Week, Month) • Damage cleanups, grouped by (Day, Week, Month) • Spam, grouped by (Day, Week, Month)
Vulnerability Reports	• Machine risk level assessment • Vulnerability assessment • Most commonly cleaned infections (10, 25, 50, 100) • Worst damage potential vulnerabilities (10, 25, 50, 100) • Vulnerabilities ranked by risk level

Table A-16. Gateway Product Reports and Report Types

Gateway Product Reports	Report Types
Spyware/Grayware Detection Reports	• Spyware/Grayware detected • Most commonly detected Spyware/ Grayware (10, 25, 50, 100)
Virus Detection Reports	• Viruses detected • Most commonly detected viruses (10, 25, 50, 100)
Comparative Reports	• Spyware/Grayware, grouped by (Day, Week, Month) • Spam, grouped by (Day, Week, Month) • Viruses, grouped by (Day, Week, Month)

Gateway Product Reports	Report Types
Deployment Rate Reports	• Detailed summary • Basic summary • Detailed failure rate summary • OPS deployment rate for IMSS

Table A-17. Mail Server Product Reports and Report Types

Mail Server Product Reports	Report Types
Spyware/Grayware Detection Reports	• Spyware/Grayware detected • Most commonly detected Spyware/ Grayware (10, 25, 50, 100)
Virus Detection Reports	• Viruses detected • Top senders of infected email (10, 25, 50, 100) • Most commonly detected viruses (10, 25, 50, 100)
Comparative Reports	• Spyware/Grayware, grouped by (Day, Week, Month) • Viruses, grouped by (Day, Week, Month)
Deployment Rate Reports	• Detailed summary • Basic summary • Detailed failure rate summary

Table A-18. Server Based Product Reports and Report Types

Server Based Product Reports	Report Types
Spyware/Grayware Detection Reports	• Spyware/Grayware detected • Most commonly detected Spyware/ Grayware (10, 25, 50, 100)

Server Based Product Reports	Report Types
Virus Detection Reports	• Viruses detected • Most commonly detected viruses (10, 25, 50, 100)
Comparative Reports	• Spyware/Grayware, grouped by (Day, Week, Month) • Viruses, grouped by (Day, Week, Month)
Deployment Rate Reports	• Detailed summary • Basic summary • Detailed failure rate summary

Table A-19. Desktop Product Reports and Report Types

Desktop Product Reports	Report Types
Spyware/Grayware Detection Reports	• Spyware/Grayware detected • Most commonly detected Spyware/ Grayware (10,25,50,100)
Virus Detection Reports	• Viruses detected • Most commonly detected viruses (10,25,50,100)
OfficeScan Client Information Reports	• Detailed summary • Basic summary
OfficeScan Product Registration Report	Registration status
Comparative Reports	• Spyware/Grayware, grouped by (Day, Week, Month) • Viruses, grouped by (Day, Week, Month)

Desktop Product Reports	Report Types
OfficeScan Server Deployment Reports	• Detailed summary • Basic summary • Detailed failure rates summary
OfficeScan Damage Cleanup Services Reports	• Detailed summary • Most commonly cleaned infections (10, 25, 50, 100)

Table A-20. Network Product Reports and Report Types

Network Product Reports	Report Types
Network VirusWall Reports	• Policy violation report, grouped by (Day, Week, Month) • Most commonly detected violative clients (10, 25, 50, 100) • Service violation report, grouped by (Day, Week, Month)
Trend Micro Total Discovery Appliance Reports	• Incident summary report, grouped by (Day, Week, Month) • High risk clients (10, 25, 50, 100) • Summary of known and unknown risks report

TABLE A-21. Data Loss Prevention Reports and Report Types

DATA LOSS PREVENTION REPORTS	REPORT TYPES
Top DLP Incident Sources	• Incidents by sender (10, 20, 30, 40, 50) • Incidents by host name (10, 20, 30, 40, 50) • Incidents by recipient (10, 20, 30, 40, 50) • Incidents by source IP address (10, 20, 30, 40, 50) • Incidents by URL (10, 20, 30, 40, 50) • Incidents by User (10, 20, 30, 40, 50) • Top template matches (10, 20, 30, 40, 50) • Incident distribution by channel • Incident trend, grouped by (Day, Week, Month) • Incidents by channel, grouped by (Day, Week, Month)

Data Loss Prevention Reports	Report Types
Significant Incident Increase	• Significant incident increase (%) by channel (10, 20, 30, 40, 50) • Significant incident increase by channel (10, 20, 30, 40, 50) • Significant incident increase (%) by sender (10, 20, 30, 40, 50) • Significant incident increase by sender (10, 20, 30, 40, 50) • Significant incident increase (%) by host name (10, 20, 30, 40, 50) • Significant incident increase by host name (10, 20, 30, 40, 50) • Significant incident increase (%) by user (10, 20, 30, 40, 50) • Significant incident increase by user (10, 20, 30, 40, 50) • Significant incident increase (%) by source IP address (10, 20, 30, 40, 50) • Significant incident increase by source IP address (10, 20, 30, 40, 50) • Significant incident increase (%) by template (10, 20, 30, 40, 50) • Significant incident increase by template (10, 20, 30, 40, 50)

Adding One-time Reports

Control Manager supports generating one-time reports from Control Manager 3 and Control Manager 5 report templates. Users need to create Control Manager 5 report templates, while Trend Micro created Control Manager 3 report templates. The process for creating a one-time report is similar for all report types and involves the following:

1. Access the **Add One-time Report** screen and select the report type.

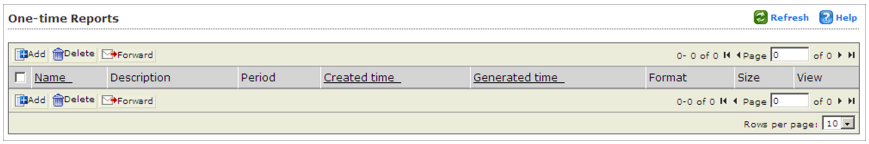
2. Specify the product/products from which the report data generates.
3. Specify the date when the product/products produced the data.
4. Specify the recipient of the report.

Step 1: Access the Add One-time Report Screen and Select the Report Type

Procedure

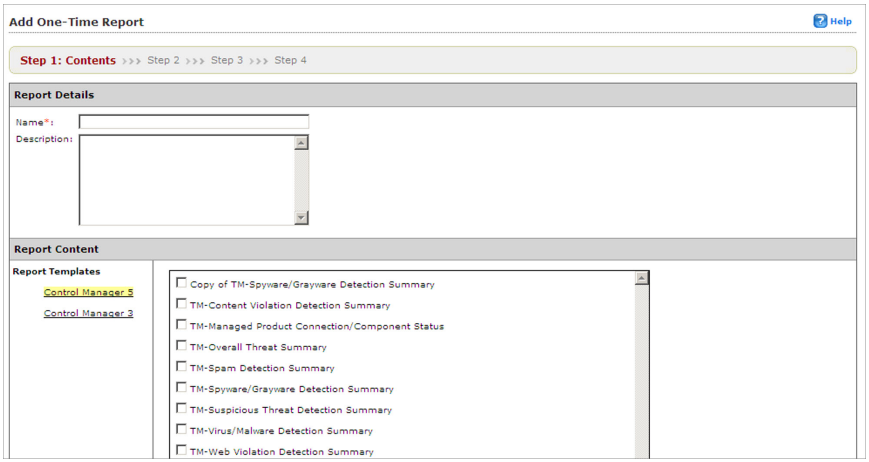
1. Navigate to **Reports** > **One-time Reports**.

   The **One-time Reports** screen appears.



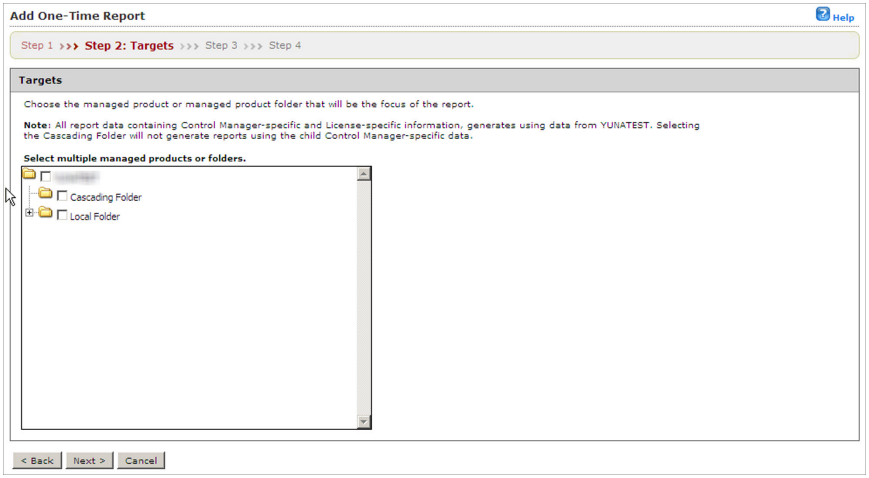
2. Click **Add**.

   The **Add One-time Report > Step 1: Contents** screen appears.



3. Type a name for the report in the **Name** field, under Report Details.
4. Type a description for the report in the **Description** field, under Report Details.
5. Select the Control Manager template to generate the report:
   - **Control Manager 5 report template**:
     a. Select the Control Manager 5 template to generate the report. If the existing reports do not fulfill your requirements, create one from the **Report Templates** screen.
   - **Control Manager 3 report template**:
     a. Click **Control Manager 3** under Report Content. The Control Manager 3 templates appear in the work area to the right, under Report Content.
     b. Select the report category on which to base the report.
     c. Select the Control Manager 3 template data on which to base the template.
6. Select the report generation format:
   - **Control Manager 5 report formats**:
     - Adobe PDF Format (*.pdf)
     - HTML Format (*.html)
     - XML Format (*.xml)
     - CSV Format (*.csv)
   - **Control Manager 3 report formats**:
     - Rich Text Format (*.rtf)
     - Adobe PDF Format (*.pdf)
     - ActiveX
     - Crystal Report Format (*.rpt)
7. Click **Next**.

The **Add One-Time Report > Step 2: Targets** screen appears.



Step 2: Specify the Product/Products From Which the Report Data Generates:

Procedure

1. Select the managed product or directory from which Control Manager gathers the report information.
2. If the report contains data from a Network VirusWall Enforcer device, specify the clients from which the reports generate:
   - **All clients**: Reports generate from all Network VirusWall Enforcer devices
   - **IP range**: Reports generate from a specific IP address range
   - **Segment**: Reports generate from a specific network segment
3. Click **Next**.

Step 3: Specify the Date That the Product/Products Produced the Data:

Procedure

1. Specify the data generation date:
   - From the drop down list select one of the following:
     - All dates
     - Last 24 hours
     - Today
     - Last 7 days
     - Last 14 days
     - Last 30 days
   - Specify a date range:
     - Type a date in the **From** field.
     - Specify a time in the accompanying **hh** and **mm** fields.
     - Type a date in the **To** field.
     - Specify a time in the accompanying **hh** and **mm** fields.

     Note

     Click the calendar icon next to the **From** and **To** fields to use a dynamic calendar to specify the date range.

2. Click **Next**.

Step 4: Specify the Recipient of the Report:

Procedure

1. Type a title for the email message that contains the report in the **Subject** field.
2. Type a description about the report in the **Message** field.
3. Select **Email the report as an attachment** to enable sending the report to a specified recipient.
4. Specify to select users or groups from the **Report Recipients** list.
5. Select the users/groups to receive the report and click the **>>** button.
6. Click **Finish** after selecting all users/groups to receive the report.

Adding Scheduled Reports

Control Manager supports generating scheduled reports from Control Manager 3 and Control Manager 5 report templates. Users need to create Control Manager 5 report templates, while Trend Micro created Control Manager 3 report templates. The process for creating a scheduled report is similar for all report types:

1. Access the **Add Scheduled Report** screen and select the report type.
2. Specify the product/products from which the report data generates.
3. Specify the date when the product/products produced the data.
4. Specify the recipient of the report.

Step 1: Access the Add Scheduled Report Screen and Select the Report Type

Procedure

1. Navigate to **Reports** > **Scheduled Reports**.

2. Click **Add**.
3. Type a name for the report in the **Name** field.
4. Type a meaningful description for the report in the **Description** field.
5. Select the Control Manager template to generate the report:
   - Control Manager 5 report template:
     a. Select the Control Manager 5 template to generate the report. If the existing reports do not fulfill your requirements, create one from the Report Templates screen.
   - Control Manager 3 report template:
     a. Click **Control Manager 3** under Report Content. The Control Manager 3 templates appear in the work area to the right, under Report Content.
     b. Select the report category on which to base the report.
     c. Select the Control Manager 3 template data on which to base the template.
6. Select the report generation format:
   - Control Manager 5 report formats:
     - Adobe PDF Format (*.pdf)
     - HTML Format (*.html)
     - XML Format (*.xml)
     - CSV Format (*.csv)
   - Control Manager 3 report formats:
     - Rich Text Format (*.rtf)
     - Adobe PDF Format (*.pdf)
     - ActiveX
     - Crystal Report Format (*.rpt)

7. Click **Next**.

Step 2: Specify the Product/Products from Which the Report Data Generates

Procedure

1. Select the managed product or directory from which Control Manager gathers the report information.
2. If the report contains data from a Network VirusWall Enforcer device, specify the clients from which the reports generate:
   - **All clients**: Reports generate from all Network VirusWall Enforcer devices
   - **IP range**: Reports generate from a specific IP address range
   - **Segment**: Reports generate from a specific network segment
3. Click **Next**.

Step 3: Specify the Date that the Product/Products Produced the Data

Procedure

1. Specify how often reports generate:
   - **Daily**: Reports generate daily.
   - **Weekly**: Reports generate weekly on the specified day.
   - **Bi-weekly**: Reports generate every two weeks on the specified day.
   - **Monthly**: Reports generate monthly on the first day of the month, the 15th of the month, or the last day of the month.
2. Specify the data range:

- **Reports include data up to the Start the schedule time specified below**: This means that a report could have up to 23 hours more data contained in the report. While this has a small affect on weekly or monthly reports, this can make a "daily" report with almost two days worth of data depending on the Start schedule time.
- **Reports include data up to 23:59:59 of the previous day**: This means that data collection for the report stops just before midnight. Reports will be an exact time period (example: Daily reports will be 24 hours) but will not contain the absolute latest data.

3. Specify when the report schedule starts:
   - **Immediately**: The report schedule starts immediately after enabling the report.
   - **Start on**: The report schedule starts on the date and time specified in the accompanying fields.

   a. Type a date in the **mm/dd/yyyy** field.

   b. Specify a time in the accompanying **hh** and **mm** fields.

   Note

   Click the calendar icon next to the **mm/dd/yyyy** field to use a dynamic calendar to specify the date range.

4. Click **Next**.

Step 4: Specify the Recipient of the Report

Procedure

1. Type a title for the email message that contains the report in the **Subject** field.
2. Type a description about the report in the **Message** field.
3. Select **Email the report as an attachment** to enable sending the report to a specified recipient.
4. Specify to select users or groups from the **Report Recipients** list.

5. Select the users/groups to receive the report and click the **>>** button.
6. Click **Finish** after selecting all users/groups to receive the report.

Appendix B

Deployment Considerations

This appendix provides an overview about Endpoint Encryption deployment planning.

Note

For information about running a pilot program before mass deployment, see *Endpoint Encryption Pilot Deployment on page C-1*.

Topics include:

- *Initial Deployment Checklist on page B-2*
- *Security Infrastructure Checklist on page B-4*
- *Establishing Policy and Security Profiles on page B-6*
- *Change Management Considerations on page B-7*
- *End User Communication on page B-11*

Initial Deployment Checklist

This questionnaire assists in defining the project team, documenting the operating environment, assessing architecture requirements, facilitating review of desktop hardware and software profiles, and defining security concerns and administrative or support processes.

TABLE B-1. Initial Deployment Checklist

ENTITY OR OBJECT	QUESTIONS
End users	1. What is the total number of users to be deployed? 2. Of that number, how many are: • Enterprise Administrator • Group Administrator • Authenticator (Help Desk Personnel) • End User
Endpoints	1. Is there a standard number of partitions on hardware? 2. Do devices have multiple physical hard drives? 3. Do any devices have dual boot managers? 4. What standard software is installed? Check the following: a. Antivirus b. Security applications that block software installs c. Previous encryption products

Entity or Object	Questions
Enterprise networks and databases	1. How many PolicyServer instances are required to support the user base? a. Estimate maximum number of users in three years. b. If domain authentication is used, one PolicyServer is required for each Active Directory domain. 2. Is load balancing on the servers required? a. Load-balancing is recommended for installations that require redundancy and high-availability for PolicyServers. b. Clustering can be used to provide redundancy and high-availability for the database servers. 3. What are the database size estimates? a. Estimate maximum number of users in three years. b. Approximate space required is 1 GB per year for every 1,000 end users. 4. Will agents be required to communicate with PolicyServer over the Internet? a. Check with internal network/ security team to understand requirements to make a web server available on the Internet. b. The following are fully supported with an external facing PolicyServer: • Domain authentication/single sign-on can be used over the Internet • Policy updates via the Internet • Device auditing via the Internet • Online password resets

Security Infrastructure Checklist

Review existing security infrastructure before deploying a new IT service into the production environment. Trend Micro provides a Security Infrastructure Checklist that contains the items that should be reviewed for the following areas:

- end user
- Incident Response
- Risk Assessment
- Human Resources
- Compliance

For more information, see *Security Infrastructure Checklist on page B-4*.

Security Infrastructure Checklist

The following table describes questions to ask about the existing and potential security infrastructure to better understand how deploying Endpoint Encryption may affect the organization.

TABLE B-2. Security Infrastructure Checklist

CHECK	QUESTIONS
End user	1. Does the end user training include the new functionality that Endpoint Encryption provides? 2. Is the Acceptable Use Policy (AUP) updated to include encryption services, especially any penalties for not using or bypassing encryption? 3. Are users notified when they log on to the endpoint that aligns with the AUP? 4. Are all users fully trained on how to report a lost or stolen device? 5. Have users been trained on procedures regarding failed login attempts and password recovery? 6. Is there a policy regarding encryption of confidential documents that are sent outside of the organization? 7. Have any new password policies been added to the AUP?
Incident Response	1. Has the Incident Response (IR) policy been updated to include actions taken when a device is lost or stolen? 2. Has an audit log review schedule been established for the PolicyServer logs? 3. Have the email alerts been added to the IR policy, including the recipients and the expected response when an alert is received? 4. Have specific criteria been developed to allow a device to be killed or wiped, including any audit trail documentation after the action is completed?
Risk Assessment	1. Has a new risk assessment been conducted to show the change in risk profile Endpoint Encryption has provided? 2. Have Risk Assessment procedures been updated to include the audit data that the PolicyServer provides?

Check	Questions
Disaster Recovery	1. Has PolicyServer been added to the Critical Services list? 2. Is the DR/BC plan updated to include the restoration of the Policy Server service? 3. Is a process developed to allow user data to be recovered from a device?
Human Resources	1. Is the New Employee checklist updated to include any new process for Endpoint Encryption? 2. Is the termination processes updated to include any new process for Endpoint Encryption - especially device kill/wipe?
Compliance	1. Is the compliance profile updated to include the benefits that Endpoint Encryption provides? 2. Has a compliance review been conducted on all aspects on the Endpoint Encryption implementation and deployment?

Establishing Policy and Security Profiles

Trend Micro Endpoint Encryptionestablished default security policies that should be reviewed based on deployment and protection objectives. There are default policies for user name, password complexity and change requirements, device control, policy synchronization, device lock, and device wipe, among other default policy settings. Default policies can easily be changed depending upon security objectives and regulatory compliance mandates for data protection.

When using Endpoint Encryption to control removable media, make decisions about what USB media is allowed, when they can be used, and where they can be used (on or off network; any time) to ensure that users are compliant with security policies and objectives.

Refer to the *Endpoint Encryption Administrator's Guide* for a complete description of policies, default values, and configurable options.

Note

When using Endpoint Encryption to manage policies and removable media:

- Test and validate policies templates before distributing.
- Decide which USB devices are allowed for USB drives and removable media, when they can be used, and where they can be used (on-network, off-network, or both) to ensure users are compliant.

Change Management Considerations

PolicyServer and related databases are mission critical services. Change management considerations help ensure availability for end users attempting to authenticate on the network. When changes are necessary:

- Actively monitor CPU usage and establish a threshold for when the PolicyServer Windows Service should be restarted.
- Regularly restart the service on a schedule that fits with the organization's established maintenance windows (daily, weekly, monthly).
- Restart PolicyServer Windows service whenever maintenance is performed on the Active Directory environment, the server, database, or related communications.
- Regularly back up PolicyServer databases, similar to any enterprise critical databases.
- Primary and log databases with off-site storage nightly back up is recommended.

WARNING!

Any changes to the Active Directory or database environments may affect connectivity with PolicyServer.

Full Disk Encryption Pre-installation Checklist

The Full Disk Encryption installer automatically checks the target system to make sure that all necessary system requirements are met before installing the agent. If a system

incompatibility is discovered, the installer closes and generates the `PreInstallCheckReport.txt` in the same location as the installer.

Use the pre-installation checklist to determine which system requirements are not met. The checklist file is located in the same folder as the Full Disk Encryption installer.

TABLE B-3. Conditions Checked by the Installer

SPECIFICATION	REQUIREMENT	DESCRIPTION
Supported OS	Not all operating systems are supported	Full Disk Encryption cannot be installed on certain versions of Windows.
Encryption Management for Microsoft BitLocker is already installed	No other full disk encryption product can be installed	Encryption Management for Microsoft BitLocker must not be installed. Uninstall Encryption Management for Microsoft BitLocker to install Full Disk Encryption or use Encryption Management for Microsoft BitLocker instead.
Fixed media	Internal hard drive	Full Disk Encryption cannot be installed on removable drives running Windows.
Multiple hard disks	Only one hard disk is allowed.	The endpoint must only have one hard disk. Multiple disk environments are not supported.
Free space	256 MB minimum	
Memory	512 MB minimum 1 GB recommended	
Partition count	Fewer than 25 partitions	Partitions with extended MBRs are not available.
Partition type	Only MBR is supported	GUID partition table (necessary for disks larger that 2 TB) is not currently supported.

Specification	Requirement	Description
Physical drive is bootable	A bootable partition is required	Full Disk Encryption must be installed on a bootable table.
SCSI disk	ATA, AHCI or IRRT drive controller. SCSI is not supported	• Check only provides a warning; Windows may report a SATA drive as SCSI • If the disk is not a true SCSI, Full Disk Encryption can be installed. If unsure, physically check the drive
Microsoft .Net Framework	.Net 2.0 SP1 or newer required for Windows XP or earlier	Skipped for Windows Vista or newer operating systems.
SED hardware compatibility	Hardware encryption is enabled if present	Full Disk Encryption currently supports the following: • Seagate DriveTrust drives • Seagate OPAL and OPAL 2 drives • SanDisk self-encrypting solid-state drives
BitLocker is enabled	BitLocker must be disabled	Full Disk Encryption and BitLocker cannot simultaneously provide full disk encryption.

Note

If the pre-installation check fails for any of these reasons, contact Trend Micro for assistance.

Pre-Installation Check Report Example

```
Trend Micro Full Disk Encryption PreInstall Checks
------------------------------
    Name:     Supported OS Test
    Description:    Checks the supported OS.
    Status:     Pass
------------------------------
    Name:     Fixed Media
    Description:    Checks that the physical disk is fixed (not
                    removable).
    Status:     Pass
------------------------------
    Name:     Free space
    Description:    Checks that the disk has enough free space.
    Status:     Pass
------------------------------
    Name:     Memory
    Description:    Checks that there is enough RAM to run
                    Trend Micro Full Disk Encryption.
    Status:     Pass
------------------------------
    Name:     Partitions Count
    Description:    Checks that the disk does not have too many
                    partitions.
    Status:     Pass
------------------------------
    Name:     Partition Type
    Description:    Checks that the disk is partition with a
                    compatible partitioning method.
    Status:     Pass
------------------------------
    Name:     PhysicalDrive is bootable
    Description:    Checks that the PhysicalDisk0 contains the
                    boot partition.
    Status:     Pass
------------------------------
    Name:     SCSI disk
    Description:    Checks that the disk is SCSI or not.
    Status:     Warn
------------------------------
```

```
    Name:      .Net Framework runtime
    Description:    Checks that the .NET runtime version is at
                    least 2.0 (SP1).
    Status:     Skip
-----------------------------
    Name:     SED hardware compatibility
    Description:    Checks that the Machine has SED hardware
                    compatibility
    Status:     Skip
-----------------------------
    Name:     BitLocker is not installed
    Description:    Checks that the device does not have
                    BitLocker installed.
    Status:     Pass
```

End User Communication

To limit the impact to productive and to ease the transition to encryption security, forewarn end users with a communication plan. In addition, post-deployment communicate plays an important role in easing the adjustment to using Endpoint Encryption.

End User Questions to Answer

A common barrier to enterprise adoption is lack of communication. The need for clear end user communication that addresses three questions is essential to a successful implementation:

1. Why do we need Endpoint Encryption?
2. How does Endpoint Encryption help me and the organization?
3. What will change?

Share What, When, and Why

Trend Micro recommends that the executive sponsor of the data protection project send a message to the end users communicating the importance of the project to the

company and the benefits to the users. The Knowledge Base has a number of end user communication templates that can be leveraged and customized to meet your communications needs before distributing Endpoint Encryption.

Introduce the Change

1. One month before roll-out, have the executive sponsor outline why new software/ hardware encryption is being introduced and how complying with the new processes benefits the end user as well as the company.
2. Provide a roll-out schedule to the users, what to expect after day 1, and confirm how end users can get help with the new software.

Communicate a Week Before Roll-out

1. Reiterate what changes are coming and what to expect on the day new authentication procedures are required on their endpoints.
2. Include screen captures and detailed instructions on user name or password conventions, and other internal support services.

Communicate the Day Before Roll-out

1. Reinforce the timing of the roll-out schedule, what to expect and where to go for help.
2. Distribute cheat-sheets, Help Desk information and provide the contact information for the on-site point of contact that will be available to assist users the next day.

Communicate After Roll-out

1. Reiterate Help Desk information and provide the contact information for the on-site point of contact that will be available to assist users the next day.
2. Provide tools for troubleshooting assistance.

Appendix C

Endpoint Encryption Pilot Deployment

This appendix explains how to conduct a pilot program before deploying Endpoint Encryption across the entire organization. Trend Micro recommends running a pilot program and performing a test deployment to a small group of users before deploying to a larger audience.

Note

For information about general deployment considerations, see *Deployment Considerations on page B-1*.

Topics include:

- *About a Pilot Program on page C-2*
- *Assigning a Project Team on page C-2*
- *Implement a Phased Roll-out Strategy on page C-2*
- *Endpoint Encryption Pilot Checklist on page C-3*

About a Pilot Program

A pilot program allows an organization to finalize the deployment methodology to be used when installing Endpoint Encryption. The most effective pilot programs involve different departments, target users, and devices. For example, if the organization supports ten different laptops manufacturers, then each of those devices should be included in the pilot. Similarly, if certain high-profile groups are of particular concern, one or two members of the group(s) should be enlisted to participate in the pilot.

Assigning a Project Team

A successful implementation includes maintaining continuity as well as achieving buy-in from internal users. Structuring the team to include one or more strategic members from the departments impacted by the software deployment can help achieve buy-in and results in stronger project team leadership. At a minimum, it is recommended your project team include one or more members from each of the following groups:

- Executive Management
- Enterprise Application Servers
- Enterprise Database Administrators
- Data Security
- Desktop Support
- Disaster Recovery

Implement a Phased Roll-out Strategy

If the pilot program was successful, start deploying the program by targeting batches of 25-50 endpoints to begin production distribution of the solution. Ensure that the deployment engineers are on-site with the first deployment group the day after the new solution is installed so immediate assistance can be provided. After building upon the success of the initial batch of agents, deploy 100-200 a night. As the deployment

methodology is further validated in the production environment and as the internal IT and Help Desk teams agree, it is possible to target thousands of devices at a time for deployment.

Endpoint Encryption Pilot Checklist

Pilot Program Check List	Date	Notes
PolicyServer configured as required • Policies set • Groups created • Users created/imported		
Client software installed (Full Disk Encryption and/or File Encryption) • Software copied locally to machine and run successfully		
Administrator, Authenticator and User accounts can access devices based on policy settings • Fixed Password • Single Sign-on • Smart Card		

Pilot Program Check List	Date	Notes
All computers compatible with new software • Preboot authentication and/or connectivity confirmed • Encryption completes • Machine functions normally • Files/Folders encrypted per policy • USB port controlled as defined by policy • PolicyServer alerts, event logs and reports confirm administrator and end user activity		
End-users can perform business as usual activities • Access windows via existing user name/password or SSO from pre-boot • Machine functions normally both on and off the network • User has access to all user data, applications and network resources		

Pilot Program Check List	Date	Notes
System Administrators test support processes • Create backup administrator accounts • Test reporting and alerts • Use Full Disk Encryption Recovery Console to back up and recover files • Use Full Disk Encryption Recovery CD to decrypt device and remove pre-boot • Test Remote Help authentication process • Test device lock and device wipe.		

Appendix D

Endpoint Encryption Services

The following table describes all Endpoint Encryption services. Use it to understand which services control which Endpoint Encryption agent or feature and to troubleshoot a problem.

TABLE D-1. Endpoint Encryption Services

PLATFORM	SERVICE OR DAEMON NAME	DISPLAY NAME	DESCRIPTION	FILE NAME
PolicyServer	PolicyServer Windows Service	PolicyServer Windows Service	Manages communication between Endpoint Encryption services and databases.	`PolicyServerWindowService.exe`
	TMEEService	Endpoint Encryption Service	Manages Endpoint Encryption agent 5.0 (and above) communication in an encrypted channel (RESTful).	`TMEEService.exe`
	IIS/ MAWebService2	Legacy Web Service	Manages Endpoint Encryption agent 3.1.3 (and older) communication in an encrypted channel (SOAP).	N/A
	TMEEForward	TMEEForward	Forwards traffic from Endpoint Encryption 5.0 Patch 3 agents to PolicyServer.	TMEEForward.exe
	TMEEProxyWindowsService	PolicyServer LDAProxy Windows Service	Provides secure communications from Trend Micro PolicyServer to remote LDAP servers	`LDAProxyWindowsServices.exe`

Platform	Service or Daemon Name	Display Name	Description	File Name
Full Disk Encryption	DrAService	Trend Micro Full Disk Encryption	Provides Trend Micro endpoint security and full disk encryption.	`DrAService.exe`
Encryption Management for Microsoft BitLocker	FDE_MB	Trend Micro Full Disk Encryption, Encryption Management for Microsoft BitLocker	Provides data security for endpoints using Microsoft BitLocker.	`FDEforBitLocker.exe`
Encryption Management for Apple FileVault	Daemon: TMFDEMM Agent: Trend Micro Full Disk Encryption	Trend Micro Full Disk Encryption, Encryption Management for Apple FileVault	Provides endpoint security for endpoints using Apple FileVault.	
File Encryption	FileEncryption Service	Trend Micro File Encryption	Provides Trend Micro endpoint security and data protection for files, folders, and removable media devices.	`FEService.exe`

Appendix E

Glossary

The following table explains the terminology used throughout the Endpoint Encryption documentation.

TABLE E-1. Endpoint Encryption Terminology

TERM	DESCRIPTION
Agent	Software installed on an endpoint that communicates with a management server.
Authentication	The process of identifying a user.
ColorCode™	The authentication method requiring a color-sequence password.
Command Line Helper	A Trend Micro tool for creating encrypted values to secure credentials when creating Endpoint Encryption agent installation scripts.
Command Line Installer Helper	A Trend Micro tool for creating encrypted values to secure credentials when creating Endpoint Encryption agent installation scripts.
Control Manager	Trend Micro Control Manager is a central management console that manages Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels.

Term	Description
Domain authentication	The authentication method for single sign-on (SSO) using Active Directory.
DriveTrust™	Hardware-based encryption technology by Seagate™.
Encryption Management for Microsoft BitLocker	The Endpoint Encryption Full Disk Encryption agent for Microsoft Windows environments that simply need to enable Microsoft BitLocker on the hosting endpoint. Use the Encryption Management for Microsoft BitLocker agent to secure endpoints with Trend Micro full disk encryption protection in an existing Windows infrastructure. For more information, see *About Full Disk Encryption on page 6-3*.
Encryption Management for Apple FileVault	The Endpoint Encryption Full Disk Encryption agent for Mac OS environments that simply need to enable Apple FileVault on the hosting endpoint. Use the Encryption Management for Apple FileVault agent to secure endpoints with Trend Micro full disk encryption protection in an existing Mac OS infrastructure. For more information, see *About Full Disk Encryption on page 6-3*.
Endpoint Encryption Device	Any computer, laptop, or removal media (external drive, USB drive) managed by Endpoint Encryption.
Endpoint Encryption Service	The PolicyServer service that securely manages all Endpoint Encryption 5.0 Patch 3 agent communication. For more information, see *About PolicyServer on page 1-14*. For Endpoint Encryption 3.1.3 and below agent communication, see Legacy Web Service.
Enterprise	The Endpoint Encryption Enterprise is the unique identifier about the organization in the PolicyServer database configured when installing PolicyServer. One PolicyServer database may have multiple Enterprise configurations. However, Endpoint Encryption configurations using Control Manager may only have one Enterprise.

Term	Description
File Encryption	The Endpoint Encryption agent for file and folder encryption on local drives and removable media. Use File Encryption to protect files and folders located on virtually any device that appears as a drive within the host operating system. For more information, see *About File Encryption on page 6-4*.
FIPS	Federal Information Processing Standard. The computer security standard established by the United States federal government.
Fixed password	The authentication method for using a standard user password consisting of letters and/or numbers and/or special characters.
Full Disk Encryption	The Endpoint Encryption agent for hardware and software encryption with preboot authentication.
KeyArmor	The Endpoint Encryption password-protected, encrypted USB device. **Note** Endpoint Encryption 5.0 does not have KeyArmor devices. However, legacy KeyArmor devices are supported.
Legacy Web Service	The PolicyServer service that securely manages all Endpoint Encryption 3.1.3 and below agent communication. For details, see *About PolicyServer on page 1-14*. For Endpoint Encryption 5.0 Patch 3 communication, see Endpoint Encryption Service.
OCSP	Online Certificate Status Protocol. The protocol used for X. 509 digital certificates.

Term	Description
OfficeScan	OfficeScan protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks. An integrated solution, OfficeScan consists of an agent that resides at the endpoint and a server program that manages all agents.
OPAL	Trusted Computing Group's Security Subsystem Class for client devices.
Password	Any type of authentication data used in combination with a user name, such as fixed, PIN, and ColorCode.
PIN	The authentication method for using a Personal Identification Number, commonly used for ATM transactions.
PolicyServer	The central management server that deploys encryption and authentication policies to the Endpoint Encryption agents.
Remote Help	The authentication method for helping Endpoint Encryption users who forget their credentials or Endpoint Encryption devices that have not synchronized policies within a pre-determined amount of time.
Recovery Console	The Full Disk Encryption interface to recover Endpoint Encryption devices in the event of primary operating system failure, troubleshoot network issues, and manage users, policies, and logs.
Repair CD	The Full Disk Encryption bootable CD that can decrypt a drive before removing Full Disk Encryption in the event that the disk becomes corrupted.

Term	Description
RESTful	Representational State Transfer web API . The AES-GCM encrypted communications protocol used by Endpoint Encryption 5.0 agents. After a user authenticates, PolicyServer generates a token related to the specific policy configuration. Without authentication, the service denies all policy transactions. **Note** For information about AES-GCM, visit: http://tools.ietf.org/html/rfc5084#ref-GCM%3F
RSA SecurID	A mechanism for performing two-factor authentication for a user to a network resource.
SED	Secure Encrypted Device. A hard drive, or other device, which is encrypted.
Self Help	The authentication method for helping Endpoint Encryption users provide answers to security questions instead of contacting Technical Support for password assistance.
Smart card	The authentication method requiring a physical card in conjunction with a PIN or fixed password.
SOAP	Simple Object Access Protocol. The encrypted communications protocol used by all Endpoint Encryption 3.1.3 and older agents to communicate with PolicyServer. Under certain situations, SOAP may allow insecure policy transactions without user authentication. Legacy Web Service filters SOAP calls by requiring authentication and limiting the commands that SOAP accepts.

Index

Symbols

"Log on as batch job" policy, A-64

A

about
- account types, 1-21
- client-server architecture, 1-11
- Endpoint Encryption, 1-2
- Endpoint Encryption Service, 1-14, 4-2
- File Encryption, 6-4
- FIPS, 1-10
- Full Disk Encryption
  - Encryption Management for Apple FileVault, 6-3
  - Encryption Management for Microsoft BitLocker, 6-3
- Legacy Web Service, 1-14, 4-2
- Maintenance Agreement, 8-2
- OfficeScan, 3-8, 7-2
- PolicyServer, 1-14, 4-2

accounts
- types, 1-21

Active Directory, 1-11, 4-16, 6-5
- configuration, 4-17
- overview, 4-16

agents, 1-18, 6-2
- installation, 6-1
- scripted installations, 6-40
- services, 7-14
- supported platforms, 3-2

agent tree, 7-10
- about, 7-10
- specific tasks, 7-10

AHCI, 6-48

appendices, 1

ATA, 6-48

authentication, 1-2
- account types, 1-21

automatic deployment settings
- Scheduled Download, A-59

B

BIOS, 6-48

C

central management, 1-2

change management, B-7
- Active Directory, B-7

client-server architecture, 1-11

Command Line Helper, 6-42, 6-45
- for Encryption Management for Apple FileVault, 6-44
- for File Encryption, 6-44
- for Full Disk Encryption, 6-43

Command Line Installer Helper, 6-33, 6-40

community, 8-6

components
- downloading, A-38

configuring, A-56
- managed products, A-24
- Scheduled Download
  - automatic deployment settings, A-59
- Scheduled Download Exceptions, A-48
- Scheduled Download Settings, A-57
- user accounts, A-9

Control Manager, 1-18, 3-7, 5-2, A-1, A-6
- about, 1-18, 3-7, 5-2, A-1
- accounts, A-9

agent, A-7
antivirus and content security components, A-39, A-40
basic features, A-3
configuring accounts, A-9
features, A-3
mail server, A-6
managed product, A-15
MCP, A-7
report server, A-6
requirements, 2-7
SQL database, A-6
Trend Micro Management Infrastructure, A-7
web-based management console, A-7
web server, A-6
widget framework, A-8
Control Manager antivirus and content security components
Anti-spam rules, A-39
Engines, A-39
Pattern files/Cleanup templates, A-39
Control Manager integration, 1-11, 1-18, 5-2
creating
folders, A-35

D

DAAutoLogin, 6-45
database requirements, 2-2
data protection, 1-2
data views
understand, A-67
decryption, 6-59
deployment
change management, B-7
considerations, B-1, B-3
end users, B-2
File Encryption, 6-29
MMC only, 3-6
OfficeScan, 7-12, 7-13
options, 3-11
Phased roll-out, C-2
pilot program, C-1
planning, B-2
policies, B-6
project team, C-2
scaling, 3-17
security infrastructure, B-4
supported platforms
File Encryption, 3-2
Full Disk Encryption, 3-2
KeyArmor, 3-2
PolicyServer, 3-2
three layer network topology, 3-15
with Control Manager, 3-10
with OfficeScan, 3-10
deployment plans, A-60
deployment requirements, 3-2
device, 1-2
devices, 1-20
Directory Management options, A-34
Directory Manager, A-33
disk controller, 6-48
domain authentication, 6-5
Download Center, 8-5
download components
manually, A-41
downloading and deploying components, A-38

E

editing managed servers, 5-11
encryption, 1-10
features, 1-2

file and folder, 6-4
FIPS, 1-10
full disk, 6-3
hardware-based, 1-10, 6-3
installation scripts, 6-38
project planning, 3-2
software-based, 1-10, 6-3
Encryption Management for Apple FileVault
change, 6-57
installation, 6-8, 6-25
preparing endpoint, 6-8
supported operating systems, 2-12
system requirements, 2-12
upgrades, 6-50
Encryption Management for Microsoft BitLocker
agent service, 7-14
change, 6-58
installation, 6-16
preparing hard disk, 6-9
supported operating systems, 2-11
system requirements, 2-11
Endpoint Encryption
about, 1-2
pilot checklist, C-3
enhancements, 1-3

F

features, A-3
File Encryption
agent service, 7-14
change, 6-59
change PolicyServer, 6-59
deployment, 6-29
file encryption, 6-4
installation, 6-28, 6-31, 6-32
policies, 6-30
system requirements, 2-13
uninstalling, 6-63
upgrades, 6-49
FIPS
about, 1-10
FIPS 140-2, 1-10
security levels, 1-10
folders
creating, A-35
renaming, A-36
Full Disk Encryption
agent service, 7-14
change, 6-56
change PolicyServer, 6-52
changing enterprises, 6-54
device encryption, 6-11
hard disk preparation, 6-9
installation, 6-11, 6-14
automating, 6-6
scripts, 6-6
policies, 6-11
preparing endpoint, 6-7
preparing hard disk, 6-9
Recovery Console, 6-53
Windows, 6-53
replacing another product, 6-51
supported operating systems, 2-9
system requirements, 2-9
uninstalling, 6-59
upgrades, 6-47

G

GPO, 6-40

H

hard drives

installation preparation, 6-9
hardware based encryption, 2-9, 2-11, 2-12

I

installation, 4-3, 6-4
checklist, 6-11, B-7
Encryption Management for Microsoft BitLocker, 6-16
File Encryption, 6-28
Full Disk Encryption, 6-6
managed endpoint, 6-14
hard drive preparation, 6-9
managed requirements, 6-5
pilot checklist, C-3
plug-in program, 7-5
PolicyServer, 4-1
PolicyServer databases, 4-3
PolicyServer MMC, 4-8
PolicyServer web services, 4-3
security infrastructure checklist, B-4
Intel Matrix Manager, 6-49
Intel Rapid Recovery Technology, 6-49

K

key features, 1-2

L

LANDesk, 6-40
logs, A-65
querying, A-67

M

Maintenance Agreement
about, 8-2
expiration, 8-2
renewal, 8-2
managed endpoint
requirements, 6-5
managed products
configuring, A-24
issue tasks, A-25
recovering, A-30
renaming, A-36
searching for, A-31
viewing logs, A-26
managed server list
editing servers, 5-11
manually download components, A-41
MCP, A-7
Microsoft .NET, 3-2
Microsoft SMS, 6-33
migration
control manager, 4-31
Control Manager, 5-3
migrations
agents, 6-56
MobileArmor-branded Full Disk Encryption Agent SP7, 6-48
MobileArmor cryptographic, 6-42

O

OfficeScan
Control Manager
supported versions, 2-7
supported versions, 2-7
system requirements, 2-7
uninstalling agents, 6-64, 7-19
online
community, 8-6
OPAL, 2-9, 2-11

P

passwords, 1-2
pilot program, C-1
Plug-in Manager, 7-4

plug-in program
installation, 7-5
policies, 1-2
allow user recovery, 6-53
security planning, B-6
synchronization, 6-3
policy management
editing managed servers, 5-11
PolicyServer
AD synchronization, 4-1, 4-16
client web service, 1-11
installation
database, 4-3
PolicyServer MMC, 4-8
web services, 4-3
installation process, 4-1
installation requirements, 4-1
requirements, 2-2
accounts, 2-5
files, 2-5
SQL, 2-4
scaling, 3-17
setup files, 2-5
software requirements, 2-2
SQL accounts, 2-5
SQL requirements, 2-4
system requirements
hardware, 2-4
uninstallation
web services, 4-32
upgrades
database, 4-27
web services, 4-27
upgrading, 3-22
upgrading the PolicyServer MMC, 4-30
Windows Server 2008, 2-3
Windows Server 2008 R2, 2-3
PolicyServer MMC, 1-11, 1-17
add top group, 4-11
authentication, 4-9
first time use, 4-9
groups
adding users, 4-13
allow install, 4-15
users
add enterprise user, 4-13
add to group, 4-13
allow to install, 4-15
pre-installation checklist, 6-11, B-7
pre-installation considerations, 6-4
product components, 1-11
product definitions, E-1
Product Directory
deploying components, A-22
proxy options, 3-15

Q

query logs, A-67

R

recovering
managed products, A-30
recovery console
logon, 6-53
Recovery Console
access, 6-53
Windows, 6-53
changing enterprises, 6-54
changing PolicyServer, 6-56
log on, 6-53
registering
to Control Manager, A-8
registration

key, 8-2
profile, 8-2
URL, 8-2
renaming
folders, A-36
managed products, A-36
reporting, 1-2
reports
one-time reports, A-81
scheduled reports, A-86
templates, A-69
report templates, A-69

S

SATA, 6-49
scaling
server and database requirements, 3-17
scaling requirements, 3-2
SCCM, 6-40
schedule bar, A-12
Scheduled Download
configuring
automatic deployment settings, A-59
Scheduled Download Exceptions
configuring, A-48
Scheduled Download Frequency
configuring, A-56
Scheduled Downloads, A-49
Scheduled Download Schedule
configuring, A-56
Scheduled Download Schedule and Frequency, A-56
Scheduled Download Settings
configuring settings, A-57
scripted installations, 6-33
scripts
arguments, 6-38
encryption, 6-38
Encryption Management for Apple FileVault, 6-44
File Encryption, 6-38, 6-44
Full Disk Encryption, 6-38, 6-43
requirements, 6-34
Seagate DriveTrust drives, 2-9, 2-11
searching
managed products, A-31
security
anti-malware/antivirus protection, 1-2
security infrastructure, B-4
security infrastructure checklist, B-4
single sign-on, 6-5
software, 2-2
support
knowledge base, 8-6
resolve issues faster, 8-8
TrendLabs, 8-9
supported agents, 3-25, 4-25
supported versions, 2-7
system requirements, 2-6
agents, 2-9
Control Manager, 2-7
Encryption Management for Apple FileVault, 2-12
Encryption Management for Microsoft BitLocker, 2-11
File Encryption, 2-13
Full Disk Encryption, 2-9
OfficeScan, 2-7
PolicyServer, 2-2, 2-4
PolicyServer MMC, 2-6

T

terminology, E-1

tools
Command Line Helper, 6-42
Command Line Installer Helper, 6-40
DAAutoLogin, 6-42
Recovery Console, 6-54, 6-59
top group, 4-11
TrendLabs, 8-9
Trend Micro Control Manager
managed product user access, A-11
registering to, A-8
trial license, 4-3, 4-8, 4-27, 8-3
Trivoli, 6-40

U

UEFI, 6-7
understand
data views, A-67
deployment plans, A-60
log queries, A-67
logs, A-65
understanding
Endpoint Encryption, 1-1
uninstall
client applications, 6-59
File Encryption, 6-63
Full Disk Encryption, 6-59
manual, 6-59
uninstallation, 4-31
database, 4-32
uninstalling
agents, 6-64, 7-19
upgrade
agents, 3-21, 4-23, 6-46
PolicyServer, 3-21, 4-23, 6-46
PolicyServer web services, 4-27
upgrades
agents, 4-23
File Encryption, 6-49
Full Disk Encryption, 6-47
paths, 3-23, 4-23
PolicyServer, 3-22, 4-23
PolicyServer databases, 4-27
PolicyServer MMC, 4-30
summary, 3-26
URLs
registration, 8-2
users, 1-21
adding new user to group, 4-13
allow install, 4-15

V

viewing
managed products logs, A-26
VMware Virtual Infrastructure, 2-4

W

Windows 8, 2-9, 6-7
upgrading to, 6-46
Windows Server 2008 considerations, 2-2

TREND MICRO INCORPORATED
10101 North De Anza Blvd. Cupertino, CA., 95014, USA
Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: APEM56168/130917