TREND MICRO™

5.0 TREND MICRO™ Endpoint Encryption

Patch 4

Installation Guide

Comprehensive Endpoint Encryption for Data at Rest

Endpoint Security

Document Part No.: APEM57328/160222

Release Date: March 2016

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

Chapter 4: PolicyServer Installation

Chapter 5: Control Manager Integration

Chapter 6: Endpoint Encryption Agent Deployment

Chapter 7: Upgrade and Migration

Chapter 8: Uninstallation

Index

Chapter 1

Home

Welcome to the Trend Micro™ Endpoint Encryption™ Installation Guide. This guide is intended to assist security administrators and IT professionals to set up PolicyServer, install Endpoint Encryption™ agents, and integrate PolicyServer with Trend Micro Control Manager. This guide explains system requirements, deployment considerations, product installation, upgrade scenarios, and product uninstallation.

Deployment Overview

Procedure

1. Decide how to deploy Endpoint Encryption into your environment and prepare for Endpoint Encryption installation.

   See *Deployment Planning on page 2-1*.

2. Review all system requirements for compatible product versions.

   See *System Requirements on page 3-1*.

3. Install PolicyServer and PolicyServer MMC.

   See *Installing PolicyServer on page 4-4*.

4. Optionally, set up Control Manager for Endpoint Encryption management.

   See the supporting documentation at:

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

   a. Install and configure Control Manager.

   b. Add PolicyServer to Control Manager.

      See *Adding PolicyServer as a Managed Product to Control Manager on page 5-3*

5. Prepare endpoints for deployment.

   See *Agent Installation Prerequisites on page 6-3*.

6. Install Endpoint Encryption agents.

   - If you plan to install agents manually or remotely, follow the steps provided in *Endpoint Encryption Agent Deployment on page 6-1*.
   - If you plan to install Full Disk Encryption agents using OfficeScan, see the *OfficeScan Plug-in Online Help*:

     http://docs.trendmicro.com/en-us/enterprise/endpoint-encryption-50-patch-4-officescan-plug-in-online-help/tmee_oscepls_intro.aspx

7. Manage your agents using your prefered management console.

   - If you are using Control Manager for management, see the *Endpoint Encryption Administrator's Guide*:

     http://docs.trendmicro.com/en-us/enterprise/endpoint-encryption-50-patch-4-administrator-guide/home_cmcolh.aspx

   - If you are using PolicyServer MMC for management, see the *Endpoint Encryption PolicyServer MMC Guide*:

     http://docs.trendmicro.com/en-us/enterprise/endpoint-encryption-50-patch-4-policyserver-mmc-guide/home_psolh.aspx

Chapter 2

Deployment Planning

This chapter describes preparation and preinstallation information for Trend Micro™ Endpoint Encryption™ software installation.

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.

Topics include:

Deployment Considerations

This section explains the high-level considerations for installing the main Endpoint Encryption components.

COMPONENT	DETAILS
PolicyServer	PolicyServer is the main server software that manages Endpoint Encryption agents. This software includes a front-end server program and a backend SQL Server database. When planning your PolicyServer installation, consider how many devices will be managed by PolicyServer and whether your environment requires server or database redundency. After installing PolicyServer, you can configure ActiveDirectory domain authentication and proxy communication.
Endpoint Encryption agents	In the client-server model, “agents” are the client software installed on computers and devices that communicate with PolicyServer. For information about the available agents, see *Endpoint Encryption Agent Deployment on page 6-1*. When planning agent deployment, consider whether you will install agents on individual endpoints or whether you will install them remotely. If your environment is protected by Trend Micro™ OfficeScan™, you can install Full Disk Encryption agents using OfficeScan through the Endpoint Encryption Deployment Tool Plug-in.

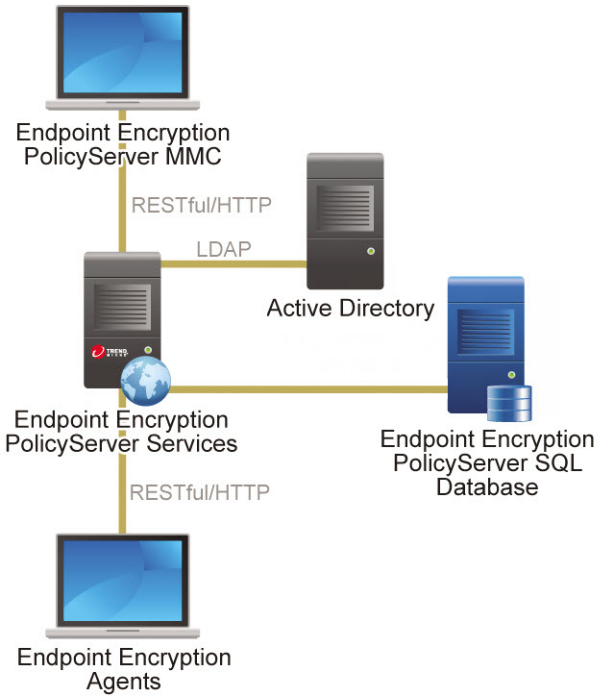
COMPONENT	DETAILS
Management console	The management console determines the encryption, authentication, and configuration policies for the Endpoint Encryption agents. The main decision you will need to make when planning your installation is what primary management console you will use. You can manage PolicyServer on either of the following consoles: • Control Manager: This is the central management console for Trend Micro products. Trend Micro recommends using Control Manager to manage Endpoint Encryption, but using Control Manager is optional. • PolicyServer MMC: This console performs advanced operations for Endpoint Encryption. If preferred, PolicyServer MMC can perform user, device, and policy management. **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.

Sample Deployments

Endpoint Encryption has the flexibility to be deployed in different network environments. This section shows several example implementations of Endpoint Encryption into different network security infrastructures.

Simple Deployment

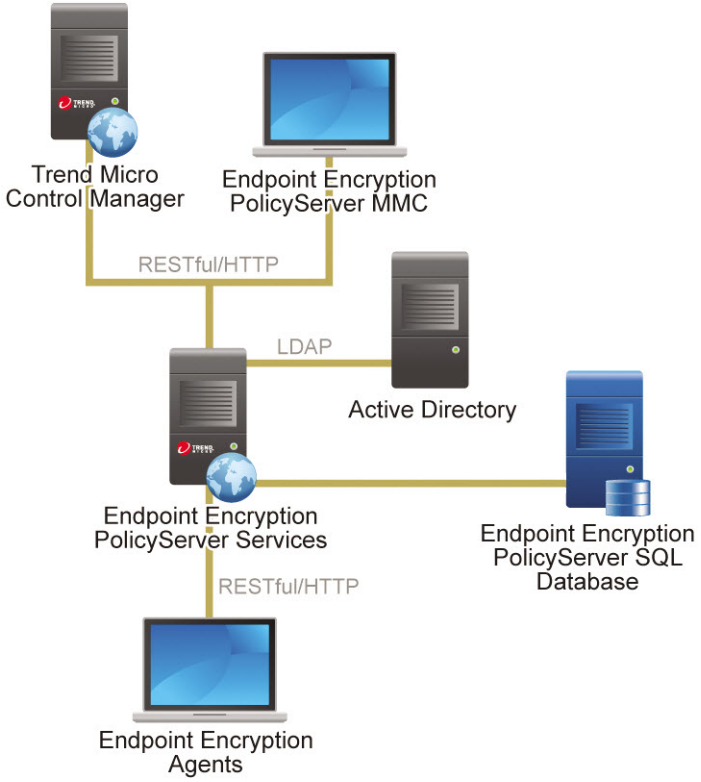
The following illustration shows how to deploy Endpoint Encryption using only PolicyServer MMC to manage PolicyServer.



Control Manager Deployment

The following illustration shows how to deploy Endpoint Encryption 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*.



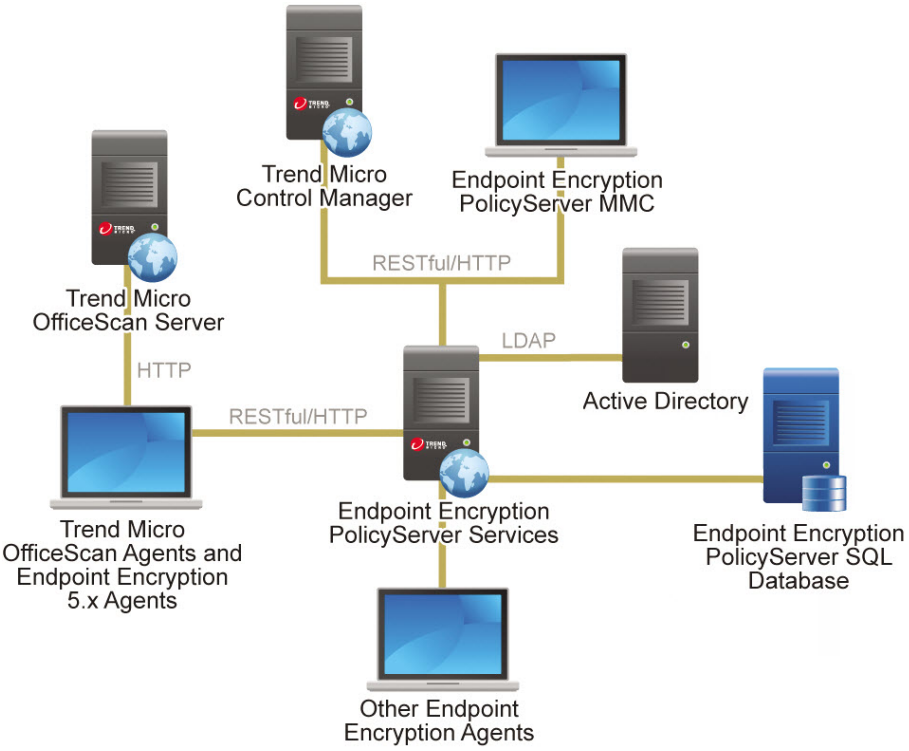
In environments that use Control Manager, changes to PolicyServer policies are always controlled by Control Manager. Any changes made using PolicyServer MMC are overwritten the next time that Control Manager synchronizes policies to the PolicyServer database.

OfficeScan Deployment

The following illustration shows how to deploy Endpoint Encryption on OfficeScan managed endpoints. In this example, Control Manager is the primary management

console. However, administrators can use either Control Manager or PolicyServer MMC to manage PolicyServer in OfficeScan deployments.

For more information about OfficeScan integration, see the *OfficeScan Plug-in Online Help*.



Large Enterprise Deployment

The following illustration shows the network environment of a large enterprise with 40,000 devices. The multiple traffic routes to the firewalls show redundant network

paths to account for high availability. For more information about scaling requirements, see *Hardware and Scaling Requirements on page 3-2*.

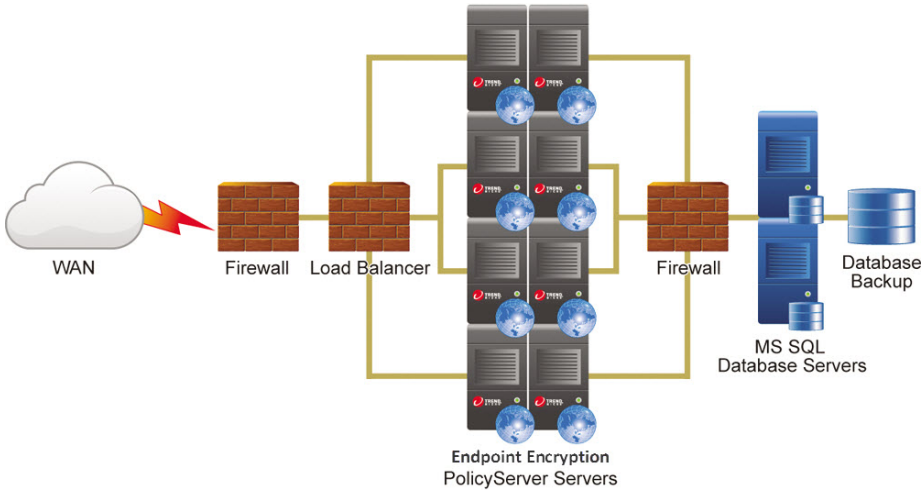
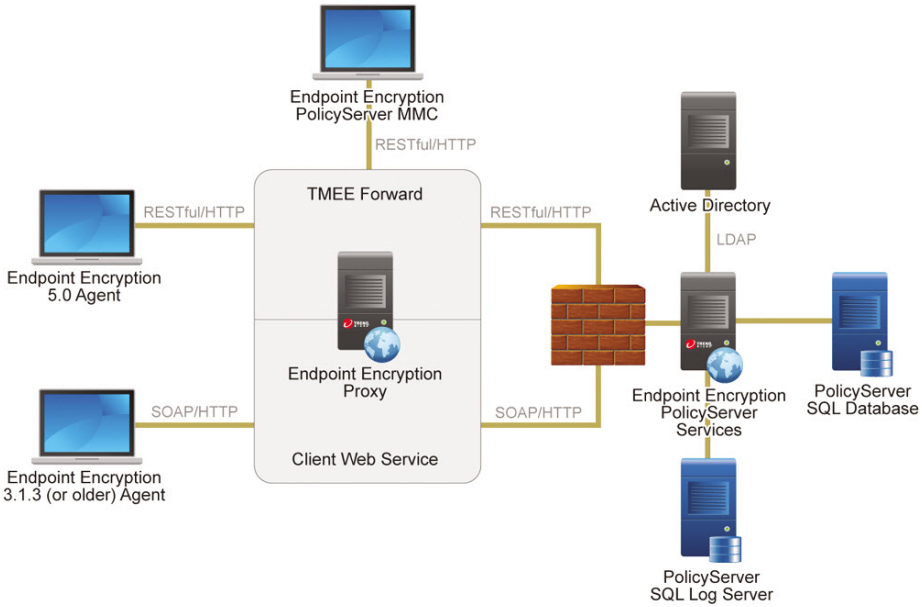


FIGURE 2-1. PolicyServer Scaled to Support 40,000 Users

Deployment Including Legacy Agents

The following illustration shows a complex network environment using both Endpoint Encryption 5.0 and Endpoint Encryption legacy (3.1.3) agents. In this example, an endpoint between PolicyServer MMC and the Endpoint Encryption agents directs and filters traffic using the Endpoint Encryption proxy service. The Endpoint EncryptionProxy includes the TMEE Forward service to communicate with 5.0 agents, and the Client Web Service to communicate with legacy agents.

For more information, see *Traffic Forwarding Services for Legacy Agents on page 4-16*.



Administration Considerations

This section includes a list of tasks and changes that security and IT administrators should consider when deploying Endpoint Encryption.

Network Infrastructure Checklist

This questionnaire assists IT administrators in defining the project team, documenting the operating environment, assessing architecture requirements, facilitating review of desktop hardware and software profiles, and defining security concerns or support processes.

Category	Questions
End users	1. What is the total number of users to be deployed? 2. Of that number, how many are: • Administrators (for either the Enterprise or Group) • Authenticator (Help Desk Personnel) • End users
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: • Antivirus • Security applications that block software installation • Previous encryption products 5. Do the endpoints use BIOS or UEFI?

CATEGORY	QUESTIONS

Enterprise networks and databases	• How many PolicyServer instances are required to support the user base?
	  • Estimate the maximum number of users in the future. For example, think about the company's potential growth within three years.
	  • If domain authentication is used, one PolicyServer is required for each Active Directory domain.
	• Is load balancing on the servers required?
	  • Load-balancing is recommended for installations that require redundancy and high-availability for PolicyServers.
	  • Clustering can be used to provide redundancy and high-availability for the database servers.
	• What are the database size estimates?
	  • Estimate the maximum number of users in the future. For example, think about the company's potential growth within three years.
	  • Approximate space required is 1 GB per year for every 1,000 end users.

Internet connectivity	1. Will agents be required to communicate with PolicyServer over the Internet?
	  • Check with internal network/security team to understand requirements to make a web server available on the Internet.
	2. If agents are required to communicate over the Internet, which of the following functions do you need to set up:
	  • 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. The following table provides specific questions to ask about your existing and potential security infrastructure to better understand how deploying Endpoint Encryption may affect the organization.

CATEGORY	QUESTIONS
End users	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?

CATEGORY	QUESTIONS
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?
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 PolicyServer 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 process updated to include Endpoint Encryption? Consider the following: • Backing up, formatting, or restoring devices • Locking or killing devices • Disabling accounts in PolicyServer
Removeable media	1. What USB and other removeable media devices are allowed in your network? 2. Will removeable media devices be accessible at all hours of the day, or will you have set times where removeable device authentication is not allowed? 3. Where can users access removeable media devices: on-network, off-network, over VPN, at home?
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?

End User Communication

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 following is a high-level communication strategy to promote adoption of Endpoint Encryption and ease the transition into your enterprise's new security practices.

TIME	COMMUNICATION TASKS
One month before rollout	• Have the executive sponsor outline why new encryption is being introduced and how complying with the new processes benefits the end user as well as the company. • Provide a roll-out schedule to the users, including what to expect from the new product and how the users can get technical support.
One week before rollout	• Reiterate what changes are coming and what to expect on the day new authentication procedures are required on their endpoints. • Include screen captures and detailed instructions on user name or password conventions, and other internal support services.
One day before rollout	• Reinforce the timing of the roll-out schedule and what to expect. • Distribute cheat-sheets, installation information, and any on-site contacts who will be available to assist users the next day.
The day of rollout	• Announce system maintenance start and expected length of down time, if any.
After rollout	• Reiterate contact information for help desk personnel who can assist users. • Provide tools for troubleshooting assistance.

Network Maintenance

PolicyServer and related databases are mission-critical services. Trend Micro recommends the following for optimal maintenance of your Endpoint Encryption product and related services:

- Actively monitor CPU usage and establish a threshold for when the PolicyServer Windows Service and Trend Micro Endpoint Encryption Service should be restarted.
- Restart the service on a regular schedule that fits with the organization's established maintenance windows (daily, weekly, monthly).
- Restart the PolicyServer Windows service whenever maintenance is performed on the Active Directory environment, the server, database, or related communications.
- Back up PolicyServer databases when you back up similar enterprise-critical databases.
- Back up primary and log databases regularly off site for redundancy.

WARNING!

Any changes to the Active Directory or database environments may affect connectivity with PolicyServer.

Chapter 3

System Requirements

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

Topics include:

PolicyServer System Requirements

Hardware and Scaling Requirements

The following shows deployment and scaling requirements in several different-sized environments. In smaller network environments, PolicyServer SQL databases can be installed on the same server. For PolicyServer deployments in environments greater than 1500 devices, Trend Micro recommends having at least two dedicated servers:

1. A dedicated server for the PolicyServer services, also known as the "front-end server"
2. A dedicated server for the database, or add the database to an existing SQL cluster

With larger environments, Trend Micro recommends adding additional servers to avoid having single points of failure. The following table displays two sets of requirements for the PolicyServer SQL database: one set for the basic requirements at that scale, and one set for an environment with increased redundancy.

Devices	PolicyServer Front-end Requirements	PolicyServer SQL Database Requirements	PolicyServer SQL Database with Zero Single Points of Failure (Recommended)
1,500	• One front-end and SQL database multi-role server with an Intel Xeon quad-core 2.0 GHz processor or equivalent • 8 GB RAM • 120 GB hard drive	Installed on PolicyServer front-end server	Not recommended for deployments at this scale

Devices	PolicyServer Front-end Requirements	PolicyServer SQL Database Requirements	PolicyServer SQL Database with Zero Single Points of Failure (Recommended)
3,000	• One front-end server with two Intel Xeon quad-core 2.0 GHz processors or equivalent • 4 GB RAM • 40 GB hard drive	• One SQL database server with an Intel Xeon quad-core 2.0 GHz processor or equivalent • 8 GB RAM • 100 GB hard drive	Not recommended for deployments at this scale
10,000	• Two front-end servers each with an Intel Xeon quad-core 2.0 GHz processor or equivalent • 4 GB RAM • 40 GB hard drive	• One SQL database server with an Intel Xeon quad-core 2.0 GHz processor or equivalent • 8 GB RAM • 120 GB hard drive	• One SQL server cluster of two nodes, each with an Intel Xeon quad-core 2.0 GHz processor or equivalent • 8 GB RAM • 60 GB RAID 5 hard drive • 150 GB shared SAN RAID 5 hard drive

DEVICES	POLICYSERVER FRONT-END REQUIREMENTS	POLICYSERVER SQL DATABASE REQUIREMENTS	POLICYSERVER SQL DATABASE WITH ZERO SINGLE POINTS OF FAILURE (RECOMMENDED)
20,000	• Four front-end servers each with two Intel Xeon quad-core 2.0 GHz processors or equivalent • 4 GB RAM • 40 GB hard drive	• One SQL database server with an Intel Xeon quad-core 2.0 GHz processor or equivalent • 16 GB RAM • 160 GB RAID 5 hard drive	• One SQL server cluster of two nodes, each with an Intel Xeon quad-core 2.0 GHz processor or equivalent • 8 GB RAM • 60 GB RAID 5 hard drive • 180 GB shared SAN RAID 5 hard drive
40,000	• Eight front-end servers each with two Intel Xeon quad-core 2.0 GHz processors or equivalent • 4 GB RAM • 40 GB hard drive	• Two SQL database cluster servers each with an Intel Xeon quad-core 2.0 GHz processor or equivalent • 16 GB RAM • 320 GB shared SAN RAID 5 hard drive	• Four SQL database cluster servers each with an Intel Xeon quad-core 2.0 GHz processor or equivalent • 16 GB RAM • 60 GB RAID 5 hard drive • 350 GB shared SAN RAID 5 hard drive

Note

Virtual hardware is supported under VMware Virtual Infrastructure.

Microsoft or VMware on virtual hardware does not support Microsoft Cluster Service.

Software Requirements

SPECIFICATION	REQUIREMENTS
Operating system	• Windows Server 2008 / 2008 R2 (64-bit) • Windows Server 2012 / 2012 R2 (64-bit)
Database server	• Microsoft SQL Server 2005 SP3 / 2008 / 2008 R2 / 2012 • Microsoft SQL Server Express 2005 SP3 / 2008 / 2012 • Mixed Mode Authentication (SA password) installed • Reporting services installed **Note** For Windows Server 2008 R2, you must install SQL Server 2008 SP1.

Application server	PolicyServer 5.0 Patch 4 requires Microsoft Internet Information Services (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

SPECIFICATION	REQUIREMENTS
	For Windows Server 2008 and 2008 R2 you must install the “Application server” role and the “Web server” role. Additionally, you must add SMTP and Microsoft IIS Support features. 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)

Installation Files

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. To upgrade to the full product version, register your product with your Activation Code in Control Manager or PolicyServer MMC.

Required Accounts

Account	Function	Description
SQL SA	PolicyServer Installer	Account is used only to create the PolicyServer databases
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

PolicyServer MMC System Requirements

Note

PolicyServer MMC can be installed on the PolicyServer front-end server or on a different endpoint that has network connectivity with PolicyServer.

Specification	Requirements
Processor	Intel Core 2 Duo 2.0 GHz processor or equivalent
RAM	512 MB
Disk space	100 MB
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

Full Disk Encryption System Requirements

SPECIFICATION	REQUIREMENTS
Processor	Intel Core 2 Duo 2.0 GHz processor or equivalent
RAM	1 GB
Disk space	• 30 GB • 20% free disk space • 256 MB contiguous free space
Network connectivity	Communication with PolicyServer required for managed agents
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)
Firmware interface	• BIOS: all supported operating systems • For devices with UEFI, set the boot priority to **Legacy First**.
Other software	• Microsoft .NET Framework 3.5 (Windows 7 and later operating systems) • Microsoft .NET Framework 2.0 SP1 (Windows XP) • Microsoft Windows Installer (Windows XP)

Specification	Requirements
Hard disk	Full Disk Encryption uses software-based encryption for all standard drives (drives without self-encryption). Full Disk Encryption uses hardware-based encryption for the following self-encrypting drives (SEDs): • Seagate DriveTrust drives • Seagate OPAL and OPAL 2 drives • SanDisk self-encrypting solid-state drives Full Disk Encryption has the following limitations: • Full Disk Encryption does not support endpoints with multiple hard disks. • Full Disk Encryption does not support RAID and SCSI drives. • Full Disk Encryption does not support eDrive drives for Windows 8 or later environments. • Full Disk Encryption does not support GUID Partition Table (GPT) drives.
Hard disk controllers	• Software encryption: ATA, AHCI, or IRRT hard disk controller • Hardware encryption: AHCI hard disk controller

File Encryption System Requirements

The following table explains the File Encryption system requirements.

Specification	Requirements
Processor	Intel Core 2 Duo 2.0 GHz processor or equivalent
RAM	1 GB

SPECIFICATION	REQUIREMENTS
Disk space	• 30 GB • 20% free disk space
Network connectivity	Communication with PolicyServer required for managed agents
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	• Microsoft .NET Framework 3.5 (Windows 8 and later operating systems) • Microsoft .NET Framework 2.0 SP1 or later (Windows XP) • Microsoft Windows Installer 3.1

Encryption Management for Microsoft BitLocker System Requirements

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

SPECIFICATION	REQUIREMENTS
Processor	Intel Core 2 Duo 2.0 GHz processor or equivalent

SPECIFICATION	REQUIREMENTS
RAM	Requirements are the based on Windows system requirements: • 64-bit systems: 2 GB • 32-bit systems: 1 GB
Disk space	• 30 GB • 20% free disk space
Hard disk	• Standard drives supported by Windows
Network connectivity	Connectivity with PolicyServer
Operating system	• Windows™ Embedded POSReady 7 (32-bit/64-bit) • Windows™ 10 Enterprise and Professional editions (32-bit/64-bit) • Windows™ 8.1 Enterprise and Professional editions (32-bit/64-bit) • Windows™ 8 Enterprise and Professional editions (32-bit/64-bit) • Windows™ 7 Enterprise and Professional editions (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

Encryption Management for Apple FileVault System Requirements

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

SPECIFICATION	REQUIREMENT
Processor	Intel Core 2 Duo 2.0 GHz processor or equivalent
Memory	• 512 MB minimum • 1 GB recommended
Disk space	• 400 MB minimum
Network connectivity	• Connectivity with PolicyServer
Operating system	• OS X™ “El Capitan” • OS X™ “Yosemite” • OS X™ “Mavericks” • OS X™ “Mountain Lion”
Other software	• Mono runtime environment (MRE) 2.1 • Apple FileVault is disabled
Hardware considerations	• Mac OS local accounts or mobile accounts are able to initiate encryption on Mac OS X Mountain Lion or later. 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 6-29*. • Encryption Management for Apple FileVault supports Apple Fusion Drives on Mac OS X Mountain Lion or later (starting with Mac OS build 10.8.2).

Chapter 4

PolicyServer Installation

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.

This chapter how to install and configure PolicyServer for the first time, how to set up Active Directory.

Note

For system requirements, see *PolicyServer System Requirements on page 3-2*.

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 during PolicyServer configuration. One PolicyServer database may have one Enterprise configuration.

COMPONENT	DESCRIPTION
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 Proxy	The Endpoint Encryption Proxy acts as an intermediary between agents and PolicyServer to manage requests and communication over your network. This service can distinguish requests to new agents (5.0 and later) and legacy agents (3.1.3 and earlier) through the Traffic Forward Service and Client Web Service respectively. To secure PolicyServer behind the network firewall, deploy the Endpoint Encryption Proxy to an endpoint residing in the network DMZ.
Endpoint Encryption Service	All Endpoint Encryption 5.0 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.
Legacy Web Service	All Endpoint Encryption 3.1.3 and earlier 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. This service is optional, and can be installed on the same endpoint as the Endpoint Encryption Service using the Endpoint Encryption proxy installer.

Topics include:

- *Traffic Forwarding Services for Legacy Agents on page 4-16*

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)

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 *Traffic Forwarding Services for Legacy Agents on page 4-16*.

Procedure

1. Verify that all system requirements are met.

   See *PolicyServer System Requirements on page 3-2*.

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. At the **Product Activation** screen, select your licensing method:

   - Click **Register Online** to register your product and receive an Activation Code.
   - Select **Use a full license** if you have an Activation Code to specify your code and activate 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.

6. At the **Create Enterprise Name and Administrator Logon** screen, specify the credentials for your main Enterprise administrator account and then click **Continue**.

OPTION	DESCRIPTION
Enterprise Name	The name of the Enterprise. This will be required for user and device authentication.
Administrator	The first Enterprise Administrator account user name.
Password	The first Enterprise Administrator account password.
Confirm Password	Confirm the first Enterprise Administrator account password.

Enterprise administrator accounts can manage all device, user, and policy settings from PolicyServer MMC and Control Manager. You can create more Enterprise administrator accounts at a later time. If you are upgrading or reinstalling PolicyServer, the Enterprise administrator account that you specified previously appears automatically.

7. At the **Windows Service Logon** screen, click **Continue**.

8. At the **Database Administrator Logon** screen, choose your database connection method:

- Select **Microsoft SQL Express** to create a new database instance.

> **Note**
>
> Use Microsoft SQL Express only for networks of fewer than 1500 endpoints, or for evaluation purposes. Microsoft SQL Express is only available in environments that do not have SQL Server configured.

- Select **SQL Server** to specify an existing Microsoft SQL Server instance.

  If you select **SQL Server**, specify the following information:

Field	Description
SQL Server	The SQL Server host name or IP address. **Note** For environments with multiple SQL Server instances, append the SQL instance to the end of the database host name 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.

9. 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.

10. 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 4 agents use to communicate with PolicyServer (default: 8080).

OPTION	DESCRIPTION
	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 encrypted 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.

11. Click **Continue**.
12. 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**.
13. 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.
14. When prompted, click **OK**.
15. Click **Finished**.
16. Click **Exit** to close the PolicyServer installer.
17. Add the initial Endpoint Encryption users and groups.

    See *Configuring PolicyServer on page 4-9*.

Installing PolicyServer MMC

If you did not install PolicyServer MMC during PolicyServer installation, follow this procedure to install PolicyServer MMC. PolicyServer MMC can be installed on a separate endpoint from PolicyServer.

Note

Trend Micro recommends installing the same version of PolicyServer MMC as PolicyServer. Legacy versions of PolicyServer MMC (version 3.1.3 or earlier) are unable to manage PolicyServer 5.0 Patch 4.

Procedure

1. Run `PolicyServerMMCSnapinSetup.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**.

   Depending on your processor, the default installation path is: `C:\Program Files\Trend Micro\PolicyServer MMC\` or `C:\Program Files (x86)\Trend Micro\PolicyServer MMC\`

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

   After the installation completes, the PolicyServer MMC installs to the specified location. A new PolicyServer MMC shortcut appears on the desktop:

FIGURE 4-1. PolicyServer PolicyServer MMC shortcut

6. Click **Close** to finish.
7. Double-click the PolicyServer MMC shortcut on the desktop.
8. Once PolicyServer MMC opens, authenticate using the Enterprise and Enterprise Administrator account created when the PolicyServer databases and services were installed.

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.

Configuring PolicyServer

The following are the main tasks required for initial PolicyServer configuration. Use the Enterprise and Enterprise administrator account that were configured during PolicyServer installation.

Procedure

1. Install PolicyServer and PolicyServer MMC.

   See *Installing PolicyServer on page 4-4*.

   If you intend to install PolicyServer MMC separate from PolicyServer, 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 Agents in a Group on page 4-15*.

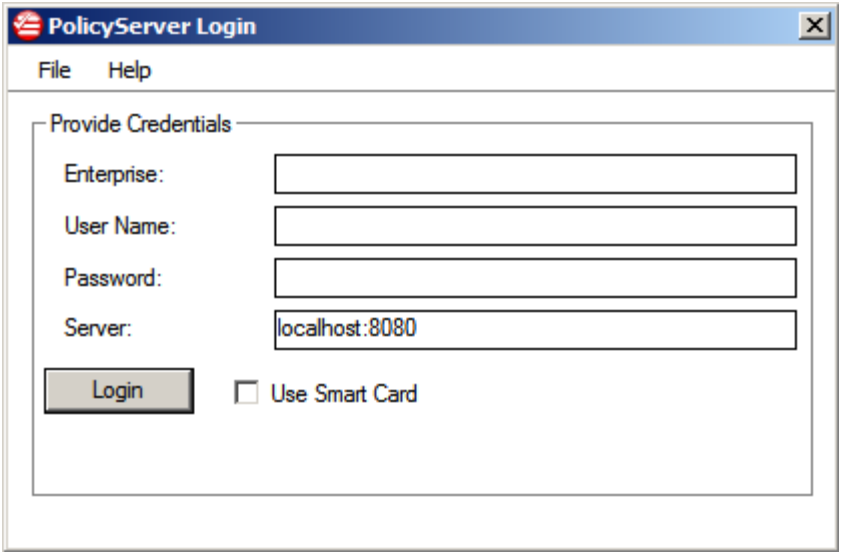
Logging on to PolicyServer MMC

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 `PolicyServerMMC.msc`.

   The PolicyServer MMC authentication screen appears.



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.
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**.

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.

PolicyServer requires a Top Group for user

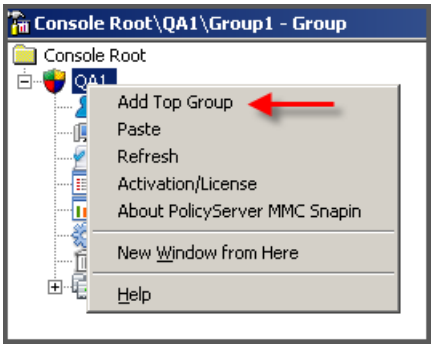
Note

Enterprise administrators and authenticators may not be added to groups because their permissions supercede all groups. If you add an administrator or authenticator to a group, that account will be a group administrator or authenticator.

Procedure

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

The **Add New Group** screen appears.

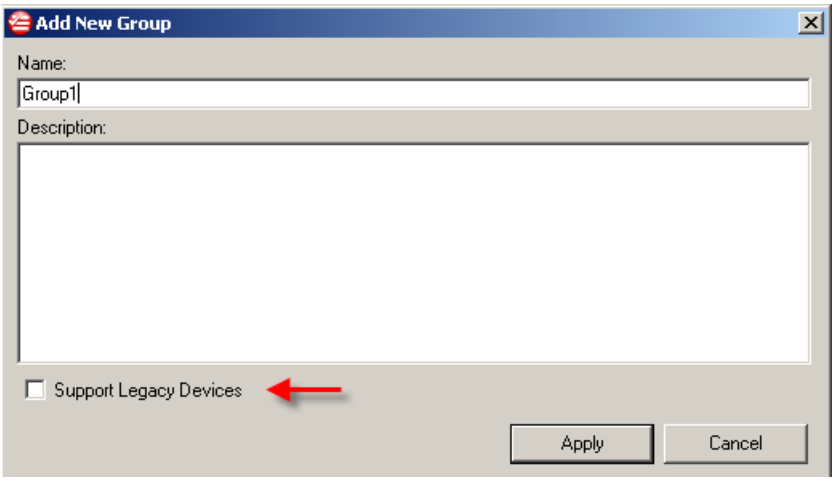


2. Specify the name and description for the group.
3. If using Endpoint Encryption devices that do not support Unicode, select **Support Legacy Devices**.

   Endpoint Encryption 5.0 and later devices support Unicode. Do not select this option if all devices are Endpoint Encryption 5.0 and later.

Note

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



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

Add one or more users to your group during initial configuration if you intend to have multiple users perform agent installation.

Note

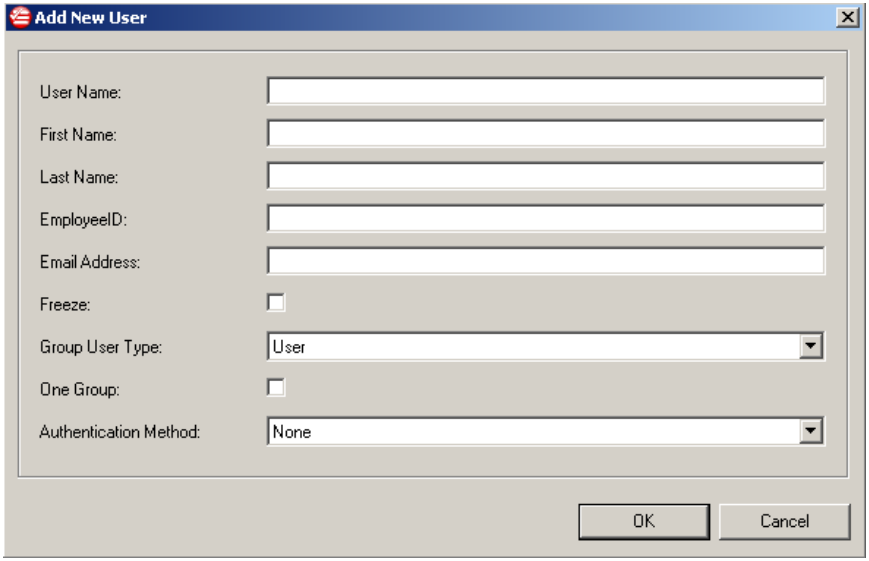
Adding a user to the Enterprise does not assign the user to any groups.

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. On the right pane, right-click the whitespace and select **Add New User**.

The **Add New User** screen appears.



3. Specify the following options:

Option	Description
User Nme	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).
Email Address	Specify the email address that applies to the user name (optional).
Freeze	Select whether to temporarily disable the new user account (optional). While frozen, the user is unable to log on devices.
Group User Type	Select the privileges of the new account. Options include:

Option	Description
	• User • Authenticator • Administrator **Note** Giving a user in a group administrator or authenticator privileges only applies those privileges within that group. That user is treated as a group administrator or group authenticator. Add an administrator or authenticator in the Enterprise, outside of the group, to give that user Enterprise-level privileges.
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. Options include: • **None** • **Fixed Password** • **Smart Card** If the **Group User Type** selection is **User**, the default authentication method is **None**. If the **Group User Type** selection is **Administrator** or **Authenticator**, the default authentication method is **Fixed Password**.

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 Agents in 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**.

Traffic Forwarding Services for Legacy Agents

Endpoint Encryption 5.0 Patch 4 includes backwards compatibility to manage all 5.0 versions of Endpoint Encryption as well as authenticate and perform commands on legacy agents (3.1.3 and earlier). Endpoint Encryption uses different architecture for 3.1.3 and earlier agents from 5.0 and later agents, so Endpoint Encryption requires different traffic forwarding services to manage communications between agents and servers.

The Endpoint Encryption Proxy manages the following services:

SERVICE	DESCRIPTION
Traffic Forwarding Service	The Traffic Forwarding Service directs network traffic between Endpoint Encryption 5.0 and later agents and PolicyServer residing in different local area networks. Endpoint Encryption 5.0 and later agents communicate using RESTful. The Traffic Forwarding Service sits between the agents and PolicyServer to prevent insecure policy access. The Traffic Forwarding Service installer configures the TMEEForward service that runs on the Endpoint Encryption Proxy endpoint.
Client Web Service	The Client Web Service directs traffic between legacy Endpoint Encryption agents (3.1.3 and earlier) 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 the MAWebService2 (Legacy Web Service), which is the same Microsoft IIS service installed by the PolicyServer installer in environments that do not use a proxy.

Configuring Traffic Forwarding Services

To create a network topology that includes endpoints of different versions, separately deploy services to an endpoint residing in the network DMZ, and configure

PolicyServer safely behind a firewall. Install the Endpoint Encryption proxy on the separate endpoint to direct and filter traffic between Endpoint Encryption agents and PolicyServer.

For an example network scenario including legacy agents, see *Deployment Including Legacy Agents on page 2-7*.

The Endpoint Encryption proxy has the following requirements:

- Traffic Forwarding Service and Client Web Service may not be deployed on the same endpoint as PolicyServer.
- The default port for the Traffic Forwarding Service is 8080.

  The default port for the Client Web Service is 80.
- In environments using both new and legacy Endpoint Encryption agents, configure different ports for Traffic Forwarding Service and Client Web Service.

Procedure

1. Copy the PolicyServer installation folder to the local hard drive.
2. Go to the path `<installation folder> \TMEE_PolicyServer\Tools \Optional Installations\TMEEProxy Installer` and run `TMEEProxyInstaller.exe`.

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

   The Endpoint Encryption proxy installer analyzes the endpoint.
4. Specify the PolicyServer IP address or host name and the port number of the Endpoint Encryption service.
5. Click **Continue**.

   The installation begins. Wait for the Endpoint Encryption proxy to install.
6. After installation completes, note the IP address and port number displayed in the installation screen.

This IP address and port will be used in agent installation.

7. Click **Finish**.

8. Verify the Client Web Service 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.

   Client Web Service is installed.

9. Verify the Traffic Forwarding Service installation.

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

      The **Services** screen appears.

   b. Verify that **TMEEForward** service has started.

   Traffic Forwarding Service is installed.

Chapter 5

Control Manager Integration

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

This chapter assumes that you have already installed and configured PolicyServer. For PolicyServer installation instructions, see *PolicyServer Installation on page 4-1*.

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. If you want to change the PolicyServer managed by Control Manager, remove the existing PolicyServer and add the new one.

Topics include:

Control Manager Integration Overview

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.

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 4.

   See *Upgrading PolicyServer on page 7-6*.

2. Install and configure a supported version of Control Manager.

   To verify which version of Control Manager to install, see *Supported Control Manager Versions on page 5-3*.

   For Control Manager installation instructions, 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 5-3*.

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

   See *Endpoint Encryption Users* in the *Endpoint Encryption Administrator's Guide*.

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

   See *Creating a Policy* in the *Endpoint Encryption Administrator's Guide*.

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

   See *Specifying Policy Targets* in the *Endpoint Encryption Administrator's Guide*.

7. Use Control Manager to deploy policies.

Supported Control Manager Versions

Endpoint Encryption supports the following Control Manager versions.

TABLE 5-1. Supported Control Manager versions

ENDPOINT ENCRYPTION VERSION	CONTROL MANAGER VERSION
5.0	6.0
5.0 Patch 1	6.0 SP1
5.0 Patch 2	6.0 SP2, 6.0 SP3
5.0 Patch 3	6.0 SP2, 6.0 SP3
5.0 Patch 4	6.0 SP3

Apply the latest patches and critical hot fixes for these Control Manager versions to enable Control Manager to manage Endpoint Encryption. To obtain the latest patches and hot fixes, contact your support provider or visit the Trend Micro Update Center at:

http://www.trendmicro.com/download

After installing Endpoint Encryption, register it to Control Manager and then configure settings for Endpoint Encryption on the Control Manager management console. See the *Control Manager documentation* for information on managing Endpoint Encryption servers.

Adding PolicyServer as a Managed Product to Control Manager

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

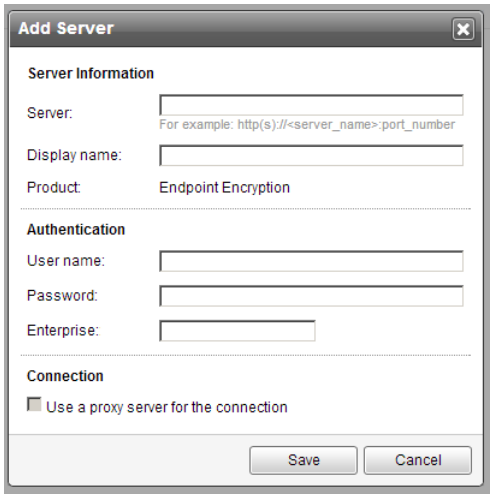
To perform additional Control Manager configuration, see the *Endpoint Encryption Administrator's Guide*.

Procedure

1. Log on to Control Manager.
2. Go to **Administration** > **Managed Servers**.

   The **Managed Servers** screen appears.
3. In the **Server Type** drop-down list, select **Endpoint Encryption**.
4. Click **Add**.

   The **Add Server** screen appears.



5. Specify **Server Information** options.

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

     `http://<server_name>:port_number`

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

- **Display name**: Specify the name for PolicyServer shown in the **Managed Servers** screen.

6. Under **Authentication**, specify the user name and password of the Endpoint Encryption Enterprise Administrator account and the Enterprise specified during PolicyServer installation.
7. Under **Connection**, select **Use a proxy server for the connection** if PolicyServer requires a proxy connection.
8. 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.

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. You may add another PolicyServer instance to Control Manager at this time.

Chapter 6

Endpoint Encryption Agent Deployment

Endpoint Encryption includes different agents to perform specific encryption and authentication tasks. This chapter describes the the deployment process for each agent, including installation prerequisites, manual installation tasks, and automated deployment tools.

Topics include:

Endpoint Encryption Agents

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

AGENT	DESCRIPTION
Full Disk Encryption	The Endpoint Encryption agent for hardware and software encryption with preboot authentication. Full Disk Encryption secures 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. The Full Disk Encryption agent may be installed on the same endpoint as the File Encryption agent. The Full Disk Encryption agent may not be installed on the same endpoint as either the Encryption Management for Microsoft BitLocker agent or the Encryption Management for Apple FileVault agent.
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. The Encryption Management for Microsoft BitLocker agent may be installed on the same endpoint as the File Encryption agent.
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.
File Encryption	The Endpoint Encryption agent for file and folder encryption on local drives and removable media. File Encryption protects files and folders located on virtually any device that appears as a drive within the host operating system. The File Encryption agent may be installed on the same endpoint as either the Full Disk Encryption agent or the Encryption Management for Microsoft BitLocker agent.

Agent Installation Prerequisites

Before installing the Endpoint Encryption agents, consult the following table for specific agent installation requirements.

CATEGORY	REQUIREMENTS
Endpoints	1. Each endpoint meets the minimum system requirements to install the intended agents. See *System Requirements on page 3-1*. 2. All UEFI-based endpoints have the boot priority changed to **Legacy First**. See *Changing UEFI Boot Priority on page 6-14*. 3. The boot drive of each endpoint has an unmodified MBR boot sector. For example, endpoints with multiple operating systems that include modified boot sectors are not supported. **Note** GUID Partition Table (GPT) disks are not supported. 4. Each endpoint has network access and can communicate with PolicyServer during installation. 5. The relevant agent installation packages are stored on each endpoint.
PolicyServer	1. PolicyServer is installed or upgraded to version 5.0 Patch 4. See *PolicyServer Installation on page 4-1*. 2. For environments using PolicyServer MMC, there is at least one top-level group configured. 3. For environments using Control Manager, there is at least one policy configured.

CATEGORY	REQUIREMENTS
Accounts	1. The Endpoint Encryption user account has permission to add devices to the group or policy. Enterprise administrator and authenticator accounts have device installation privileges. To give installation privileges to other user accounts, see *Allowing a User to Install Agents in a Group on page 4-15*. 2. The installing Windows account has Local Administrator privileges. For automated deployments, the installing account for each endpoint must have Local Administrator privileges as well. 3. 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
Automated deployments	1. An automated software distribution tool is installed, such as SMS, SCCM, Tivoli, GPO, or LANDesk. 2. Direct access to the endpoint hard drive is available for script deployment. Do not run Endpoint Encryption deployment scripts from USB devices or from shared network drives. 3. You have installation scripts for each agent. For help making installation scripts, use Command Builder and Command Line Helper. See *Automated Deployments on page 6-4*.
OfficeScan deployments	• For environments using OfficeScan, the environment is ready for agent deployment through OfficeScan Plug-in Manager. For more information, see the *OfficeScan Plug-in Online Help*.

Automated Deployments

Endpoint Encryption allows users to deploy agents in the following ways:

Deployment Method	Description
Manual	Run the agent installation program and configure PolicyServer settings manually on each endpoint. This option is prefered for test installations and endpoints that have individual hardware specifications.
Automated	Use an installation script to install and configure the agent automatically on one endpoint or on many endpoints at once (mass deployment). This option is prefered for environments that include many similar endpoints such as large enterprises. **WARNING!** Automated deployments skip pre-installation checking. Insufficient system setup or hard disk drive preparation may result in irreversible data loss. Verify that you have completed all relevant prerequisites before continuing. See *Agent Installation Prerequisites on page 6-3*.
OfficeScan	Deploy Full Disk Encryption agents to endpoints that already have OfficeScan agents through the Endpoint Encryption Deployment Tool plug-in. For information about using the plug-in, see the *OfficeScan Plug-in Online Help*.

To assist with creating scripts for automated deployments, Endpoint Encryption includes the following tools:

Tool	Description
Command Builder	The Command Builder generates complete installation command scripts for Full Disk Encryption, File Encryption, and Encryption Managemement for Microsoft BitLocker based on PolicyServer, Enterprise, and authentication values. **Tip** The Command Builder is a larger tool that encompasses the functionality of the Command Line Helper. If you intend to use the Command Builder, you do not need to use the Command Line Helper.

TOOL	DESCRIPTION
Command Line Helper	The Command Line Helper is a command line utility that generates individual encrypted strings to use for installation, upgrade, or patch scripts.

Command Builder

Full Disk Encryption and File Encryption are compliant with automated software distribution tools, such as SMS, SCCM, Tivoli, GPO, and LANDesk. Use the Command Builder to generate scripts used to install PolicyServer and Endpoint Encryption agents.

If you intend to use the Command Builder, ensure that your environment meets the agent installation prerequisites, including the automated deployment requirements. See *Agent Installation Prerequisites on page 6-3*.

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 Builder is available in the `Tools` folder of the installation directory.

Note

To run this tool, verify that PolicyServer or an Endpoint Encryption agent is installed on the same endpoint.

Procedure

1. Download the Command Builder tool and locate the tool in your Endpoint Encryption download folder.

   The Command Builder tool is part of the PolicyServer installation package. Go to Trend Micro Download Center, select the Endpoint Encryption, and download the PolicyServer package.

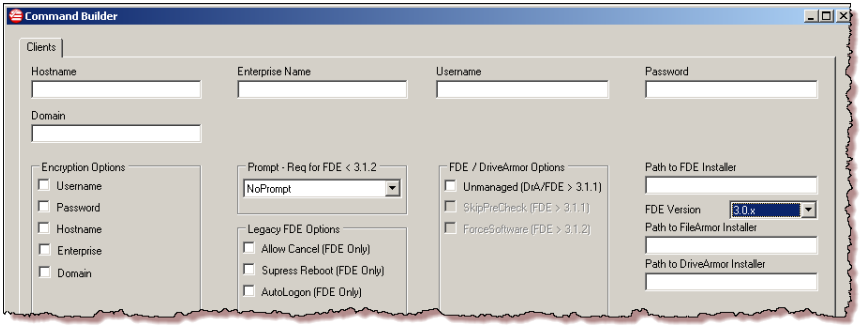
   http://downloadcenter.trendmicro.com/

The Command Builder tool is located in the following directory:

`<download_directory>\TMEE_PolicyServer\Tools\Command Line Helper`

2. Run `CommandBuilder.exe` from an endpoint with PolicyServer installed.

   The **Command Builder** screen appears.



3. Specify the following:

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

4. Select which the values you want to encrypt from the **Encryption Options**.

   The options selected in **Encryption Options** will replace the previously specified values with encrypted values in the generated command text.

5. Select whether to prompt the end user, or to do a silent installation.

Note

This function is only supported for legacy versions of the Full Disk Encryption agent.

6. 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.
7. Specify the path to the installation files.
8. Click **Generate Command**.

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

   The resulting script is copied to the clipboard.
10. 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 automated 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 Full Disk Encryption or PolicyServer installed.

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.

The following shows the fields that may use encrypted values, and the arguments used to receive encrypted values.

Field	Arguments		
	Full Disk Encryption Unencrypted	Full Disk Encryption Encrypted	File Encryption
Enterprise	`ENTERPRISE`	`eENTERPRISE`	`PSENTERPRISE`
PolicyServer	`HOST`	`eHOST`	`PSHOST`
User name	`USERNAME`	`eUSERNAME`	`FAUSER`
Password	`PASSWORD`	`ePASSWORD`	`FAPASSWORD`

Using the Command Line Helper

Command Line Helper enables encrypted values to pass via the installation script to the Full Disk Encryption preboot and installer. You can manually use Command Line Helper to generate encrypted values of strings for installation scripts or patch management.

Procedure

1. Download the Command Line Helper tool and locate the tool in your Endpoint Encryption download folder.

   The Command Line Helper tool is part of the PolicyServer installation package. Go to Trend Micro Download Center, select the Endpoint Encryption, and download the PolicyServer package.

   http://downloadcenter.trendmicro.com/

   The Command Line Helper tool is located in the following directory:

```
<download_directory>\TMEE_PolicyServer\Tools\Command Line
Helper
```

2. Open a command prompt.

3. Change the directory to the directory of the Command Line Helper tool.

   Example:

   ```
   cd C:\TMEE_PolicyServer\Tools\Command Line Helper
   ```

4. Type `CommandLineHelper.exe` followed by the string that you want to encrypt, and press ENTER.

   Example:

   ```
   CommandLineHelper.exe examplepassword
   ```

   Tip

   It may be easier to copy the generated value directly from a text file.

   In that case, the above example would be modified as follows:

   ```
   CommandLineHelper.exe examplepassword > file.txt
   ```

   The Command Line Helper produces an encrypted string.

Full Disk Encryption Deployment

The following section describes how to install and configure the Full Disk Encryption agent.

Before installing Endpoint Encryption agents, verify that your environment meets the *Agent Installation Prerequisites on page 6-3*.

Full Disk Encryption Manual Deployment

Installing the Full Disk Encryption Agent

To install Full Disk Encryption, perform the following procedure.

Procedure

1. Verify that all of the agent installation prerequisites have been completed.

   See *Agent Installation Prerequisites on page 6-3*.

2. Verify that the hard disk is not already encrypted, no other full disk encryption product is installed, and that Microsoft BitLocker is disabled.

3. Run a hard drive integrity utility on the system drive.

   For example, to run the Windows utility Check Disk, open a command prompt and run `chkdsk /f /r`. Windows will perform Check Disk on the next restart.

   If bad sectors are found, fix or replace the hard drive depending on your enterprise hardware policy.

4. Defragment the system drive.

5. Copy the installation files to the system drive.

6. 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 Full Disk Encryption installer checks the endpoint for installation issues. If a system incompatibility is discovered, the installer closes and generates the `PreInstallCheckReport.txt` in the same location as the installer. For more information, see *Pre-Installation Check on page 6-12*.

7. Specify the following PolicyServer information:

OPTION	DESCRIPTION
Server name	Specify the PolicyServer IP address, host name, or FQDN 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. At the **Installation Complete** screen, click **Close**.

   A message appears asking if you want to restart or shut down the endpoint. The endpoint restarts for software-based encryption or shuts down for hardware-based encryption.

9. Click **Yes** to restart or shutdown the endpoint.

   Full Disk Encryption installation is complete when the Full Disk Encryption preboot displays. At the preboot screen, the user must log on. The user is required to change their password after logging on. The next time Windows starts, Full Disk Encryption encrypts the disk.

   Policies are synchronized with PolicyServer after the endpoint restarts.

Pre-Installation Check

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. The following are the requirements that Full Disk Encryption installer checks.

SPECIFICATION	REQUIREMENT
Supported Operating System	The endpoint must have a supported operating system installed.

SPECIFICATION	REQUIREMENT
Encryption Management for Microsoft BitLocker is already 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	The physical disk must be fixed and not removable. Full Disk Encryption cannot be installed on removable drives running Windows.
Multiple hard disks	Only one hard disk is allowed on the endpoint.
Free space	The drive must have at least 256 MB of contiguous free disk space.
Disk size	The total disk space for each device must be no more than 2 TB.
Memory	The endpoint must have at least 512 MB of RAM. Trend Micro recommends having at least 1 GB of RAM.
Partition count	The drive must have fewer than 25 partitions. Partitions with extended MBRs are not supported.
Physical drive is bootable	The drive must be bootable.
SCSI disk	SCSI drives are not supported. **Note** This check only records a warning, because Windows may report a SATA drive as SCSI. If the disk is not SCSI, Full Disk Encryption may be installed. To verify that the drive is not SCSI, physically check the device.
Microsoft .NET Framework	Microsoft .NET Framework 2.0 SP1 or later is required for Windows XP or earlier devices. Microsoft .NET Framework 3.5 or later is required for Windows 8 or later devices.

SPECIFICATION	REQUIREMENT
SED hardware compatibility	If a drive is a self-encrypting drive, Full Disk Encryption enables hardware encryption for that drive. 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	Microsoft BitLocker must not be enabled. Two full disk encryption solutions may not run on the same drive. If your environment uses Microsoft BitLocker for encryption, install the Encryption Management for Microsoft BitLocker agent instead of Full Disk Encryption.
Intel Rapid Storage Technology	Drives using Intel Rapid Storage Technology with mSATA caches are not supported.
Keyboard	The Full Disk Encryption Preboot supports the current keyboard layout.
Wi-Fi/NIC	The Full Disk Encryption Preboot supports the system Network Interface Controller (NIC) and Wi-Fi hardware.

Changing UEFI Boot Priority

Endpoints that natively run Windows 8 or later operating systems are usually UEFI-based systems with GPT file systems. Full Disk Encryption 5.0 Patch 4 does not support UEFI firmware interfaces. If your endpoint uses UEFI, set the boot prioirty to **Legacy First** before installing Full Disk Encryption.

Procedure

1. From Windows, hold SHIFT and restart the device.

   The device restarts and UEFI BIOS loads.

2. Click the **Troubleshoot** tile.

The **Advanced options** screen appears.

3. 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.

4. Set **UEFI/Legacy Boot Priority** to **Legacy First**.

5. Restart the endpoint.

   The Full Disk Encryption agent may now be installed on the endpoint.

Full Disk Encryption Automatic Deployment

If performing automated and mass deployments, use the tools described in *Automated Deployments on page 6-4*. This section describes automatic deployment information specific to Full Disk Encryption.

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.

Tip

If you are performing a mass deployment, to simplify installation and minimize user impact, you may want to disable encryption. You can enable encryption at a later time to encrypt all devices simultaneously or when fewer users may be affected.

Depending on your primary management console, do the following to disable encryption during employment.

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 Script Example

The following is an example script to use for automated deployment. Use Command Line Helper to encrypt necessary credentials, and use Command Builder to generate the deployment script.

For example, the following values are placed into Command Builder:

Hostname	PolicyServer.mycompany.com
Enterprise Name	MyCompany
Username	GroupAdministrator
Password	123456
Path to FDE Installer	C:\Program Files\Trend Micro\Full Disk Encryption \TMFDEInstaller.exe

In this example, under **Encryption Options**, the fields **Username** and **Password** are selected.

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=
```

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.

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 6-19*.

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.

Encryption Management for Microsoft BitLocker Manual Deployment

Installing the Encryption Management for Microsoft BitLocker Agent

To install Encryption Management for Microsoft BitLocker, perform the following procedure.

Procedure

1. Verify that all of the agent installation prerequisites have been completed.

   See *Agent Installation Prerequisites on page 6-3*.

2. Verify that the hard disk is not already encrypted and that no other full disk encryption product is installed.

3. Run a hard drive integrity utility on the system drive.

   For example, to run the Windows utility Check Disk, open a command prompt and run `chkdsk /f /r`. Windows will perform Check Disk on the next restart.

   If bad sectors are found, fix or replace the hard drive depending on your enterprise hardware policy.

4. Defragment the system drive.

5. Copy the installation files to the system drive.

6. Run `TMFDEInstall_MB.exe`.

   Note

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

7. Specify the following PolicyServer information:

OPTION	DESCRIPTION
Server name	Specify the PolicyServer IP address, host name, or FQDN 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 **Install**.

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

9. 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

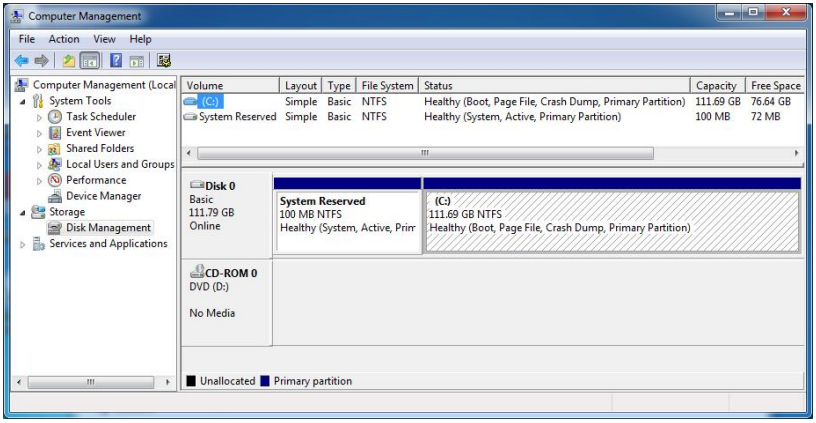
Encryption Management for Microsoft Bitlocker requires separate boot and system partitions on the local endpoint. On Microsoft Windows 7 and later versions, a system partition and a boot partition are both typically created during the installation process. If you attempt to install or upgrade Encryption 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, this procedure also shows how to 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.

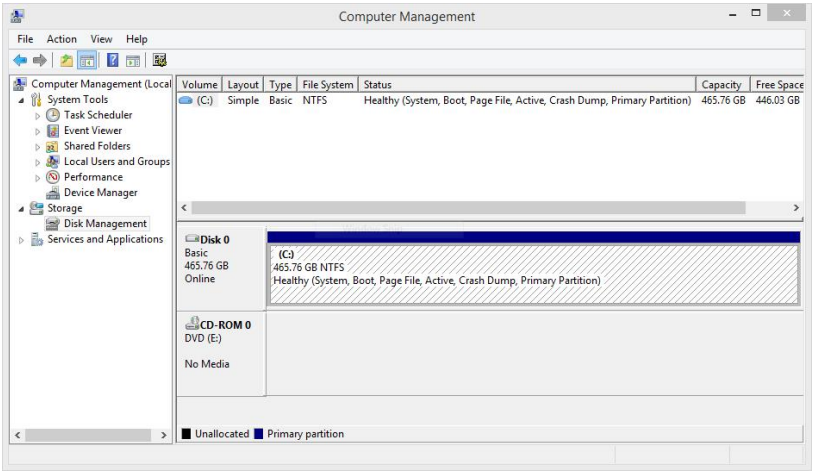
The following is an example of an endpoint that contains separate system and boot partitions:



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.

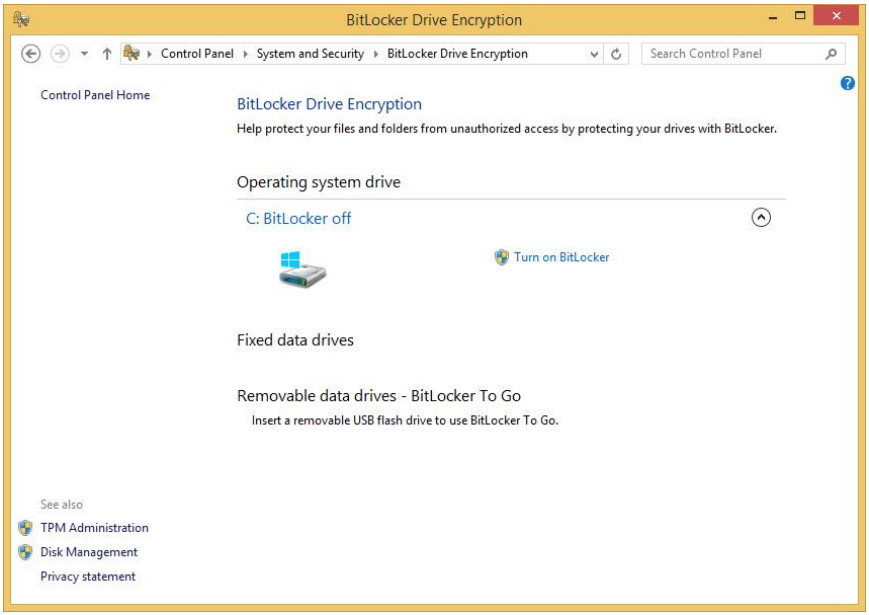
Important

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 backing up important files 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**.



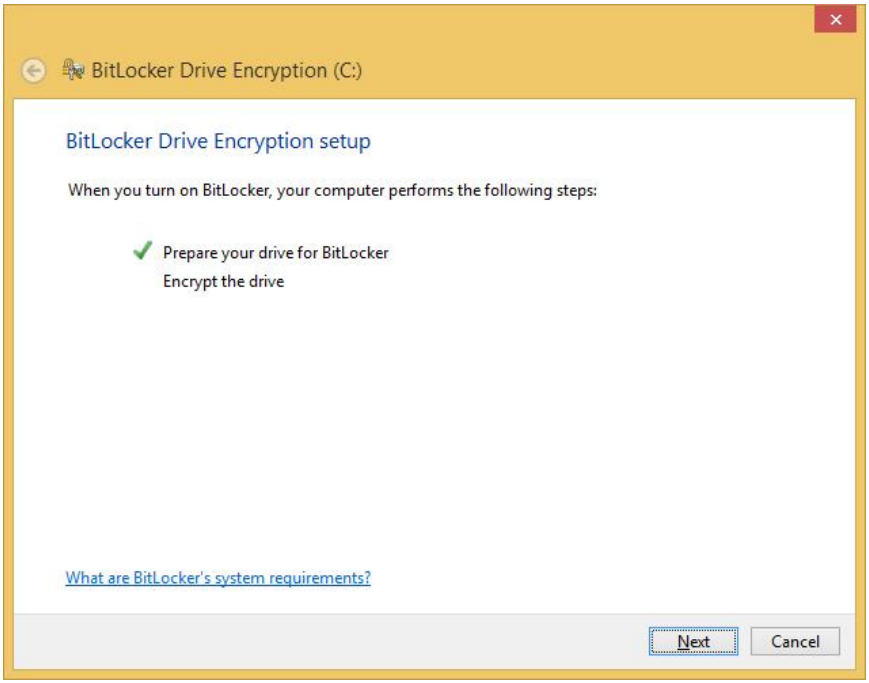
The **BitLocker Drive Encryption** window appears.

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.

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

Tip

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

The system partition has been created.

At this point you may re-install the Encryption Management for Microsoft BitLocker agent.

Troubleshooting Password and Encryption Issues

After installing Encryption Management for Apple FileVault and restarting the endpoint, Apple FileVault attempts to encrypt the disk. If the password specified during installation did not match the specified user account, the following window appears:

After specifying the correct password, restart the endpoint again. If the password was the issue, after restarting, Apple FileVault encrypts the endpoint.

If this problem persists, or if the encryption status displays that the endpoint is not encrypting, then another issue is restricting Apple FileVault functionality. Do the following procedure to determine the location of the issue and whether to send the issue to Trend Micro Support.

Procedure

1. From the Apple menu, go to **Security & Privacy** > **FileVault**.
2. If the lock icon is locked, click the lock icon to make changes.

3. Click **Turn On FileVault...**.

   A window appears that asks for your password.

4. Type your password and click **Start Encryption**.

   If your user account has permission to turn on FileVault, your credentials are correct, and FileVault is working properly, FileVault begins encrypting the disk.

5. If FileVault encounters any issues during encryption after this point, take relevant screenshots of those issues and contact Trend Micro Support.

Encryption Management for Microsoft BitLocker Automatic Deployment

If performing automated and mass deployments, use the tools described in *Automated Deployments on page 6-4*. This section describes automatic deployment information specific to Encryption Management for Microsoft BitLocker.

Encryption Management for Microsoft BitLocker Script Example

The following is an example script to use for automated deployment. Use Command Line Helper to encrypt necessary credentials, and use Command Builder to generate the deployment script.

For example, the following values are placed into Command Builder:

Hostname	PolicyServer.mycompany.com
Enterprise Name	MyCompany
Username	GroupAdministrator
Password	123456
Path to DriveArmor Installer	C:\Program Files\Trend Micro\FDE Management for Microsoft BitLocker\TMFDEInstall_MB.exe

In this example, under **Encryption Options**, the fields **Username** and **Password** are selected.

Output to install Encryption Management for Microsoft BitLocker:

```
C:\Program Files\Trend Micro\
FDE Management for Microsoft BitLocker\TMFDEInstall_MB.exe
ENTERPRISE=MyCompany HOST= PolicyServer.mycompany.com
eUSERNAME==jJUJC/Lu4C/Uj7yYwxubYhAuCrY4f7AbVFp5hKo2PR4O
ePASSWORD==5mih67uKdy7T1VaN2ISWGQQ=
```

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 X infrastructure.

Encryption Management for Apple FileVault Manual Deployment

Installing the Encryption Management for Apple FileVault Agent

To install Encryption Management for Apple FileVault, perform the following procedure.

Procedure

1. Verify that all of the agent installation prerequisites have been completed.

   See *Agent Installation Prerequisites on page 6-3*.

2. Verify that the hard disk is not already encrypted, no other full disk encryption product is installed, and that Apple FileVault is 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**.

3. Run a hard drive integrity utility on the system drive.

   For example, run Verify Disk from OS X Disk Utility. To use this feature, do the following:

   a. Restart your Mac in Recovery Mode by holding Command + R during startup.

   b. Click Disk Utility.

   c. Select your startup disk.

   d. Click **Verify Disk**.

e. If errors are found on the disk, click **Repair Disk**.

4. Check with your system administrator about whether you should defragment your system drive.

5. Copy the installation files to the system drive.

6. Run `TMFDEInstall_FV.exe`.

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

   The Installer checks that the system requirements are met.

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

9. Select the hard disk to install that agent.

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

    The installation begins.

11. Specify the following PolicyServer information:

OPTION	DESCRIPTION
Server name	Specify the PolicyServer IP address, host name, or FQDN 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. **Important** Make sure that you type the correct password at this time, or you may need to troubleshoot your encryption status later.

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

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

13. 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 later. 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 attempts to initiate 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.

Encryption Management for Apple FileVault Automatic Deployment

If performing automated and mass deployments, use the tools described in *Automated Deployments on page 6-4*. This section describes automatic deployment information specific to Encryption Management for Apple FileVault.

Deploying Encryption Management for Apple FileVault Automatically

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 6-33*.

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 7-15*.

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`.

   For help creating the `RegisterDevice` command script, see *Command Builder on page 6-6*.

   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 6-1. 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.

`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.

RETURN CODE	DESCRIPTION
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.

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=
```

File Encryption Deployment

This section describes how to install the File Encryption agent. Use File Encryption to protect files and folders 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 Manual Deployment

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

Procedure

1. Verify that all of the agent installation prerequisites have been completed.

   See *Agent Installation Prerequisites on page 6-3*.

2. Run `FileEncryptionInst.exe`

   The File Encryption Setup Wizard appears.

3. Click **Next**.

   Note

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

   The File Encryption installer initiates and automatically installs the agent.

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, host name, or FQDN and include the port number assigned to that configuration.
Enterprise	Specify the Enterprise. Only one Enterprise is supported.

7. Click **OK** to complete installation.
8. Go to the system tray and click the icon to open the File Encryption agent.

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

File Encryption Automatic Deployment

If performing automated and mass deployments, use the tools described in *Automated Deployments on page 6-4*. This section describes automatic deployment information specific to File Encryption.

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=
```

Chapter 7

Upgrade and Migration

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. This section also describes methods to migrate existing configurations to the most recent version of Endpoint Encryption.

WARNING!

Before upgrading the agent, make sure to first upgrade PolicyServer to version 5.0 Patch 4. Endpoint Encryption 5.0 and later agents cannot communicate with PolicyServer 3.1.3 or earlier.

Topics include:

- *Migration Scenarios on page 7-16*

Upgrade Summary of Operations

The following set of tasks are the recommended order for upgrading your environment.

Important

To avoid having endpoints lose connection to PolicyServer, make sure to upgrade PolicyServer before upgrading the agents. The keys to access data encrypted on those endpoints may become inaccessible if you upgrade in the wrong order.

If an agent is unable to 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 3-1*.

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

3. Make sure that Endpoint Encryption 5.0 Patch 4 supports the upgrade.

   See *Supported Agent Versions on page 7-10*.

4. Upgrade PolicyServer.

   See *Upgrading PolicyServer on page 7-6*.

5. Optionally install or upgrade Control Manager and configure as necessary.

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

6. Optionally install or upgrade OfficeScan and configure as necessary.

   See the *OfficeScan Plug-in Online Help*.

7. Upgrade Endpoint Encryption agents.

See *Upgrading Endpoint Encryption Agents on page 7-10*.

Upgrade Paths

The following table describes the upgrade path from each previous product version to version 5.0 Patch 4. Some older versions cannot upgrade directly to 5.0 Patch 4 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 4. For older versions of Endpoint Encryption that require multiple upgrades, you may need to perform reconfiguration for proper agent validation and PolicyServer synchronization.

TABLE 7-1. Upgrade Paths

PRODUCT/AGENT	VERSION	UPGRADE PATH
PolicyServer	5.0 and later	5.0 → 5.0 Patch 4
	3.1.3 SP1	3.1.3 SP1 → 5.0 Patch 4
	3.1.3	3.1.3 → 5.0 Patch 4
	3.1.2	3.1.2 → 5.0 → 5.0 Patch 4
Full Disk Encryption	5.0 and later	5.0 → 5.0 Patch 4
	3.1.3 SP1	3.1.3 SP1 → 5.0 Patch 4
	3.1.3	3.1.3 → 5.0 Patch 4

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 4
	SP7g	SP7g → 3.1.3 → Full Disk Encryption 5.0 → Full Disk Encryption 5.0 Patch 4
	SP7-SP7f	SP7-SP7f → SP7g → 3.1.3 → Full Disk Encryption 5.0 → Full Disk Encryption 5.0 Patch 4
File Encryption	5.0 and later	5.0 → 5.0 Patch 4
FileArmor	3.1.3 SP1	FileArmor 3.1.3 SP1 → File Encryption 5.0 → File Encryption 5.0 Patch 4
	3.1.3	FileArmor 3.1.3 → File Encryption 5.0 → File Encryption 5.0 Patch 4
	3.0.14	FileArmor 3.0.14 → FileArmor 3.1.3 → File Encryption 5.0 → File Encryption 5.0 Patch 4
	3.0.13	FileArmor 3.0.13 → FileArmor 3.1.3 → File Encryption 5.0 → File Encryption 5.0 Patch 4
Encryption Management for Microsoft BitLocker	5.0 and later	5.0 → 5.0 Patch 4
Encryption Management for Apple FileVault	5.0	5.0 → 5.0 Patch 4
OfficeScan Plug-in Service (Full Disk Encryption Deployment Tool)	5.0	5.0 → 5.0 Patch 4
Control Manager widgets	5.0	5.0 → 5.0 Patch 4

Upgrading PolicyServer

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 7-3*

WARNING!

Before upgrading the agent, make sure to first upgrade PolicyServer to version 5.0 Patch 4. Endpoint Encryption 5.0 Patch 4 agents cannot communicate with PolicyServer 3.1.3 or earlier.

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 4-4*.

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 *Traffic Forwarding Services for Legacy Agents on page 4-16*.

Procedure

1. Verify that all system requirements are met.

   See *PolicyServer System Requirements on page 3-2*.

2. Stop the services "TMEEservice" and "PolicyServerWindowsService".

3. Run `PolicyServerInstaller.exe`

   The PolicyServer Installer opens.

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

5. 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 7-4*.

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

7. At the **Windows Service Logon** screen, click **Continue**.

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

OPTION	DESCRIPTION
Server	The Microsoft SQL Server host name (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 database host name or IP address used. Use the following syntax to specify an instance:

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

The installer verifies the database connection.

9. At the **PolicyServer Question** message, do one of the following:
   - Click **Yes** to back up existing data
   - Click **No** to overwrite existing data
10. 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 4 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 encrypted 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.

11. 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**.
12. 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 4 does not support older versions of PolicyServer MMC. Only click **No** if another endpoint with PolicyServer MMC 5.0 Patch 4 installed manages PolicyServer.

The installation process begins.

13. At the **PolicyServer Installation** message, click **OK**.
14. Click **Finished**.
15. From the PolicyServer Installer window, click **Exit**.
16. 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 services "TMEEservice" and "PolicyServerWindowsService" 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 7-6*.
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 4. Upgrading the PolicyServer MMC is required.

Procedure

1. Complete *Uninstalling the PolicyServer MMC on page 8-7*.
2. Complete *Installing PolicyServer MMC on page 4-8*.

Upgrading Endpoint Encryption Agents

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 4. Endpoint Encryption 5.0 Patch 4 agents cannot communicate with PolicyServer 3.1.3 or earlier.

Supported Agent Versions

Although PolicyServer supports policy management for all agents, older agents cannot register as a new device in PolicyServer 5.0 Patch 4 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 7-2. SUPPORTED LEGACY AGENTS FOR NEW DEVICES

AGENT	VERSION	CAN REGISTER AS A NEW DEVICE	POLICIES SUPPORTED
Full Disk Encryption	5.0 Patch 3	●	●
	5.0 Patch 2	●	●
	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 3	●	●
	5.0 Patch 2	●	●
	5.0 Patch 1	●	●
	5.0	●	●
FileArmor	3.1.3	●	●
	3.0.14		
	3.0.13		
Encryption Management for Microsoft BitLocker	5.0 Patch 3	●	●
	5.0 Patch 2	●	●
	5.0 Patch 1	●	●
	5.0	●	●

Agent	Version	Can Register as a New Device	Policies Supported
Encryption Management for Apple FileVault	5.0 Patch 3	●	●
	5.0 Patch 2	●	●
	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 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 8-6*.
   - To manually uninstall Full Disk Encryption, see *Uninstalling Full Disk Encryption on page 8-2*.

- To manually uninstall File Encryption, see *Uninstalling File Encryption on page 8-5*.
- To manually uninstall Encryption Management for Microsoft BitLocker, see *Uninstalling Encryption Management for Microsoft BitLocker on page 8-4*.

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 6-10*.
   - For information about installing File Encryption, see *File Encryption Deployment on page 6-36*.

Upgrading Full Disk Encryption

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 4. 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. Verify that your current version upgrades directly to 5.0 Patch 4.

   See *Upgrade Paths on page 7-4*.

   If your version does not directly upgrade to the latest version, contact Trend Micro support to assist you with your upgrade.

2. Copy the installation package to the local hard drive.
3. 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 upgrade process begins.

WARNING!

Do not shut down or restart the endpoint or put the endpoint to sleep, as these actions may interrupt the upgrade process. If upgrade is interrupted, at the next system start, you may be unable to access or log on the Full Disk Encryption preboot.

4. When the upgrade completes, restart the endpoint.

Upgrading File Encryption

Before you begin

- Verify *File Encryption System Requirements on page 3-9*
- Review *Upgrade Paths on page 7-4*

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 4.

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 6-26*.

Upgrading Encryption Management for Microsoft BitLocker

Procedure

1. Complete *Uninstalling Encryption Management for Microsoft BitLocker on page 8-4*.

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 6-17*.

Migration Scenarios

Administrators may need to migrate Endpoint Encryption devices when employees move to a different department or office location. Each PolicyServer instance supports one Enterprise configuration that may represent a business unit or department.

Moving to a new Enterprise adds the Endpoint Encryption device to the new Enterprise within the same PolicyServer instance. The Endpoint Encryption remains in the old Enterprise until removed.

Moving to a new PolicyServer 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 Deployment on page 6-10*.

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.

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 7-20*.

Changing the Enterprise requires access to Full Disk Encryption Recovery Console. For more information, see *Recovery Console* in the *Endpoint Encryption Administrator's Guide*.

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 7-1. 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 Agents 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.

Procedure

1. Start or restart the endpoint.

   The Full Disk Encryption preboot appears.

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

3. Specify Endpoint Encryption user account credentials.

   Note

   By default, only Administrator and Authenticator accounts may access the Recovery Console. To allow other users to access the Recovery Console, enable user recovery from your management console.

4. Click **Login**.

   The Recovery Console opens.

5. Go to **Network** > **Setup**.
6. Select the **PolicyServer** tab.
7. Click **Change Server**.
8. At the warning message, click **Yes**.
9. Specify the new server address.
10. 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 Agents to a New PolicyServer on page 7-20*.

Procedure

1. Uninstall the Encryption Management for Apple FileVault agent.

   See *Uninstalling Encryption Management for Apple FileVault on page 8-3*.

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 6-26*. 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 Agents to a New PolicyServer on page 7-20*.

Procedure

1. Uninstall the Encryption Management for Microsoft BitLocker agent.

   See *Uninstalling Encryption Management for Microsoft BitLocker on page 8-4*.

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 6-17*. 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 Agents to a New PolicyServer on page 7-20*.

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**.

Chapter 8

Uninstallation

The following section explains how to manually uninstall PolicyServer or Endpoint Encryption agents.

When uninstalling Endpoint Encryption, uninstall all Endpoint Encryption agents first, and then uninstall PolicyServer.

Topics include:

Uninstalling 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.

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.

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

Procedure

1. 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.

2. Click **Next**.

   Full Disk Encryption begins to uninstall.

3. Click **OK** to confirm hard drive decryption.

   To view decryption status, open Full Disk Encryption from the system tray.

WARNING!

Do not shut down or restart the endpoint or put the endpoint to sleep, as these actions may interrupt the decryption process. If decryption is interrupted, some data may become corrupted.

4. When decryption completes, click **OK**.

5. Run `TMFDEUninstall.exe` again to complete uninstallation.

6. Restart the endpoint.

   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 6-26*.

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.

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 uninstallation is unable to complete, manually uninstall the agent. See the *Endpoint Encryption Installation Guide*.

   When uninstallation completes, the Endpoint Encryption agent is removed and the product folder is deleted from the endpoint.

Uninstalling PolicyServer

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 4-4*.

Uninstalling the Endpoint Encryption Proxy

Uninstall the Endpoint Encryption Proxy using the Endpoint Encryption Proxy installer.

Procedure

1. Download or locate the Endpoint Encryption Proxy installer on the endpoint with the Endpoint Encryption Proxy installed.
2. Run `TMEEProxyInstaller.exe` with administrator privileges.

   The Endpoint Encryption Proxy installer detects that the Endpoint Encryption Proxy is already installed. A message appears that asks whether you would like to uninstall the proxy, or reinstall or upgrade the proxy.
3. Click **Yes** to uninstall the proxy.

   The Endpoint Encryption Proxy uninstalls the Client Web Service and the TMEEForward service.
4. After the services have been successfully uninstalled, click **Finish**.

Index

V

W

TREND MICRO INCORPORATED

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

www.trendmicro.com

Item Code: APEM57328/160222