



3.1 TREND MICRO™ Endpoint Encryption

Installation Guide

Comprehensive Endpoint Encryption for Data at Rest



Endpoint Security

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

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

Trend Micro, the Trend Micro t-ball logo, Endpoint Encryption, PolicyServer, Full Disk Encryption, FileArmor, and KeyArmor are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2012. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM35671/120920

Release Date: Dec 2012

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

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

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

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

Evaluate this documentation on the following site:

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

Table of Contents

Preface

| | |
|----------------------------|------|
| Preface | v |
| Product Document Set | vi |
| Document Conventions | vi |
| Intended Audience | vii |
| Terminology | viii |
| About Trend Micro | x |

Chapter 1: Introducing Trend Micro Endpoint Encryption

| | |
|--------------------------------------|------|
| About Endpoint Encryption | 1-2 |
| Endpoint Encryption Components | 1-2 |
| System Requirements | 1-4 |
| Key Features & Benefits | 1-8 |
| Management and Integration | 1-9 |
| Understanding Encryption | 1-9 |
| File Encryption | 1-10 |
| Full Disk Encryption | 1-10 |
| Key Management | 1-11 |
| About FIPS | 1-11 |

Chapter 2: Deployment Considerations

| | |
|--------------------------------------------------------|-----|
| Supported Platforms and Pre-deployment Checklist | 2-3 |
| Initial Deployment Questions | 2-5 |
| Assigning a Project Team | 2-7 |
| Security Infrastructure Checklist | 2-7 |
| Establishing Policy and Security Profiles | 2-8 |
| The Importance of a Pilot Program | 2-8 |

| | |
|-----------------------------------------------------------|------|
| Change Management Considerations | 2-9 |
| End-user Communication | 2-9 |
| Questions to Answer | 2-10 |
| Implement a Phased Rollout Strategy | 2-10 |
| Let Users Know What, When and Why | 2-10 |
| Scaling: PolicyServer and SQL Database Requirements | 2-11 |
| Scaling Example | 2-16 |

Chapter 3: PolicyServer Installation

| | |
|---------------------------------------------------------|------|
| Introducing PolicyServer | 3-2 |
| Installation Folder Contents | 3-2 |
| PolicyServer Requirements | 3-3 |
| Hardware Requirements | 3-3 |
| Software Requirements | 3-4 |
| Required Installation Files | 3-5 |
| Required Accounts | 3-5 |
| PolicyServer Installation Process | 3-6 |
| Installing PolicyServer Database and Web Services | 3-6 |
| PolicyServer MMC | 3-9 |
| PolicyServer AD Synchronization | 3-12 |
| Active Directory Overview | 3-12 |
| Configuring Active Directory | 3-13 |
| Optional LDAP Proxy | 3-17 |
| LDAP Requirements | 3-17 |
| LDAP Proxy Hardware Checklist | 3-18 |

Chapter 4: Endpoint Encryption Client Installation

| | |
|------------------------------------------------|-----|
| Pre-installation Considerations | 4-2 |
| Installing Full Disk Encryption | 4-2 |
| Pre-deployment Options | 4-2 |
| Pre-installation Checklist | 4-3 |
| Full Disk Encryption System Requirements | 4-3 |
| Hard Disk Drive Preparation | 4-4 |

| | |
|-----------------------------------------------|------|
| Full Disk Encryption Installation | 4-7 |
| Installing FileArmor | 4-12 |
| FileArmor Deployment Outline | 4-12 |
| FileArmor Installation | 4-14 |
| KeyArmor | 4-16 |
| KeyArmor System Requirements | 4-16 |
| Device Components | 4-17 |
| KeyArmor Deployment Outline | 4-17 |
| KeyArmor End-user Guidelines | 4-18 |
| Protecting KeyArmor Files | 4-18 |
| Using Scripts to Automate Installations | 4-19 |
| Requirements | 4-19 |
| Script Arguments | 4-20 |
| Command Line Installer Helper | 4-21 |
| Command Line Helper | 4-22 |

Chapter 5: Upgrades, Migrations and Uninstalls

| | |
|-----------------------------------------------------------|------|
| Upgrading Server and Client Software | 5-2 |
| Upgrading PolicyServer | 5-2 |
| Upgrading Full Disk Encryption | 5-6 |
| Upgrading FileArmor | 5-7 |
| Upgrading to Windows 8 | 5-8 |
| Patch Management with Full Disk Encryption | 5-9 |
| Using Command Line Helper | 5-9 |
| Patching Process for Full Disk Encryption | 5-10 |
| Replacing a Previously Installed Encryption Product | 5-10 |
| Option 1: Remove Previous Encryption Product | 5-11 |
| Option 2: Back Up and Re-image the Device | 5-11 |
| Migrating Endpoint Clients to a New PolicyServer | 5-12 |
| Changing the Full Disk Encryption PolicyServer | 5-12 |
| Moving Full Disk Encryption to a New Enterprise | 5-13 |
| Changing the FileArmor PolicyServer | 5-15 |
| Moving KeyArmor to a New Enterprise | 5-15 |

| | |
|-----------------------------------------|------|
| Uninstalling Client Applications | 5-16 |
| Uninstalling Full Disk Encryption | 5-16 |
| Uninstalling FileArmor | 5-17 |

Chapter 6: Getting Support

| | |
|------------------------------------|-----|
| Trend Community | 6-2 |
| Support Portal | 6-2 |
| Contacting Technical Support | 6-3 |
| Resolving Issues Faster | 6-3 |
| TrendLabs | 6-4 |

Appendix A: Endpoint Encryption Pilot Checklist

Appendix B: Security Infrastructure Checklist

Appendix C: Full Disk Encryption Pre-installation Checklist

Index

| | |
|-------------|------|
| Index | IN-1 |
|-------------|------|

Preface

Preface

Welcome to the Trend Micro™ Endpoint Encryption Installation Guide. This guide encourages Administrators to get “up and running” in the shortest possible time by introducing Endpoint Encryption functions and the security architecture. Topics include system requirements, how to prepare for deployment, how to install PolicyServer and client software, describes what should be explained to end-users, and how to upgrade or migrate server and client applications.

This preface covers the following topics:

- *Product Document Set on page vi*
- *Document Conventions on page vi*
- *Intended Audience on page vii*
- *Terminology on page viii*
- *About Trend Micro on page x*

Product Document Set

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

TABLE 1. Product Documentation

| DOCUMENT | DESCRIPTION |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Installation Guide | The Installation Guide explains system requirements and contains detailed instructions about how to deploy, install, migrate, and upgrade PolicyServer and endpoint clients. |
| Administrator's Guide | The Administrator's Guide explains product concepts, features and detailed instructions about how to configure and manage PolicyServer and endpoint clients. |
| Readme file | The Readme file contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, known issues, and product release history. |
| Knowledge Base | An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following website: http://esupport.trendmicro.com |



Note





All documentation is accessible from:

docs.trendmicro.com

Document Conventions

The documentation uses the following conventions:

TABLE 2. Document Conventions

| CONVENTION | DESCRIPTION |
|-----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UPPER CASE | Acronyms, abbreviations, and names of certain commands and keys on the keyboard |
| Bold | Menus and menu commands, command buttons, tabs, and options |
| <i>Italics</i> | References to other documents |
| Monospace | Sample command lines, program code, web URLs, file names, and program output |
| Navigation > Path | The navigation path to reach a particular screen For example, File > Save means, click File and then click Save on the interface |
|  Note | Configuration notes |
|  Tip | Recommendations or suggestions |
|  Important | Information regarding required or default configuration settings and product limitations |
|  WARNING! | Critical actions and configuration options |

Intended Audience

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

- Device hardware setup and configuration

- Hard drive partitioning, formatting, and maintenance
- Client-server architecture

Terminology

The following table provides terminology used throughout the documentation:

TABLE 3. Endpoint Encryption Terminology

| TERM | DESCRIPTION |
|-------------------------------|----------------------------------------------------------------------------------------------------|
| Authentication | The process of identifying a user. |
| ColorCode™ | A color-sequence password. |
| Command Line Helper | Create encrypted values to secure credentials when creating an installation script. |
| Command Line Installer Helper | Create encrypted values to secure credentials when generating scripts for automated installations. |
| Device | Computer, laptop, or removal media (external drive, USB drive) hardware. |
| Domain authentication | Single sign-on (SSO) using Active Directory. |
| DriveTrust™ | Hardware-based encryption technology by Seagate™. |
| Endpoint client | Any device with an Endpoint Encryption application installed. |
| FileArmor | The Endpoint Encryption client for file and folder encryption on local drives and removable media. |
| FIPS | Federal Information Processing Standard. United States federal government computing standards. |
| Fixed password | A standard user password consisting of letters and/or numbers and/or special characters. |
| Full Disk Encryption | The Endpoint Encryption client for hardware and software encryption with preboot authentication. |

| TERM | DESCRIPTION |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| KeyArmor | The Endpoint Encryption client for a password-protected, encrypted USB drive. |
| OCSP | The Online Certificate Status Protocol (OCSP) is an Internet protocol used for X.509 digital certificates. |
| OPAL | Trusted Computing Group's Security Subsystem Class for client devices. |
| Password | Any type of authentication data, such as fixed, PIN, and ColorCode. |
| PolicyServer | The central management server that deploys encryption and authentication policies to the endpoint clients (Full Disk Encryption, FileArmor, KeyArmor). |
| SED | Secure Encrypted Device. A hard drive, or other device, which is encrypted. |
| Smart card | A physical card used in conjunction with a PIN or fixed password. |
| PIN | A Personal Identification Number, commonly used for ATM transactions. |
| Recovery Console | Recover a device in the event of primary OS failure, troubleshoot network issues, and manage users, policies, and logs. |
| Remote Help | Interactive authentication for users who forget their credentials or devices that have not synchronized policies within a pre-determined amount of time. |
| Repair CD | Use this bootable CD to decrypt drive before removing Full Disk Encryption in the event that the disk becomes corrupted, |
| RSA SecurID | A mechanism for performing two-factor authentication for a user to a network resource. |
| Self Help | Question and answer combinations that allow users to reset a forgotten password without contacting Support. |

About Trend Micro

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

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

<http://www.trendmicro.com>

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

Chapter 1

Introducing Trend Micro Endpoint Encryption

When assessing the value of any Endpoint Encryption project, careful planning is essential.

This chapter introduces the following topics:

- *About Endpoint Encryption on page 1-2*
- *System Requirements on page 1-4*
- *Key Features & Benefits on page 1-8*
- *Management and Integration on page 1-9*
- *Understanding Encryption on page 1-9*

About Endpoint Encryption

Trend Micro Endpoint Encryption is a fully integrated hardware-based and software-based encryption solution to protect laptops and desktops, files and folders, removable media, and encrypted USB drives with embedded anti-malware/antivirus protection. With Endpoint Encryption, Administrators can use a single management console to flexibly manage a combination of hardware and software-based encryption with full transparency for end-users.

Trend Micro Endpoint Encryption ensures end-to-end data protection by providing FIPS 140-2 encryption of the data residing on the management server; all data transmitted to/from the server; all data stored on the endpoint device; and, all locally stored client logs.

Using FIPS 140-2 accredited cryptography, Endpoint Encryption offers the following benefits:

- Comprehensive data protection through fully integrated full disk, file, folder, USB drives, and removable media encryption.
- Centralized policy administration and key management through a single management server and console.
- Device management through device-specific information gathering and remote lock, reset, and the capability to wipe all endpoint data.
- Advanced real-time reporting and auditing to ensure security compliance.

Endpoint Encryption Components

Endpoint Encryption consists of one central management server (PolicyServer Web Service) that manages the policy and log databases (MobileArmor DB), LDAP authentication with Active Directory, and all client-server activity. Endpoint Encryption clients cannot interface directly with PolicyServer and must connect through the Client Web Service. For an illustration of this architecture, see *Figure 1-1: Endpoint Encryption Client-Server Architecture on page 1-3*.

**Note**

The port settings for all HTTP traffic is configurable at time of installation or through settings on the Endpoint Encryption client.

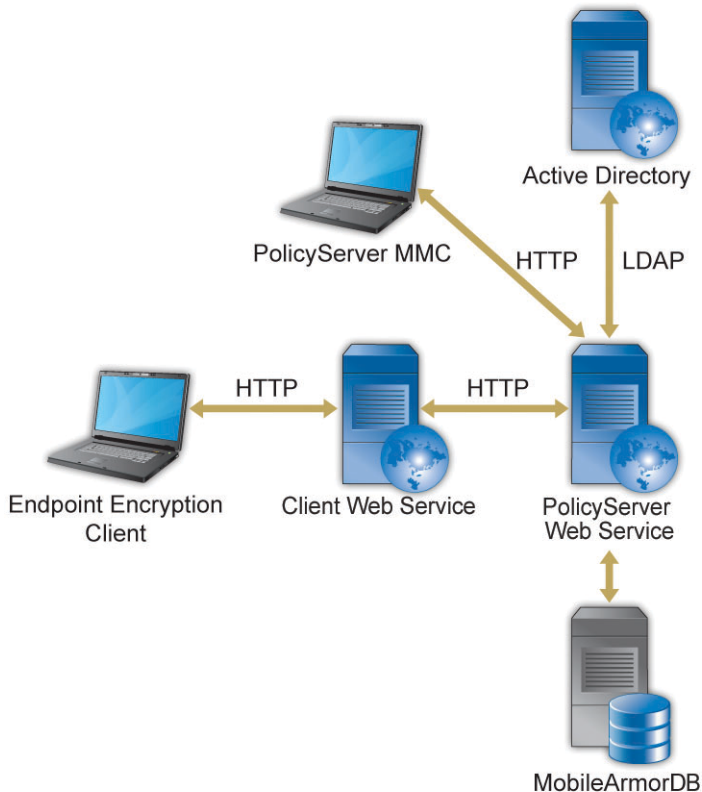



FIGURE 1-1. Endpoint Encryption Client-Server Architecture

The following table describes these components.

TABLE 1-1. Endpoint Encryption Components

| COMPONENT | DESCRIPTION |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PolicyServer Web Service | The IIS web service that provides central management of policy administration, authentication, and reporting. |
| PolicyServer MMC | The PolicyServer Microsoft™ Management Console (MMC) is the interface used to control PolicyServer. |
| Endpoint Encryption client | <p>An Endpoint Encryption client is any device with either Full Disk Encryption, FileArmor, or KeyArmor installed.</p> <ul style="list-style-type: none"> • Full Disk Encryption provides hardware and software full disk encryption, and preboot authentication. • FileArmor provides file and folder encryption for content on local drives and removable media. • KeyArmor is a hardened, encrypted USB drive with integrated antivirus protection. |
| MobileArmorDB | The Microsoft™ SQL Server database storing all user, policy, and log details. |
| Active Directory | <p>The PolicyServer Web Service synchronizes user account information by communicating with Active Directory using LDAP. Account information is cached locally in the MobileArmorDB.</p> <hr/> <p> Note Active Directory is optional.</p> <hr/> |
| Client Web Service | The IIS web service that Endpoint Encryption clients use to communicate with the PolicyServer Web Service. |

System Requirements

The tables below outline the system requirements for Endpoint Encryption.

TABLE 1-2. PolicyServer Hardware Requirements

| SEPARATE HOSTS | | SINGLE HOST |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| PolicyServer Host (3,000 Users) | SQL Server Host (3,000 Users) | PolicyServer and SQL Server (1,500 Users) |
| <ul style="list-style-type: none"> • 2GHz Dual Quad Core Core2 Intel™ Xeon™ Processors • 4GB RAM • 40GB hard disk space | <ul style="list-style-type: none"> • 2GHz Dual Quad Core Core2 Intel™ Xeon™ Processors • 8GB RAM • 100GB hard disk space | <ul style="list-style-type: none"> • 2GHz Quad Core Core2 Intel™ Xeon™ Processors • 8GB RAM • 120GB hard disk space |

TABLE 1-3. PolicyServer Minimum Software Requirements



| FUNCTION | REQUIREMENT |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operating System | <ul style="list-style-type: none"> • Windows Server 2003 SP2 32/64-bit • Windows Server 2008 or 2008 R2 64-bit |
| Applications and Settings | <ul style="list-style-type: none"> • Application Server <ul style="list-style-type: none"> • IIS • Allow Active Server pages • Allow ASP.NET • .Net Framework 2.0 SP2 <hr/> <p> Note PolicyServer 3.1.3 requires two IIS locations. The PolicyServer Administration Interface and the Client Application Interface should be installed on different IIS locations.</p> <hr/> |
| Database | <ul style="list-style-type: none"> • Microsoft SQL 2005/2008/2008 R2 • Microsoft SQL Express 2005(SP3)/2008 • Mixed Mode Authentication (SA password) installed • Reporting services installed |

TABLE 1-4. Full Disk Encryption System Requirements

| ITEM | REQUIREMENT |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Processor | Intel™ Core™ 2 or compatible processor. |
| Memory | <ul style="list-style-type: none"> • Minimum: 1GB |
| Disk space | <ul style="list-style-type: none"> • Minimum: 30GB • Required: 20% free disk space • Required: 256MB contiguous free space |
| Network connectivity | Communication with PolicyServer 3.1.3 required for managed installations |
| Operating Systems | <ul style="list-style-type: none"> • Windows 8™ (32/64-bit) • Windows 7™ (32/64-bit) • Windows Vista™ with SP1 (32/64-bit) • Windows XP™ with SP3 (32-bit) |
| Other software | <p>Additional requirements Windows 8:</p> <ul style="list-style-type: none"> • Microsoft .NET Framework 3.5 is enabled • For devices with UEFI, see Preparing the Device on page 4-5 to change the boot priority. <p>Additional requirements for Windows XP:</p> <ul style="list-style-type: none"> • Microsoft .NET Framework 2.0 SP1 or later • Microsoft Windows Installer 3.1 |
| Hard disk | <ul style="list-style-type: none"> • Seagate DriveTrust drives • Seagate OPAL and OPAL 2 drives <hr/> <p> Note</p> <ul style="list-style-type: none"> • RAID and SCSI disks are not supported. • Full Disk Encryption for Windows 8 does not support RAID, SCSI, eDrive, or OPAL 2 drives. |

| ITEM | REQUIREMENT |
|----------------|-----------------------------------------|
| Other hardware | ATA, AHCI, or IRRT hard disk controller |

TABLE 1-5. FileArmor System Requirements

| ITEM | REQUIREMENT |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Processor | Intel™ Core™2 or compatible processor. |
| Memory | <ul style="list-style-type: none"> • Minimum: 512MB • Recommended: 1GB |
| Disk space | <ul style="list-style-type: none"> • Minimum: 2GB • Required: 20% free disk space |
| Network connectivity | Communication with PolicyServer required for managed installations |
| Operating Systems | <ul style="list-style-type: none"> • Windows 8™ (32/64-bit) • Windows 7™ (32/64-bit) • Windows Vista™ with SP1 (32/64-bit) • Windows XP™ with SP3 (32-bit) |
| Other software | <p>Additional requirements for Windows 8:</p> <ul style="list-style-type: none"> • Microsoft .NET Framework 3.5 is enabled • For devices with UEFI, see Preparing the Device on page 4-5 to change the boot priority. <p>Additional requirements for Windows XP:</p> <ul style="list-style-type: none"> • Microsoft .NET Framework 2.0 SP1 or later • Microsoft Windows Installer 3.1 |

TABLE 1-6. KeyArmor System Requirements

| ITEM | REQUIREMENT |
|----------|--------------|
| Hardware | USB 2.0 port |

| ITEM | REQUIREMENT |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network connectivity | Communication with PolicyServer required for managed installations |
| Operating Systems | <ul style="list-style-type: none"> • Windows 7™ (32/64-bit) • Windows Vista™ with SP1 (32/64-bit) • Windows XP™ with SP3 (32-bit) |
| Other software | Additional software required when installing on Windows XP™: <ul style="list-style-type: none"> • Microsoft .NET Framework 2.0 SP1 or later |

Key Features & Benefits

Endpoint Encryption includes the following key features and benefits:

TABLE 1-7. Endpoint Encryption Key Features

| FEATURE | BENEFITS |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Encryption | <ul style="list-style-type: none"> • Protection for the full disk, including the master boot record (MBR), operating system, and all system files. • Hardware-based and software-based encryption for mixed environments. |
| Authentication | <ul style="list-style-type: none"> • Flexible authentication methods, including both single and multi-factor. • Policy updates before authentication and system boot. • Configurable actions on failed password attempt threshold. |
| Device management | <ul style="list-style-type: none"> • Policies to protect data on PCs, laptops, tablets, USB drives, CDs, and DVDs. • Ability to remotely lock, wipe, or kill a device. |

| FEATURE | BENEFITS |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Central administration | <ul style="list-style-type: none"> • Full control over encryption, monitoring, and data protection. • Automated policy enforcement with remediation of security events. |
| Record keeping, reports, and auditing | <ul style="list-style-type: none"> • Analyze usage statistics with scheduled reports and alert notifications. |

Management and Integration

When end-users require fortified data protection on multiple types of devices, which may require different encryption types, a centrally managed and integrated Endpoint Encryption solution reduces administration and maintenance costs. Endpoint Encryption is a centrally managed solution enabling the following data protection features:

- Centrally and transparently update the Endpoint Encryption clients when new versions are released
- Administer and leverage security policies to individuals and groups from a single policy server
- Control password strength and regularity for password changes
- Update security policies in real-time, before authentication, to revoke user credentials before booting the operating system

Understanding Encryption

Encryption is the process of making data unreadable unless there is access to the encryption key. Encryption can be performed via software or hardware (or a combination of the two) to ensure that data is protected locally on a device, on removable media, on specific files and folders, and on data in transit across networks or

the Internet. Endpoint encryption is the most important way to assure data security and to ensure that regulatory compliance mandates for data protection are met.

File Encryption

FileArmor protects individual files and folders on local hard drives, and removable media devices (USB drives). Administrators can set policies specifying which folders and drives are encrypted on the device and policies about encrypted data on removable media. File and folder encryption is performed after authentication takes place.

FileArmor can also protect different files with different keys, allowing Administrators to set access policies to a device and separate policies for access to certain files. This is useful in environments where multiple users access one endpoint.

Full Disk Encryption

Full disk encryption is the most common encryption solution deployed to endpoints today because it protects all drive data, including operating system, program, temporary, and end-user files. Many full disk encryption applications also enhance operating system security by requiring the user to authenticate before booting/unlocking the drive and providing access to the operating system.

As an encryption solution, Trend Micro Full Disk Encryption offers both software-based and hardware-based encryption. While hardware-based encryption is simpler to deploy on new hardware, easier to maintain, and offers a higher level of performance, software-based encryption does not require any hardware and is cheaper to deploy to existing endpoints. Trend Micro PolicyServer is able to centrally administer Full Disk Encryption, providing organizations with flexibility to use either software-based or hardware-based encrypted devices as needed.

Unique to Endpoint Encryption is a network-aware feature that updates policies in real-time prior to allowing authentication. Endpoint Encryption also enables administrators to lock or wipe a drive before the operating system (and any sensitive data) can be accessed.

Key Management

Unmanaged encryption products require Administrators or users to keep track of the encryption key on a USB device. Endpoint Encryption secures and escrows encryption keys transparently while enabling an Administrator to use a key to log on the protected device to recover protected data.

KeyArmor USB drives secures data with always-on hardware encryption and embedded antivirus/anti-malware protection to meet regulatory compliance requirements and stringent government mandates. With KeyArmor, Administrators have complete visibility and control of who, when, where, and how USB drives are used in their organization.

About FIPS

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

TABLE 1-8. FIPS 140-2 Security Levels

| LEVEL | DESCRIPTION |
|---------|------------------------------------------------------------------------------------------------------|
| Level 1 | Requires all encryption components to be production grade, and absent of obvious security holes. |
| Level 2 | Includes level 1 requirements and adds physical tamper-evidence and role-based authentication. |
| Level 3 | Includes level 2 requirements and adds physical tamper-resistance and identity-based authentication. |
| Level 4 | Includes level 3 requirements and adds additional physical security requirements. |

Endpoint Encryption ensures end-to-end data protection by providing FIPS 140-2 level encryption of data residing on the PolicyServer; all data transmitted between PolicyServer and endpoint clients; all data stored on the endpoint device; and, all locally stored client logs.

Chapter 2

Deployment Considerations

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.

This chapter covers the following topics:

- *Supported Platforms and Pre-deployment Checklist on page 2-3*
- *Initial Deployment Questions on page 2-5*
- *Assigning a Project Team on page 2-7*
- *Security Infrastructure Checklist on page 2-7*
- *Establishing Policy and Security Profiles on page 2-8*
- *The Importance of a Pilot Program on page 2-8*

- *Change Management Considerations on page 2-9*
- *End-user Communication on page 2-9*
- *Scaling: PolicyServer and SQL Database Requirements on page 2-11*


Supported Platforms and Pre-deployment Checklist

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

TABLE 2-1. PolicyServer 3.1.3

| SUPPORT PLATFORMS | PRE-DEPLOYMENT CHECKLIST |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows Server 2003 (32/64-bit) | <ul style="list-style-type: none"> Verify Microsoft .NET 2.0 SP2 or later is installed on the host machine |
| Windows Server 2008/2008 R2 (64-bit) | <ul style="list-style-type: none"> Use an admin account to install PolicyServer MMC To authenticate to the MMC, connectivity with PolicyServer is required |

TABLE 2-2. Full Disk Encryption

| SUPPORT PLATFORMS | PRE-DEPLOYMENT CHECKLIST |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows 8™ (32/64-bit) | <ul style="list-style-type: none"> UEFI-compatible devices must set BIOS boot priority to Legacy first instead of UEFI first. Verify that Microsoft .Net 3.5 is enabled Run scandisk and defrag prior to installation Confirm standard boot sector MBR 20% free disk space Back up user data <hr/> <p> Note Full Disk Encryption for Windows 8 does not support RAID, SCSI, eDrive, or OPAL 2 drives.</p> |


| SUPPORT PLATFORMS | PRE-DEPLOYMENT CHECKLIST |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows 7™ (32/64-bit) | <ul style="list-style-type: none"> • Verify Microsoft .NET 2.0 SP1 or later is installed • Windows Installer version 3.1 • If managed, connectivity to PolicyServer • Run scandisk and defrag prior to installation • Confirm standard boot sector MBR • 20% free disk space • Back up user data |
| Windows Vista™ with SP1 (32/64-bit) | |
| Windows XP™ with SP3 (32-bit) | |
| |  Note Full Disk Encryption does not support RAID or SCSI drives. |

TABLE 2-3. FileArmor 3.1.3

| SUPPORT PLATFORMS | PRE-DEPLOYMENT CHECKLIST |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows 8™ (32/64-bit) | <ul style="list-style-type: none"> • UEFI-compatible devices must set BIOS boot priority to Legacy first instead of UEFI first. • Verify that Microsoft .Net 3.5 is enabled |
| Windows 7™ (32/64-bit) | |
| Windows Vista™ with SP1 (32/64-bit) | <ul style="list-style-type: none"> • Verify Microsoft.NET 2.0 SP1 or later is installed |
| Windows XP™ with SP3 (32-bit) | |

TABLE 2-4. KeyArmor

| SUPPORT PLATFORMS | PRE-DEPLOYMENT CHECKLIST |
|------------------------|---------------------------------------------------------------------------------|
| Windows 8™ (32/64-bit) | <ul style="list-style-type: none"> • Windows 8 is not supported. |

| SUPPORT PLATFORMS | PRE-DEPLOYMENT CHECKLIST |
|-------------------------------------|---------------------------------------------------------------------------|
| Windows 7™ (32/64-bit) | <ul style="list-style-type: none"> • USB port is available |
| Windows Vista™ with SP1 (32/64-bit) | |
| Windows XP™ with SP3 (32-bit) | |

Initial Deployment Questions

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

End-users:

1. What is the total number of users to be deployed?
2. Of that number, how many are:
 - Enterprise Administrators
 - Group Administrators
 - Authenticators (Help Desk Personnel)
 - End Users

Endpoint devices:

1. Is there a standard number of partitions on hardware?
2. Do devices have multiple physical hard drives?
3. Do any devices have dual boot managers?
4. What standard software is installed? Check the following:
 - a. Antivirus

- b. Security applications that block software installs
- c. Previous encryption products

Enterprise networks and databases:

1. How many PolicyServers will be required to support the user base?
 - a. Estimate maximum number of users in three years.
 - b. If domain authentication is used, one PolicyServer is required for each Active Directory domain.
2. Is load balancing on the servers required?
 - a. Load-balancing is recommended for installations that require redundancy and high-availability for PolicyServers.
 - b. Clustering can be used to provide redundancy and high-availability for the database servers.
3. What are the database size estimates?
 - a. Estimate maximum number of users in three years.
 - b. Approximate space required is 1GB per year for every 1,000 end-users.
4. Will endpoint clients be required to communicate with PolicyServer over the Internet?
 - a. Check with internal network/security team to understand requirements to make a web server available on the Internet.
 - b. The following are fully supported with an external facing PolicyServer:
 - Domain authentication/single sign-on can be used over the Internet
 - Policy updates via the Internet
 - Device auditing via the Internet
 - Online password resets

Assigning a Project Team

A successful implementation of any product includes maintaining continuity as well as achieving buy-in from internal users. Structuring the team to include one or more strategic members from the departments impacted by the software deployment can help achieve buy-in and results in stronger project team leadership. At a minimum, it is recommended your project team include one or more members from each of the following groups:

- Executive Management
- Enterprise Application Servers
- Enterprise Database Administrators
- Data Security
- Desktop Support
- Disaster Recovery

Security Infrastructure Checklist

Review existing security infrastructure before deploying a new IT service into the production environment. Trend Micro provides a Security Infrastructure Checklist that contains the items that should be reviewed for the following areas:

- End User
- Incident Response
- Risk Assessment
- Human Resources
- Compliance

See [Security Infrastructure Checklist on page B-1](#) for additional details.

Establishing Policy and Security Profiles

Trend Micro Endpoint Encryption established default security policies that should be reviewed based on deployment and protection objectives. There are default policies for user name, password complexity and change requirements, device control, policy synchronization, device lock, and device wipe, among other default policy settings. Default policies can easily be changed depending upon security objectives and regulatory compliance mandates for data protection.

When using Endpoint Encryption to control the use of USB media and removable media, advance decisions should be made on which USB media are allowed, when they can be used, and where they can be used (on or off network; any time) to ensure users are compliant with your security policies and objectives.

Refer to the Administrator's Guide for a complete description of policies, default values, and configurable options.



Note

When using Endpoint Encryption to manage policies and removable media:

- Test and validate policies templates before distributing.
 - Decide which USB devices are allowed for USB drives and removable media, when they can be used, and where they can be used (on-network, off-network, or both) to ensure users are compliant.
-

The Importance of a Pilot Program

Trend Micro recommends running a pilot program and performing a test deployment to a small group of users before deploying to a larger audience. A pilot program allows an organization to finalize the deployment methodology to be used when installing Endpoint Encryption. The most effective pilot programs involve different departments, target users, and devices. For example, if the organization supports ten different laptops manufacturers, then each of those devices should be included in the pilot. Similarly, if certain high-profile groups are of particular concern, one or two members of the group(s) should be enlisted to participate in the pilot.

See *Endpoint Encryption Pilot Checklist on page A-1* for details.

Change Management Considerations

PolicyServer and related databases are mission critical services. Change management considerations are important to ensure availability for end-users attempting to authenticate on the network at all times. When changes are necessary:

- Actively monitor CPU usage and establish a threshold for when the PolicyServer Windows Service should be restarted.
- Regularly restart the service on a schedule that fits with the organization's established maintenance windows (daily, weekly, monthly).
- Restart PolicyServer Windows service whenever maintenance is performed on the Active Directory environment, the server, database, or related communications.
- Regularly back up PolicyServer databases, similar to any enterprise critical databases.
- Primary and log databases with off-site storage nightly back up is recommended.



WARNING!

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

End-user Communication

End-users must be forewarned with a smart communication plan to limit the impact and make the transition easier. In addition, post-deployment communication plays an important role in easing the adjustment to using Trend Micro Endpoint Encryption.

Questions to Answer

A common barrier to enterprise adoption is lack of communication. The need for clear end-user communication that addresses three questions is essential to a successful implementation:

1. Why do we need Endpoint Encryption?
2. How does Endpoint Encryption help me and the organization?
3. What will change?

Implement a Phased Rollout Strategy

If your pilot program was successful, start deploying the program by targeting batches of 25-50 endpoint clients to begin production distribution of the solution. Ensure that the deployment engineers are on-site with the first deployment group the day after the new solution is installed so immediate assistance can be provided. After building upon the success of the initial batch of endpoint clients, deploy 100-200 a night. As your deployment methodology is further validated in your production environment and as your internal IT and Help Desk teams agree, thousands of devices can be targeted at a time for deployment.

Let Users Know What, When and Why

Trend Micro recommends that the executive sponsor of the data protection project send a message to the end-users communicating the importance of the project to the company and the benefits to the users. Our knowledge base has a number of end-user communications templates that can be leveraged and customized to meet your communications needs before distributing Endpoint Encryption.

Introduce the Change

1. One month before rollout, have the executive sponsor outline why new software/hardware encryption is being introduced and how complying with the new processes will benefit the end-user as well as the company.

2. Provide a timeline of the rollout schedule to the users, what to expect after day 1, and confirm how end-users can get help with the new software.

Communicate a Week Before Rollout

1. Reiterate what changes are coming and what to expect on the day new authentication procedures are required to their PCs, mobile device, removable media.
2. Include screen captures and detailed instructions on user name, password conventions and other internal support services.

Communicate the Day Before Rollout

1. Reinforce the timing of the rollout schedule, what to expect and where to go for help.
2. Distribute cheat sheets, Help Desk info and provide the contact information for the on-site point of contact that will be available to assist users the next day.

Communicate After Rollout

1. Reiterate Help Desk info and provide the contact information for the on-site point of contact that will be available to assist users the next day.
2. Provide tools for troubleshooting assistance.

Scaling: PolicyServer and SQL Database Requirements

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

TABLE 2-5. Scaling with No Redundancy



| DEVICES | MINIMUM REQUIREMENTS | |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | POLICYSERVER FRONT-END | POLICYSERVER SQL DATABASE |
| 1,500 | <ul style="list-style-type: none"> • PolicyServer and database multi-role server • 2GHz Quad Core Core2 Intel™ Xeon™ Processors • 8GB RAM • 120GB RAID 5 hard disk drive space | <ul style="list-style-type: none"> • Installed on PolicyServer front-end host |
| 3,000 | <ul style="list-style-type: none"> • 1 PolicyServer front-end host • 2GHz Dual Quad Core Core2 Intel™ Xeon™ Processors • 4GB RAM • 40GB RAID 1 hard disk drive space | <ul style="list-style-type: none"> • 1 PolicyServer SQL database host • 2GHz Quad Core Core2 Intel™ Xeon™ Processors • 8GB RAM • 100GB RAID 5 hard disk drive space |





TABLE 2-6. Scaling with Redundancy and High-Availability

| DEVICES | MINIMUM REQUIREMENTS | |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | POLICYSERVER FRONT-END | POLICYSERVER SQL DATABASE |
| 10,000 | <ul style="list-style-type: none"> • 2 PolicyServer front-end hosts • 2GHz Dual Quad Core Core2 Intel™ Xeon™ Processors • 4GB RAM • 40GB RAID 1 hard disk drive space | <ul style="list-style-type: none"> • 1 PolicyServer SQL database hosts • 2GHz Quad Core Core2 Intel™ Xeon™ Processors • 8GB RAM • 120GB RAID 5 hard disk drive space |

| DEVICES | MINIMUM REQUIREMENTS | |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | POLICYSERVER FRONT-END | POLICYSERVER SQL DATABASE |
| 20,000 | <ul style="list-style-type: none"> • 4 PolicyServer front-end hosts • 2GHz Dual Quad Core2 Intel™ Xeon™ Processors • 4GB RAM • 40GB RAID 1 hard disk drive space | <ul style="list-style-type: none"> • 1 PolicyServer SQL database hosts • 2GHz Quad Core2 Intel™ Xeon™ Processors • 16GB RAM • 160GB RAID 5 hard disk drive space |
| 40,000 | <ul style="list-style-type: none"> • 8 PolicyServer front-end hosts • 2GHz Dual Quad Core Core2 Intel™ Xeon™ Processors • 4GB RAM • 40GB RAID 1 hard disk drive space | <ul style="list-style-type: none"> • 2 PolicyServer SQL database cluster hosts • 2GHz Quad Core Core2 Intel™ Xeon™ Processors • 16GB RAM • 320GB RAID 5 hard disk drive space |

TABLE 2-7. Scaling with Zero Single Point of Failure

| DEVICES | MINIMUM REQUIREMENTS | |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | POLICYSERVER FRONT-END | POLICYSERVER SQL DATABASE |
| 10,000 | <ul style="list-style-type: none"> • 2 PolicyServer front-end hosts • 2GHz Quad Core Core2 Intel™ Xeon™ Processors • 4GB RAM • 40GB RAID 1 hard disk drive space <hr/> <p> Note Virtualized hardware is supported under VMware Virtual Infrastructure.</p> <hr/> | <ul style="list-style-type: none"> • 2 PolicyServer SQL database hosts • 2GHz Dual Quad Core Core2 Intel™ Xeon™ Processors • 8GB RAM • 60GB RAID 5 hard disk drive space • 130GB RAID 5 shared SAN hard disk drive space <hr/> <p> Note Microsoft or VMware on virtualized hardware does not support Microsoft Cluster Service.</p> <hr/> |

| DEVICES | MINIMUM REQUIREMENTS | |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | POLICYSERVER FRONT-END | POLICYSERVER SQL DATABASE |
| 20,000 | <ul style="list-style-type: none"> 4 PolicyServer front-end hosts 2GHz Dual Quad Core Core2 Intel™ Xeon™ Processors 4GB RAM 40GB RAID 1 hard disk drive space <hr/>  Note Virtualized hardware is supported under VMware Virtual Infrastructure. | <ul style="list-style-type: none"> 2 PolicyServer SQL database hosts 2GHz Dual Quad Core Core2 Intel™ Xeon™ Processors 8GB RAM 60GB RAID 5 hard disk drive space 180GB RAID 5 shared SAN hard disk drive space <hr/>  Note Microsoft or VMware on virtualized hardware does not support Microsoft Cluster Service. |
| 40,000 | <ul style="list-style-type: none"> 8 PolicyServer front-end hosts 2GHz Dual Quad Core Core2 Intel™ Xeon™ Processors 4GB RAM 40GB RAID 1 hard disk drive space <hr/>  Note Virtualized hardware is supported under VMware Virtual Infrastructure. | <ul style="list-style-type: none"> 4 PolicyServer SQL database hosts 2GHz Dual Quad Core Core2 Intel™ Xeon™ Processors 16GB RAM 60GB RAID 5 hard disk drive space 350GB RAID 5 shared SAN hard disk drive space <hr/>  Note Microsoft or VMware on virtualized hardware does not support Microsoft Cluster Service. |

Scaling Example

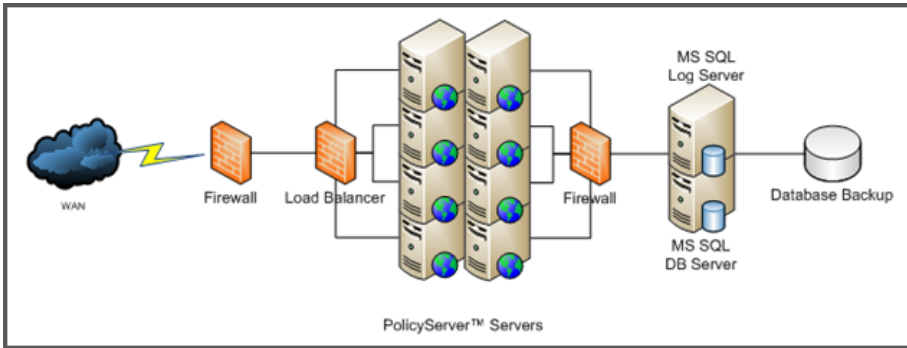


FIGURE 2-1. PolicyServer Scaled to Support 40,000 Users

Chapter 3

PolicyServer Installation

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

This chapter describes the following topics:

- *PolicyServer Requirements on page 3-3*
- *PolicyServer Installation Process on page 3-6*
- *PolicyServer AD Synchronization on page 3-12*
- *Optional LDAP Proxy on page 3-17*

Introducing PolicyServer

PolicyServer utilizes a Microsoft Management Console (MMC). PolicyServer has a hierarchical structure that distributes administrative responsibility while maintaining centralized control when:

- Defining security policy parameters
- Managing users, devices, and groups (including offline groups)
- Enabling/Disabling endpoint applications

Use PolicyServer MMC auditing and reporting functions to monitor the security infrastructure and meet compliance requirements.

Installation Folder Contents

The installation folder for Trend Micro PolicyServer contains the following installers for the Enterprise:

- PolicyServerMMCSnapinSetup.msi
- PolicyServerInstaller.exe
- LDAPProxyInstaller.exe
- Tools

The following file is also required:

- The license text file and unlock code (password) received from Trend Micro. Use the license file and unlock code to log on PolicyServer MMC for the first time.

**Note**

PolicyServer 3.1.3 includes a 30-day trial license. For more information about the trial license, see [Installing PolicyServer Database and Web Services on page 3-6](#).

PolicyServer Requirements

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

Hardware Requirements

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

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



Note

Virtualized hardware is supported under VMware Virtual Infrastructure.

TABLE 3-1. PolicyServer Hardware Requirements

| SEPARATE HOSTS | | SINGLE HOST |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| PolicyServer Host (3,000 Users) | SQL Server Host (3,000 Users) | PolicyServer and SQL Server (1,500 Users) |
| <ul style="list-style-type: none"> • 2GHz Dual Quad Core Core2 Intel™ Xeon™ Processors • 4GB RAM • 40GB hard disk space | <ul style="list-style-type: none"> • 2GHz Dual Quad Core Core2 Intel™ Xeon™ Processors • 8GB RAM • 100GB hard disk space | <ul style="list-style-type: none"> • 2GHz Quad Core Core2 Intel™ Xeon™ Processors • 8GB RAM • 120GB hard disk space |

Software Requirements

TABLE 3-2. PolicyServer Minimum Software Requirements


| FUNCTION | REQUIREMENT |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operating System | <ul style="list-style-type: none"> • Windows Server 2003 SP2 32/64-bit • Windows Server 2008 or 2008 R2 64-bit |
| Applications and Settings | <ul style="list-style-type: none"> • Application Server <ul style="list-style-type: none"> • IIS • Allow Active Server pages • Allow ASP.NET • .Net Framework 2.0 SP2 <hr/> <div style="border: 1px solid black; padding: 5px;">  Note PolicyServer 3.1.3 requires two IIS locations. The PolicyServer Administration Interface and the Client Application Interface should be installed on different IIS locations. </div> |
| Database | <ul style="list-style-type: none"> • Microsoft SQL 2005/2008/2008 R2 • Microsoft SQL Express 2005(SP3)/2008 • Mixed Mode Authentication (SA password) installed • Reporting services installed |

TABLE 3-3. Software Considerations for Windows Server 2008 and 2008 R2

| Server OS | 2008 | 2008 R2 |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Roles | <ul style="list-style-type: none"> • Install application server role • Add IIS support • Install web server role | <ul style="list-style-type: none"> • Install application server role • Add IIS support • Install web server role |

| | | |
|----------------------------|----------------|---------------------------------------------------------------------------|
| Features | • Add SMTP | • Add SMTP |
| Other Prerequisites | • .NET 3.5 SP1 | • Must install SQL 2008 SP1 to run SQL 2008 • No .NET upgrade required |

Required Installation Files

TABLE 3-4. Required Files to Install PolicyServer

| FILE | PURPOSE |
|--------------------------------|----------------------------------------------------------------------------------|
| PolicyServerInstaller.exe | Installs PolicyServer databases and services |
| PolicyServerMMCSnapinSetup.msi | Install PolicyServer management console as an MMC snap-in |
| License | Provided by Trend Micro. Required for PolicyServer MMC first-time authentication |



Important

Copy all installation files to the local drive before installation.

Required Accounts

In order to install PolicyServer, certain accounts must be available. The table below explains the account, the service it is associated with, and how PolicyServer uses the account.

TABLE 3-5. Accounts Needed to Install PolicyServer

| ACCOUNT | SERVICE | PURPOSE |
|---------|------------------------|-------------------------------------------------------------|
| SQL SA | PolicyServer Installer | Account used ONLY when creating the PolicyServer databases. |

| ACCOUNT | SERVICE | PURPOSE |
|---------------------------------------|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| SQL MADB | PolicyServer Windows Service | Account created during installation to authenticate to PolicyServer databases. |
| Service Account | PolicyServer Windows Service and IIS | Account used to run the PolicyServer Windows Service and web Service application pools. |
| PolicyServer Enterprise Administrator | PolicyServer MMC | Account provided by Trend Micro (from license file) that is required to authenticate to PolicyServer MMC for the first time. |

PolicyServer Installation Process

Install Microsoft SQL Server™ before running any PolicyServer installation file. The installers for each PolicyServer application are configured to make installation straightforward and simple.

This installation process:

1. Install the Microsoft SQL Database.



Note

This document does not explain how to install Microsoft SQL.

2. Install PolicyServer database and services.
3. Install PolicyServer MMC.

Installing PolicyServer Database and Web Services

Before you begin

Microsoft SQL Server is already set up.

The PolicyServer Installer configures database settings and installs Windows services. New to PolicyServer 3.1.3 is the ability to specify a port number for the PolicyServer Web Service. A second port is also now required for the Client Web Service. If a second port does not exist, a new port is created during the installation process. For details about the new architecture, see *Endpoint Encryption Components on page 1-2*.

In order to use Endpoint Encryption for a limited trial period, the Enterprise name and Enterprise Administrator account can be configured at the time of installation. PolicyServer functions normally with all client applications, unlimited devices, and up to 100 users for a 30-day trial period. After 30 days, contact Technical Support to receive a license file. Users and devices can still log on after the trial period expires.

Procedure

1. Run `PolicyServerInstaller.exe`.
2. Read the End User License Agreement carefully. If you agree, click **Accept**.
3. At the **PolicyServer Services** screen, verify the PolicyServer version and then click **Install**.
4. At the **Windows Service Logon** screen, the default settings are appropriate for most installations. Click **Continue**.
5. At the **Database Administrator Logon** screen, provide the Microsoft SQL Server hostname or IP address, and the credentials of an account with the sysadmin role for the specified SQL instance.



Note

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

```
<hostname or IP address>\<database instance>
```

The installer verifies the database connection.

6. At the **Create Database Logon** screen, provide the account credentials for the PolicyServer Windows Service to use for all data transactions. If this is the first time installing PolicyServer, the specified account is created.

7. At the **Web Service Install Location** screen, specify the IIS site that PolicyServer MMC and the Client Web Service will use to communicate with PolicyServer. The default port number is 8080. If port 8080 is in use, then the next available port is assigned.
 - a. Select a site from the **Target Site** drop-down.
 - b. Review the current port assigned and, if needed, specify a different port number in the **New Port** field.

**Note**

Trend Micro recommends reserving port 80 for the Client Web Service.

- c. Click **Continue**.
8. This next step is designed to configure the Client Web Service, which is the IIS site that all Endpoint Encryption clients use to communicate with PolicyServer. Depending on whether a second IIS location is available, one of the following screens display:
 - If a second IIS site is available, the **Client Web Service Location** screen displays.
 - a. Select a site from the **Target Site** drop-down.
 - b. Review the default port assignment for the Client Web Service.

**Note**

Trend Micro recommends maintaining port number 80. However, if needed, specify a different port number in the **New Port** field. The port number must be a positive integer between 1 and 65535.

- c. Click **Continue**.
- If a second IIS site is unavailable, the **Create Client Web Service Location** screen displays to configure a new IIS location.
 - a. Specify a name for the IIS location in the **Site Name** field.
 - b. Browse to the site location. If a folder does not yet exist, create a new one.

- c. Specify the IP address and port number for the new IIS location.

**Note**

Trend Micro recommends maintaining port number 80. However, if needed, specify a different port number. The port number must be a positive integer between 1 and 65535.

- d. Click **Continue**.
9. At the **Mobile Web Service Install Location** screen, review the settings and then click **Continue**.
 10. At the **Create Enterprise Name and Administrator Logon** screen, specify the new Enterprise name and the credentials for a new Enterprise Administrator account used to manage PolicyServer during the initial trial period.
 11. Click **Continue**.
The installation process begins.
 12. At the **PolicyServer Installation** message, click **OK**.
 13. Click **Finished**.
 14. From the PolicyServer Installer window, click **Exit**.
 15. Restart the server.
-

PolicyServer MMC

The PolicyServer Microsoft Management Console (MMC) is how Administrators interface with PolicyServer. The PolicyServer MMC combines a hierarchical structure with separate Administrator and authenticator roles, which allows organizations to distribute administrative responsibility while maintaining central control.

PolicyServer MMC manages:

- All Trend Micro Endpoint Encryption Applications
- PolicyServer Users and Groups (including offline groups)

- Client devices including laptops, desktops, PDAs, smartphones, and USB storage devices
- All policies including encryption, password complexity and authentication
- Event logs for viewing authentication events, management events, device encryption status, and security violations
- Remote Help password reset process
- Device lock/kill functionality

In addition, PolicyServer offers measurable benefits through its auditing and reporting options, allowing company executives and others to gauge success.

For a detailed description of PolicyServer MMC functionality, see the Endpoint Encryption Administrator's Guide.

Installing PolicyServer MMC

Procedure

1. Run `PolicyServerMMCSnapinSetup.msi`.

The installation begins.

2. Click **Next** to begin the Welcome to PolicyServer MMC Setup Wizard.
3. Carefully read the license agreement, select **I Agree** if you agree to the terms, and then click **Next**.
4. Select installation folder or leave at default location, and click **Next**.
5. Click **Next** to confirm installation.

The installation process begins. A new PolicyServer MMC shortcut is created on the desktop.

6. Click **Close** to complete installation.
7. Click **Yes** to restart the server.

8. After logging back on the server, open PolicyServer MMC from the desktop shortcut.
9. Once PolicyServer MMC opens, do one of the following:
 - Log on using the Enterprise and Enterprise Administrator account created when the PolicyServer databases and services were installed. The 30-day trial period allows for unlimited devices and up to 100 users.
 - Import a license file:

**Note**

To obtain the license file, contact Trend Micro Support.

- a. Go to **File > Import License**.
- b. Specify the unlock code, browse to the license file, and then click **Update**.
- c. Click **OK** when the **License updated successfully** window appears.

PolicyServer installation complete. Authenticate to PolicyServer MMC using the enterprise Administrator credentials sent to you by Trend Micro.

What to do next

1. Create a backup Enterprise Administrator account and change the default password.
2. Enable all applications that will be used at the enterprise level prior to creating any test or production deployment groups.
3. See the Endpoint Encryption Administrator's Guide for additional post-installation tasks such as creating devices and users, and setting policies.

PolicyServer AD Synchronization

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

Active Directory Overview

Three components are required to enable PolicyServer AD Synchronization:

1. A configured AD domain.
2. A PolicyServer group configured to point to a valid AD Organizational Unit (OU).
3. Appropriate credentials to access the AD domain that match the PolicyServer group's Distinguished Name.

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

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

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

PolicyServer Administrators may create their own users to add them to paired PolicyServer groups without having those users modified by the synchronization system. This allows Administrators to add non-domain users to groups that are synchronized with the domain.

If a PolicyServer Administrator removes a user from a paired group on the PolicyServer manually that domain user will not be re-added by the synchronization system automatically. This prevents overriding the Administrator's action for this user. If an Administrator manually moves a synchronized domain user back into a paired group

then the synchronization system will again begin to maintain the user in the group automatically.

Configuring Active Directory

This task assumes the domain controller is setup on Windows Server 2003 and that AD is installed.

Procedure

1. Go to **Start > Programs > Administrative Tools > AD Users and Devices**.

Active Directory Users and Computer opens.

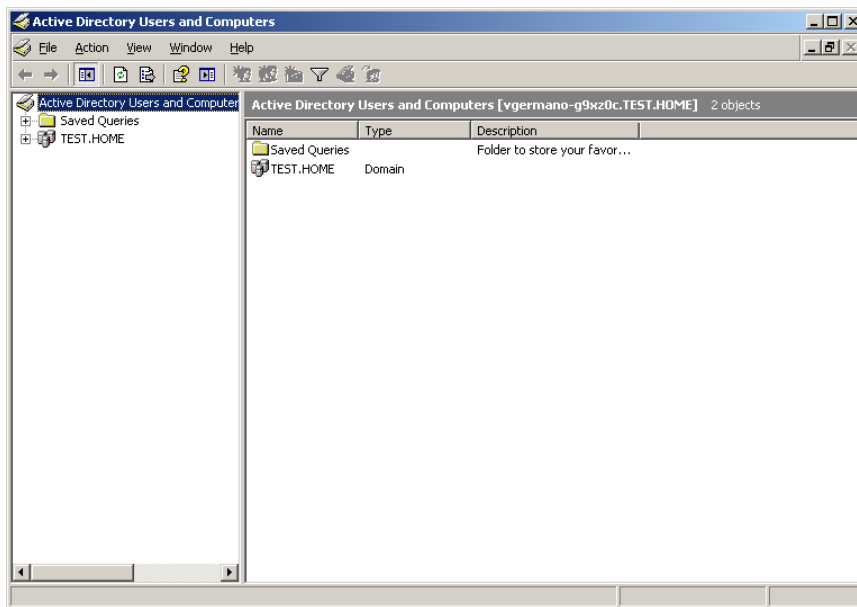


FIGURE 3-1. Active Directory Users and Computers

2. Right-click the new domain created when AD was installed and then select **New**.
3. Select **Organizational Unit**.

4. Click **Next**.
5. From the **New Object - Organizational Unit** screen, specify the new name and click **OK**.

The new group appears in the left navigation under the domain.

The new group will be used to sync with a PolicyServer group but first users must be added to the group.

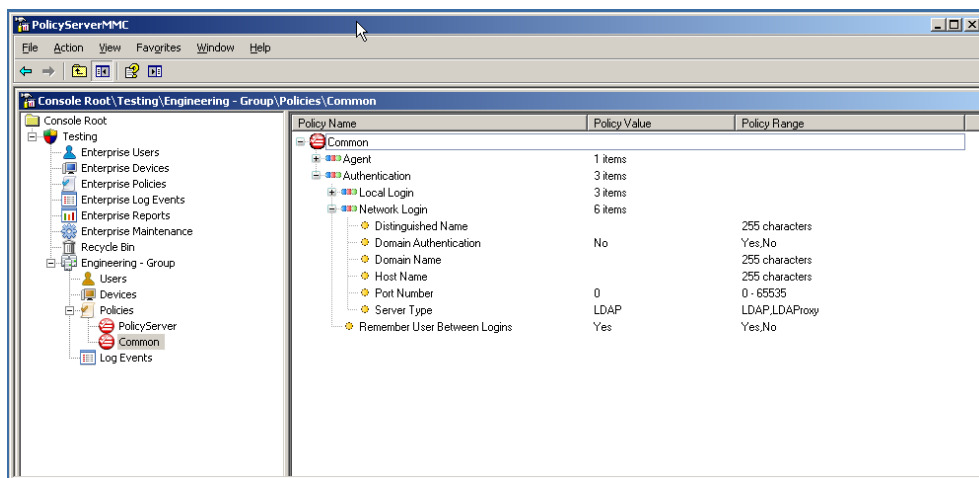
6. Right-click the new group and select **NewUser**.
7. From the **New Object - User** screen, specify the new user's account information and click **Next**.
8. Specify and confirm the new user's domain password, and click **Next** to continue

**Note**

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

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

The domain controller is configured with an new organizational unit and a user in that group. To sync that group with PolicyServer, install PolicyServer and create a group for synchronization. This next section assumes that PolicyServer is already installed.
10. Log on PolicyServer MMC.
11. Right-click the enterprise and select **Create Top level Group**.
12. Specify the name and description for the group and then click **Apply**.
13. To configure the synchronization policy, open the group and go to **Common > Authentication > Network Login**.



- Open **Distinguished Name** and specify the fully qualified Distinguished Name from the configured AD organization to sync with this group and click **OK**.



Note

The format for the Distinguished Name for an organizational unit named Engineering on domain named test.home is:
 OU=Engineering,DC=TEST,DC=HOME

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

Once PolicyServer policy is configured the final configuration required is to create the synchronization configuration via the AD Synchronization Configuration tool. This tool allows Administrators to create separate AD credentials for each synchronized organizational unit and each domain controller.

- To access the **AD Synchronization Configuration** tool, go to the Policy Server installation folder and open **ADSyncConfiguration.exe**

PolicyServer - AD Synchronization tool opens

Optional LDAP Proxy

The optional LDAP Proxy allows domain authentication/Single Sign-On (SSO) through an external proxy server located in the customer DMZ.



Note

- The LDAP Proxy installation is required for hosted environments using domain authentication/SSO.
- LDAP Proxy versions earlier than 3.1 are no longer supported.
- Existing customers utilizing the LDAP Proxy must upgrade to version 3.1.

LDAP Requirements

TABLE 3-6. LDAP Hardware and Software Specifications

| ITEM | REQUIREMENT |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Processor | Intel™ Core™ 2 or compatible processor. |
| Memory | <ul style="list-style-type: none"> • Minimum: 2GB |
| Disk space | <ul style="list-style-type: none"> • Minimum: 30GB • Required: 20% free disk space |
| Network connectivity | <ul style="list-style-type: none"> • Server must be on the domain with access to AD • Server must have an address accessible through the Internet • Incoming proxy must be allowed • PolicyServer must have access to this server's IIS server |
| Operating systems | <ul style="list-style-type: none"> • Windows Server 2003 32/64-bit • Windows Server 2008 or 2008 R2 32/64-bit |

| ITEM | REQUIREMENT |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Applications and settings | <ul style="list-style-type: none"> • Application Server role <ul style="list-style-type: none"> • IIS • Allow Active Server pages • Allow ASP.NET • .Net Framework 2.0 SP2 |

LDAP Proxy Hardware Checklist

TABLE 3-7. LDAP Proxy Hardware Checklist

| LDAP PROXY SERVER | | COMMENTS |
|----------------------------|---------------------------------------------|----------|
| Windows Server Information | OS Version | |
| | Service Pack Level | |
| Hardware Information | Make | |
| | RAM | |
| | Model | |
| | CPU | |
| Server Installed Software | IIS | |
| | Microsoft .NET SP 2.0 Sp1 or later | |
| Network Information | IP Address | |
| | Subnet Mask | |
| | Host Name | |
| | Domain Name | |
| | Domain Credentials Available (for SSO only) | |

Chapter 4

Endpoint Encryption Client Installation

Each Endpoint Encryption application has unique installation and system requirements. For detailed endpoint application explanations about configuration and usage, see the Endpoint Encryption Administrator's Guide.

This chapter explains the following topics:

- *Pre-installation Considerations on page 4-2*
- *Supported Platforms and Pre-deployment Checklist on page 2-3*
- *Installing Full Disk Encryption on page 4-2*
- *Installing FileArmor on page 4-12*
- *KeyArmor on page 4-16*

Pre-installation Considerations

Before proceeding, note the following:

- Copy all endpoint client installation files to the device.
- All endpoint client applications require Microsoft .NET Framework 2.0 SP1 or later.



Note

To install endpoint clients on Windows 8, Microsoft .NET Framework 3.5 compatibility is required.

- Full Disk Encryption and FileArmor installations can be automated.
- Administrative privileges are needed for all product installations.

For details about supported platforms and other pre-deployment considerations, see [Supported Platforms and Pre-deployment Checklist on page 2-3](#).

Installing Full Disk Encryption

Full Disk Encryption is designed to provide comprehensive endpoint data security by providing mandatory strong authentication and full disk encryption. Full Disk Encryption secures not only the data files, but also all applications, registry settings, temporary files, swap files, print spoolers, and deleted files. Strong preboot authentication restricts access to the vulnerable host operating system until the user is validated.

Pre-deployment Options

To minimize end-user impact and simplify mass deployment, temporarily disable drive encryption. Once compatibility is confirmed, encryption can be re-enabled as part of the standard product roll-out.

TABLE 4-1. Enable/Disable Device Encryption

| CONFIGURATION SETTING | OPTIONS | POLICYSERVER PATH |
|-----------------------|---------|-------------------------------------------------------------------------|
| Device encryption | Yes/No | Full Disk Encryption > PC > Encryption > Encrypt Device |

Pre-installation Checklist

The Full Disk Encryption installer checks the target system to make sure that all necessary system requirements are met before installing the application. For additional information, see the `PreInstallCheckReport.txt` file located in the installation directory after the installer runs.


For detailed information about the system check and requirements, see [Full Disk Encryption Pre-installation Checklist on page C-1](#)

Full Disk Encryption System Requirements

This section describes the minimum and recommended system requirements necessary to install Full Disk Encryption.

TABLE 4-2. Full Disk Encryption System Requirements

| ITEM | REQUIREMENT |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Processor | Intel™ Core™ 2 or compatible processor. |
| Memory | <ul style="list-style-type: none"> • Minimum: 1GB |
| Disk space | <ul style="list-style-type: none"> • Minimum: 30GB • Required: 20% free disk space • Required: 256MB contiguous free space |
| Network connectivity | Communication with PolicyServer 3.1.3 required for managed installations |

| ITEM | REQUIREMENT |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operating Systems | <ul style="list-style-type: none"> • Windows 8™ (32/64-bit) • Windows 7™ (32/64-bit) • Windows Vista™ with SP1 (32/64-bit) • Windows XP™ with SP3 (32-bit) |
| Other software | <p>Additional requirements Windows 8:</p> <ul style="list-style-type: none"> • Microsoft .NET Framework 3.5 is enabled • For devices with UEFI, see Preparing the Device on page 4-5 to change the boot priority. <p>Additional requirements for Windows XP:</p> <ul style="list-style-type: none"> • Microsoft .NET Framework 2.0 SP1 or later • Microsoft Windows Installer 3.1 |
| Hard disk | <ul style="list-style-type: none"> • Seagate DriveTrust drives • Seagate OPAL and OPAL 2 drives <hr/> <p> Note</p> <ul style="list-style-type: none"> • RAID and SCSI disks are not supported. • Full Disk Encryption for Windows 8 does not support RAID, SCSI, eDrive, or OPAL 2 drives. |
| Other hardware | ATA, AHCI, or IRRT hard disk controller |

Hard Disk Drive Preparation

Full Disk Encryption encrypts every sector on the physical drive. Since many applications, including the operating system, do not utilize the entire physical hard disk space, sectors may be damaged or the drive may be extremely fragmented.

**Note**

Trend Micro recommends doing a small pilot of fresh installs and upgrades before deploying the latest Full Disk Encryption build. If you have questions or require technical assistance, contact Trend Micro Support.

Preparing the Device

Procedure

1. Disconnect all USB store devices. You can reconnect them after installation.
 2. Make sure that the drive with the operating system is not already encrypted and BitLocker is turned off.
 3. For Windows 8 devices that support UEFI BIOS, change the boot priority to **Legacy First**.
 - a. From Windows 8, hold SHIFT and restart the device.

The device restarts and UEFI BIOS loads.
 - b. Click the **Troubleshoot** tile.

The **Advanced options** screen appears.
 - c. Click the **UEFI Firmware Settings** tile.

If the **UEFI Firmware Setting** tile does not exist, the device does not use UEFI and no change is required.
 - d. Set **UEFI/Legacy Boot Priority** to **Legacy First**.
 - e. Restart the device.
-

Preparing the Drive

Procedure

1. Run Windows defragment utility on the system drive.
2. Verify that the system drive has at least 256MB of contiguous free space.
3. Run the Windows disk integrity utility (requires a reboot).
 - a. Using a script or command prompt, run `chkdsk /f /r` and schedule to check disk after the next system restart.
 - b. Reboot device.
 - c. Replace the drive if `chkdsk` reports multiple bad sectors.
4. Check the disk for a normal Master Boot Record (MBR) and confirm that a normal boot sector is present on the boot partition. For example, a dual boot machine has a modified boot sector.



Note

GPT is not currently supported.

5. Copy the Full Disk Encryption installation software to the Windows system drive.
-

Important Notes for DataArmor SP7 and below

- SP6 and earlier:
 - In the BIOS verify the disk controller is set to ATA or AHCI mode.
 - For docked laptops, install software while undocked from a multi-bay.
- Intel™ Rapid Recovery Technology (IRRT):
 - Some newer systems support IRRT in the BIOS.
 - If the BIOS disk controller is set to IRRT mode, it will need to be changed to AHCI mode prior to Full Disk Encryption installation.

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

**Note**

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

Full Disk Encryption Installation

This section describes how to install Full Disk Encryption on Windows.

Installation Types

Full Disk Encryption can be installed as either managed or unmanaged, depending on the particular enterprise needs.

| TYPE | DETAILS |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Managed | <ul style="list-style-type: none"> • Authentication and encryption policies are managed by PolicyServer. • Most common installation type for devices normally connected to PolicyServer. |
| Unmanaged | <ul style="list-style-type: none"> • Authentication and encryption policies are managed directly within Full Disk Encryption and Recovery Console. • Suitable for devices that are not centrally managed by PolicyServer. |

Installation Options

Install Full Disk Encryption manually or build scripts to automate installation tasks.

TABLE 4-3. Full Disk Encryption Installation Options

| OPTION | DETAILS |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Automated | <ul style="list-style-type: none"> • Requires system management software: Tivoli, SCCM/SMS or LANDesk, and an installation script. • Recommended method for enterprises with a large number of endpoints. |
| Manual | <ul style="list-style-type: none"> • Simple installation directly from Windows, either by the graphical installer or command line. • Suitable for small companies, test deployments, or individual installations. |

Automated Installation

Installing Full Disk Encryption using scripts automates the process and makes it easier to distribute the software across an enterprise. See [Using Scripts to Automate Installations on page 4-19](#) for details.

Managed Installation

A managed Full Disk Encryption installation is the most common installation type for devices normally connected to PolicyServer. Authentication and encryption policies are managed by PolicyServer. This section outlines the basic installation steps for a managed endpoint client.

Before continuing, be sure to:

- Review the [Full Disk Encryption System Requirements on page 4-3](#)
- Check the [Hard Disk Drive Preparation on page 4-4](#)

**WARNING!**

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

Requirements

The following are required for managed installations:

- Client is connected to PolicyServer during installation.
- PolicyServer must be configured with an enterprise, host name, and IP address.

**Note**

Trend Micro recommends using the fully qualified domain name of PolicyServer. If the PolicyServer IP address or host name changes, then each client does not need to be manually updated.

- The user account must belong to a PolicyServer group and have permission to add devices to this group.

**WARNING!**

PolicyServer Enterprise Administrator/Authenticator accounts cannot be used to install Full Disk Encryption.

- The installing account must have local Administrator privileges.
- If domain authentication/Single Sign-on is enabled, the user name must match Active Directory. The Active Directory password is used instead.

Installing Full Disk Encryption as a Managed Client

Review the system requirements before installing Full Disk Encryption as a managed client. For details, see [Full Disk Encryption System Requirements on page 4-3](#). After Full Disk Encryption is installed, the computer restarts for software-based encryption or shuts down for hardware-based encryption.

**Note**

The installing user cannot be an Enterprise Administrator/Authenticator account.

Procedure

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

**Note**

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

The installation welcome window appears.

3. Select **Managed installation** and click **Next**.

Managed Installation screen displays.

4. Specify the user account credentials, PolicyServer address, and enterprise, then click **Next**.

Full Disk Encryption installation begins. The program closes after installation completes, which may take several minutes.

**Tip**

If the managed installation fails, use the Device ID located at the bottom-right of the installer screen to check whether the device already exists in PolicyServer. The Device ID only displays after an installation failure has occurred.



5. At the confirmation screen, click **Yes** to restart/shutdown the device.

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

What to do next

When Full Disk Encryption Preboot loads, the user must log on before gaining access to Windows. If the policy is set, he/she may be required to change the password after logging on.

Unmanaged Installation

An unmanaged Full Disk Encryption installation is similar to a managed installation except the user credentials and policies are only for the client device.

Installing Full Disk Encryption as a Unmanaged Client

Review the system requirements before installing Full Disk Encryption as a managed client. For details, see [Full Disk Encryption System Requirements on page 4-3](#). After Full Disk Encryption is installed, the computer restarts for software-based encryption or shuts down for hardware-based encryption.

Procedure

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



Note

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

The installation welcome window appears.

3. Select **Unmanaged installation** and click **Next**.

Unmanaged Installation screen displays.

4. Specify the user name and password for a new account to use when logging on the unmanaged client, and then click **Next**.

The installation begins.

5. At the **Installation Complete** screen, click **Close**.
6. At the confirmation screen, click **Yes** to restart/shutdown the device.

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

What to do next

When Full Disk Encryption Preboot loads, the user must log on before gaining access to Windows.

Installing FileArmor

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

FileArmor Deployment Outline

Procedure

1. Enable FileArmor in PolicyServer MMC.
2. Configure FileArmor Policies:
 - a. Encryption Key Used
 - b. Folders to Encrypt
 - c. Use of Removable Media
 - d. Authentication Method
3. Set up groups and users.

4. Create and test installation package.
5. Verify policy settings are enforced as defined.
6. Prepare end-user communications.

Required FileArmor Policy Settings

Procedure

1. The most important pre-deployment decision for FileArmor is to select the proper encryption key:
 - **User key:** Only the user can access the encrypted file.
 - **Group key:** All users within the policy group can access the file.
 - **Enterprise key:** All users within all groups can access the file.
2. The second decision is related to FileArmor removable media policies. All policies are located at: **FileArmor > Encryption > Removable Media**.

TABLE 4-4. FileArmor Policies to Configure

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

3. Decide whether to use FileArmor to automatically encrypt folders on the host device. Files copied to a secure folder are automatically encrypted. By default, a FileArmor encrypted folder is created on the desktop.
 - Use **Encryption > Specify Folders To Encrypt** to create secure folders on the host device.

- Use **Encryption > Removable Media > Folders To Encrypt On Removable Media** to create secure folders on a USB storage device.

FileArmor Installation

FileArmor may be installed using any of the following methods:

- Using an automation tool such as Microsoft SCCM or SMS
- Manually on a local machine

FileArmor System Requirements

TABLE 4-5. FileArmor System Requirements

| ITEM | REQUIREMENT |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Processor | Intel™ Core™2 or compatible processor. |
| Memory | <ul style="list-style-type: none"> • Minimum: 512MB • Recommended: 1GB |
| Disk space | <ul style="list-style-type: none"> • Minimum: 2GB • Required: 20% free disk space |
| Network connectivity | Communication with PolicyServer required for managed installations |
| Operating Systems | <ul style="list-style-type: none"> • Windows 8™ (32/64-bit) • Windows 7™ (32/64-bit) • Windows Vista™ with SP1 (32/64-bit) • Windows XP™ with SP3 (32-bit) |

| ITEM | REQUIREMENT |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Other software | <p>Additional requirements for Windows 8:</p> <ul style="list-style-type: none"> • Microsoft .NET Framework 3.5 is enabled • For devices with UEFI, see Preparing the Device on page 4-5 to change the boot priority. <p>Additional requirements for Windows XP:</p> <ul style="list-style-type: none"> • Microsoft .NET Framework 2.0 SP1 or later • Microsoft Windows Installer 3.1 |

Other Requirements

- The installing user must have Administrator rights on the device.
- Copy and run the installation package locally.
- Set a fixed password for all PolicyServer Users.
- The user account must belong to a PolicyServer group and have permission to add devices to this group.



Note

PolicyServer Enterprise Administrator/Authenticator accounts cannot be used to install FileArmor.

FileArmor Manual Installation

The manual installation process involves running an installer on the client and following the step-by-step instructions. FileArmor can be installed by PolicyServer Group Administrators, Authenticators, or standard users.

Procedure

1. Run `FASetup.msi` for 32-bit OS or `FASetup(x64).msi` for 64-bit OS.

The FileArmor Setup Wizard to begin the FileArmor installation process

2. Click **Next**.



Note

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

3. When the installation completes, click **Close**.
4. Click **Yes** to restart Windows.

After the device restarts, FileArmor software is installed and two FileArmor icons display - one shortcut on the desktop and one tray icon.

FileArmor Automated Installation

Installing FileArmor using scripts automates the process and makes it easier to distribute the software across an enterprise. See [Using Scripts to Automate Installations on page 4-19](#) for details.

KeyArmor

KeyArmor USB drives secures data with always-on hardware encryption and embedded antivirus/anti-malware protection to meet regulatory compliance requirements and stringent government mandates. With KeyArmor, Administrators have complete visibility and control of who, when, where, and how USB drives are used in their organization.

KeyArmor System Requirements

The following table explains the minimum requirements to use KeyArmor protected USB removable media.

TABLE 4-6. KeyArmor System Requirements

| ITEM | REQUIREMENT |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hardware | USB 2.0 port |
| Network connectivity | Communication with PolicyServer required for managed installations |
| Operating Systems | <ul style="list-style-type: none"> Windows 7™ (32/64-bit) Windows Vista™ with SP1 (32/64-bit) Windows XP™ with SP3 (32-bit) |
| Other software | Additional software required when installing on Windows XP™: <ul style="list-style-type: none"> Microsoft .NET Framework 2.0 SP1 or later |

Device Components

KeyArmor mounts two drives when the device is inserted in a USB port.

**FIGURE 4-1. KeyArmor Devices**

- **KeyArmor (E:)** contains the KeyArmor program files.
- **SECURE DATA (F:)** is KeyArmor user storage. KeyArmor encrypts all files stored in this drive.

KeyArmor Deployment Outline

Similar to Full Disk Encryption and FileArmor, the deployment outline for KeyArmor is as follows:

1. Enable KeyArmor in PolicyServer.
2. Configure applicable policies for KeyArmor :
 - Authentication Method
 - Must be Connected to Server
 - One User Per Device
 - Failed Login Action
 - Antivirus Update Options
3. Set up users and groups.
4. Prepare device authentication and passwords.
5. Prepare end-user communications.

KeyArmor End-user Guidelines

- If the device is plugged into a USB 2.0 port, Windows automatically detects and configures the device.
- When receiving a new device, end-users must complete a one-time set up process.
- Ongoing use requires nothing more than a valid user name and a password.
- KeyArmor automatically encrypts all files stored to the KeyArmor device.
- Opening, viewing, moving or copying files to a host device is a user initiated activity that can only be completed after proper authentication to the KeyArmor device.

Protecting KeyArmor Files

- Files and folders saved to KeyArmor are automatically encrypted and accessible only by a person who logs on to the device with a valid user name and password.
- Files remain encrypted as long as they are stored on KeyArmor.

- To ensure the latest antivirus definitions, Trend Micro recommends not copying any files to the KeyArmor device until the initial antivirus updates are complete.

**WARNING!**

Always follow the process to safely remove KeyArmor devices:

1. Choose **Log out** from the KeyArmor application.
2. Right-click the KeyArmor tray icon and select **Log out**.

Safely removing a KeyArmor device can prevent premature wear and data loss.

Using Scripts to Automate Installations

Scripting installations is most common for large deployments using automated tools such as Microsoft SMS or Active Directory. The Command Line Installer Helper (see [Command Line Installer Helper on page 4-21](#) for more details) is a tool used to create scripts. The arguments available allow for completely silent or partially silent installations.

**WARNING!**

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

Requirements

- All installation scripts should be run locally, not from a network share or USB drive.
- Scripts must be run as local Administrators.
- Installation scripts should be tested in a pilot program.

Script Arguments

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

TABLE 4-7. Full Disk Encryption scripted arguments for automated installations

| ARGUMENT | VALUE | NOTES |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| ENTERPRISE | Enterprise name | You can find the enterprise name from your license file. |
| HOST | DNS hostname or IP address | The name or location of PolicyServer. |
| USERNAME | <ul style="list-style-type: none"> • Group Administrator • Group Authenticator • Group User (if the allow install policy is enabled) | Enterprise-level Administrator or Authenticator account cannot be used to install Full Disk Encryption. |
| PASSWORD | Password for specified user name | The fixed password configured in PolicyServer for the user, or a domain password. |

TABLE 4-8. FileArmor scripted arguments for automated installations

| ARGUMENT | VALUE | NOTES |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| PSENERPRISE | Enterprise name | You can find the enterprise name from your license file. |
| PSHOST | DNS hostname or IP address | The name or location of PolicyServer. |
| FAUSERNAME | <ul style="list-style-type: none"> • Group Administrator • Group Authenticator • Group User (if the allow install policy is enabled) | Enterprise-level Administrator or Authenticator account cannot be used to install FileArmor. |
| FAPASSWORD | Password for specified user name | The fixed password configured in PolicyServer for the user, or a domain password. |

Command Line Installer Helper

The Command Line Installer Helper (`CommandLineInstallerHelper.exe`) can generate scripts used to install Full Disk Encryption, FileArmor, and PolicyServer. Options allow encrypting and hiding installation account information, and selecting various prompt options. Script results are easily copied to the clipboard for export. The tool has two tabs: one for clients, and one for PolicyServer.



Note

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

When using the Command Line Installer Helper:

- Only run installation scripts on an endpoint client, no from the network.
- Run scripts as a local admin.
- Test installation scripts in a pilot program first.
- Review all Full Disk Encryption and FileArmor pre-installation checklist items before executing any mass distribution of software.

Full Disk Encryption and FileArmor are compliant with automated software distribution tools, such as SMS, SCCM, Tivoli, GPO, and LANDesk.

Creating PolicyServer Installation Scripts

The minimum information required to create a script is:

- Primary database address and Administrator credentials
- Path to the PolicyServer installer



Important

Scripted installation is only supported by PolicyServer version 3.1.2 or newer.

Procedure

1. Provide all required information.
2. Provide additional information if necessary.
3. Click **Generate Command**.

The **Policy Server Install Command** code field populates.

4. Click **Copy to Clipboard**.

The resulting script is copied to the clipboard.

Creating Client Installation Scripts

The following information is required to generate a silent install script: PolicyServer hostname or IP address, the enterprise name, user name, password, and the path and version number of the endpoint client installer.

Procedure

1. Provide the required information in the appropriate text fields.
2. Select the options you want to include in the script.
3. Click **Generate Command**.

The scripts generate.

4. Click **Copy Full Disk Encryption Command** or **Copy FileArmor Command**.

The resulting script is copied to the clipboard.

Command Line Helper

The Command Line Helper is used to create encrypted values that can then be used to secure credentials when you are scripting an install for deployment or using

DAAutoLogin. The Command Line Helper tool is located in the FileArmor Tools folder.



Note

The Command Line Helper can only run on systems where PolicyServer, Full Disk Encryption, or FileArmor is installed as it makes use of the Mobile Armor cryptographic.

The program accepts a single string as its only argument and returns an encrypted value to be used in the installation script. The leading and trailing “=” signs are included as part of the complete encrypted string and must be included on the command line. If the value is encrypted and does not return a leading = sign, then an equal sign must be added to the script.

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

TABLE 4-9. Arguments for Command Line Helper

| FUNCTION | ARGUMENTS | | |
|--------------|----------------------|--------------------------------|-------------|
| | FULL DISK ENCRYPTION | FULL DISK ENCRYPTION ENCRYPTED | FILEARMOR |
| Enterprise | ENTERPRISE | eENTERPRISE | PSENERPRISE |
| PolicyServer | HOST | eHOST | PSHOST |
| User name | USERNAME | eUSERNAME | FAUSERNAME |
| Password | PASSWORD | ePASSWORD | FAPASSWORD |



Note

The FileArmor Installer can automatically handle encrypted values.

Full Disk Encryption Script Example

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

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

```
ENTERPRISE = MyCompany
```

```
HOST = PolicyServer.mycompany.com
```

```
eUSERNAME = GroupAdministrator
```

```
ePASSWORD = 123456
```

**Note**

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

Output to install Full Disk Encryption:

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

FileArmor Script Example

This is an example of a FileArmor installation script for a device running a 32-bit operating system. For 64-bit devices, use `FASetup(x64).msi` instead.

```
Software location = C:\Program Files\Trend Micro\FileArmor
\FASetup.msi
```

```
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 FileArmor:

```
C:\Program Files\Trend Micro\FileArmor\FASetup.msi  
PSEnterprise=MyCompany PSHost= PolicyServer.mycompany.com  
FAUser==jJUJC/Lu4C/Uj7yYwxubYhAuCrY4f7AbVFp5hKo2PR4O=  
FAPassword==5mih67uKdy7T1VaN2ISWGQQ=
```


Chapter 5

Upgrades, Migrations and Uninstalls

This chapter describes various aspects about upgrading, managing, migrating, and uninstalling every Trend Micro Endpoint Encryption application.

The topics covered in this chapter include:

- *Upgrading Server and Client Software on page 5-2*
- *Upgrading to Windows 8 on page 5-8*
- *Patch Management with Full Disk Encryption on page 5-9*
- *Replacing a Previously Installed Encryption Product on page 5-10*
- *Migrating Endpoint Clients to a New PolicyServer on page 5-12*
- *Uninstalling Client Applications on page 5-16*

Upgrading Server and Client Software

This section explains PolicyServer and Endpoint Encryption client software upgrades.

Upgrading PolicyServer

Before upgrading PolicyServer, be aware of the following:

- All PolicyServer front-end servers or services must be stopped before completing the database upgrade.
- When upgrading multiple PolicyServers connected to the same database:
 1. Ensure that only one PolicyServer performs the database upgrade.
 2. Stop the PolicyServer Windows Service on all PolicyServers except one.
 3. Perform the upgrade on the active server.
 4. After the upgrade completes and the database replicates, run the upgrade on the remaining servers.
- If Trend Micro LDAP Proxy is used, upgrade LDAP Proxy before upgrading to PolicyServer 3.1.3.

**Note**

Trend Micro does not currently support hosted PolicyServer environments.

Upgrading PolicyServer Databases and Services

The PolicyServer Installer configures database settings and installs Windows services. New to PolicyServer 3.1.3 is the ability to specify a port number for the PolicyServer Web Service. A second port is also now required for the Client Web Service. If a second port does not exist, a new port is created during the installation process. For details about the new architecture, see [Endpoint Encryption Components on page 1-2](#).

In order to use Endpoint Encryption for a limited trial period, the Enterprise name and Enterprise Administrator account can be configured at the time of installation.

PolicyServer functions normally with all client applications, unlimited devices, and up to 100 users for a 30-day trial period. After 30 days, contact Technical Support to receive a license file. Users and devices can still log on after the trial period expires.

Procedure

1. Run `PolicyServerInstaller.exe`
2. Read the End User License Agreement carefully. If you agree, click **Accept**.
3. Verify the PolicyServer version and then click **Upgrade**.
4. At the **Windows Service Logon** screen, the default settings are appropriate for most installations. Click **Continue**.
5. At the **Database Administrator Logon** screen, provide the Microsoft SQL Server hostname (localhost) or IP address, and the user name and password of an account with the sysadmin role for the specified SQL instance.



Note

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

```
<hostname or IP address>\<database instance>
```

The installer verifies the database connection.

6. At the **PolicyServer Question** window, click **Yes** to back up existing databases, or **No** to overwrite existing data.

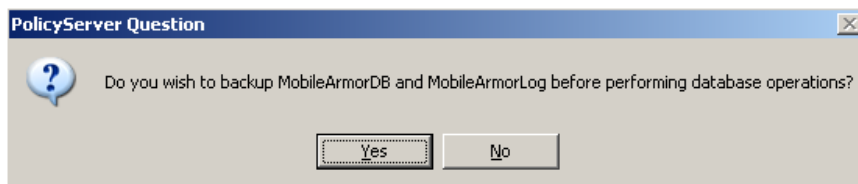


FIGURE 5-1. Database Backup Message

7. At the **Database Logon** screen, provide the credentials of the account that was previously used for PolicyServer to manage data transactions (PolicyServer Windows Service).

If this account is unavailable, type credentials to create a new account.

8. At the **Web Service Install Location** screen, specify the IIS site that PolicyServer MMC and the Client Web Service will use to communicate with PolicyServer. The default port number is 8080. If port 8080 is in use, then the next available port is assigned.
 - a. Select a site from the **Target Site** drop-down.
 - b. Review the current port assigned and, if needed, specify a different port number in the **New Port** field.

**Note**

Trend Micro recommends reserving port 80 for the Client Web Service.

- c. Click **Continue**.
9. This next step is designed to configure the Client Web Service, which is the IIS site that all Endpoint Encryption clients use to communicate with PolicyServer. Depending on whether a second IIS location is available, one of the following screens display:
 - If a second IIS site is available, the **Client Web Service Location** screen displays.
 - a. Select a site from the **Target Site** drop-down.
 - b. Review the default port assignment for the Client Web Service.

**Note**

Trend Micro recommends maintaining port number 80. However, if needed, specify a different port number in the **New Port** field. The port number must be a positive integer between 1 and 65535.

- c. Click **Continue**.

- If a second IIS site is unavailable, the **Create Client Web Service Location** screen displays to configure a new IIS location.
 - a. Specify a name for the IIS location in the **Site Name** field.
 - b. Browse to the site location. If a folder does not yet exist, create a new one.
 - c. Specify the IP address and port number for the new IIS location.

**Note**

Trend Micro recommends maintaining port number 80. However, if needed, specify a different port number. The port number must be a positive integer between 1 and 65535.

- d. Click **Continue**.
10. At the **Mobile Web Service Install Location** screen, review the settings and then click **Continue**.
 11. At the **Create Enterprise Name and Administrator Logon** screen, specify the new Enterprise name and the credentials for a new Enterprise Administrator account used to manage PolicyServer during the initial trial period.
 12. Click **Continue**.

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 PolicyServer MMC

PolicyServer MMC must be removed using Windows Add/Remove Programs feature before a new version can be installed.

Procedure

1. Go to **Start > Control Panel > Add or Remove Programs**.
2. Select PolicyServer MMC Snapin from the list and click **Remove**.
3. Click **Yes** to remove PolicyServer MMC.
4. Run `PolicyServerMMCSnapinSetup.msi`.
5. Click **Next** to begin the Welcome to PolicyServer MMC Setup Wizard.
6. Carefully read the license agreement, select **I Agree** if you agree to the terms, and then click **Next**.
7. Select installation folder or leave at default location, and click **Next**.
8. Click **Next** to confirm installation.
The upgrade process begins.
9. Click **Close** to complete installation.
10. Click **Yes** to restart the device (optional).
11. After logging back into the server, open PolicyServer MMC from the desktop shortcut.

PolicyServer MMC upgrade complete. Authenticate to PolicyServer MMC using the enterprise Administrator credentials.

**Note**

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

Upgrading Full Disk Encryption

The Full Disk Encryption upgrade installer (`TMFDEUpgrade.exe`) supports DataArmor SP7g (3.0.12.861) and DataArmor 3.1.2. To upgrade from DataArmor SP7g, the device must be connected to PolicyServer. For older versions of DataArmor and

DriveArmor, uninstall the application and reboot the device before installing Full Disk Encryption.

**Note**

Non-English operating systems currently running an older version of Full Disk Encryption (DataArmor 3.0.12 or 3.1.2) will continue to use English after the upgrade. To upgrade to a supported language, first uninstall the previous application and then install Full Disk Encryption 3.1.3. For details about uninstalling Full Disk Encryption, see [Uninstalling Full Disk Encryption on page 5-16](#).

Procedure

1. Copy the Full Disk Encryption installation package to the local hard drive.
2. Run `TMFDEUpgrade.exe`.

**Note**

If Windows User Account Control opens, click **Yes** to continue.

3. After the upgrade has finished notification appears, reboot the device.
-

Upgrading FileArmor

Use `FA_313_Upgrade.exe` to upgrade a device from FileArmor 3.0.13 or FileArmor 3.0.14. `FA_313_Upgrade.exe` is located in FileArmor installation directory tools folder.

**Note**

`FA_313_Upgrade.exe` bypasses the Allow User to Uninstall policy and upgrades whether the policy is set to **Yes** or **No**.

Procedure

1. Run `FA_313_Upgrade.exe`.

Windows installer uninstalls the older FileArmor version and then installs FileArmor 3.1.3. When complete, Windows reboots.

2. After Windows reboots, log on and check the new FileArmor folder. Encrypted files and folders are maintained.
-

Upgrading 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 FileArmor is already installed on the endpoint client. KeyArmor does not support the Windows 8 environment.

Procedure

1. Follow the instructions in the Endpoint Encryption Administrator's Guide to decrypt the device.
 2. Uninstall endpoint client applications:
 - For details about uninstalling Full Disk Encryption, see [Uninstalling Full Disk Encryption on page 5-16](#).
 - For details about uninstalling FileArmor, see [Uninstalling FileArmor on page 5-17](#).
 3. Upgrade to or install the Windows 8 operating system.
-



This document does not explain how to install the Windows 8 environment. 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 endpoint client applications:

- For details about installing Full Disk Encryption, see [Installing Full Disk Encryption on page 4-2](#).
 - For details about installing FileArmor, see [Installing FileArmor on page 4-12](#).
-

Patch Management with Full Disk Encryption

Use the **Command Line Helper** and **DAAutoLogin** together to run Windows patch management on devices with Full Disk Encryption installed. Command Line Helper creates encrypted values for scripts and DAAutoLogin grants a one-time bypass of the Full Disk Encryption Preboot.

DAAutoLogin can be used in various combinations to accomplish different needs. Patches can be pushed out, and followed by a script using DAAutoLogin to send a reboot command for the device to display the Windows GINA for confirmation of successful patching or to another round of patches can be deployed.

DAAutoLogin accepts the following switches:

```
DAAutoLogin <pre-boot Username> <pre-boot Password> [<Domain Name> <Domain Username> <Domain Password>]
```

Each required value can be passed and separated with a space. Adding in the domain switches allows for Windows authentication.



Note

- Run both tools on a device with Full Disk Encryption installed.
 - Both tools are available in the tools folder of the zip file received from Trend Micro. For assistance, Trend Micro Support.
-

Using Command Line Helper

The Command Line Helper and DAAutoLogin can be used together for seamless Full Disk Encryption patch management. Command Line Helper enables you to pass encrypted values via your script to the Full Disk Encryption Preboot. DAAutoLogin grants a one-time bypass of the Full Disk Encryption Preboot.

Procedure

1. Copy `CommandLineHelper.exe` locally to Full Disk Encryption device. (In this example `CommandLineHelper.exe` is copied to `C:\`).
 2. Open command prompt and type `C:\CommandLineHelper.exe` and specify the user name or password that will be used. If the user name is `SMSUser`, then the command is `C:\CommandLineHelper.exe SMSUser`.
 3. Click **Return** to display the encrypted value.
 4. Run Command Line Helper again for the second encrypted value. If the first time was the user name, run it again to encrypt the password.
-

Patching Process for Full Disk Encryption

Procedure

1. Push patches to targeted devices.
 2. Follow up with a script using `DAAutoLogin`.
 3. Send a reboot command for the device to load Windows GINA for confirmation of successful patching or to push another round of patches.
-

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 your disk preparation process and deployment strategy. Depending on the time required to decrypt a device and encrypt with Full Disk Encryption, it may be simply back up user data and re-image a machine 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 details, see [Installing Full Disk Encryption on page 4-2](#).
-

Option 2: Back Up and Re-image the Device

Procedure

1. Backup user files.
2. Re-image the device:
 - 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 device.
 4. Restore user files.
-

Migrating Endpoint Clients to a New PolicyServer

This section explains how to change the PolicyServer that controls an endpoint client's policies. This is useful when an end user changes to a department or business unit that is managed by a different PolicyServer instance.

Changing the Full Disk Encryption PolicyServer

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

Managing PolicyServer Settings

Procedure

1. Open the **PolicyServer** tab. There are two text fields: **Current Server** and **Current Enterprise**.
 - To change the current enterprise:
 - a. Click **Change Enterprise**.
 - b. At the warning message appears, click **Yes**.
 - c. Specify the new server user name, password, enterprise and server name, then click **Save**.

**WARNING!**

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

- To change the current server:
 - a. Click **Change Server**.
 - b. At the warning message, click **Yes**.
 - c. Specify the new server address and click **Save**.
 - 2. Click **Cancel** to return to the Recovery Console menu options screen.
-

Moving Full Disk Encryption to a New Enterprise

**WARNING!**

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

Procedure

1. Open the Recovery Console. There are two ways to open Recovery Console:
 - From Full Disk Encryption Preboot:
 - a. Select the **Recovery Console** check box.
 - b. Provide credentials and the click **Login**.
 - From Windows:
 - a. Go to `C:\Program Files\Trend Micro\Full Disk Encryption\`.
 - b. Run `RecoveryConsole.exe`.
 - c. Provide credentials and the click **Login**.

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

The **Change Enterprise** screen displays.

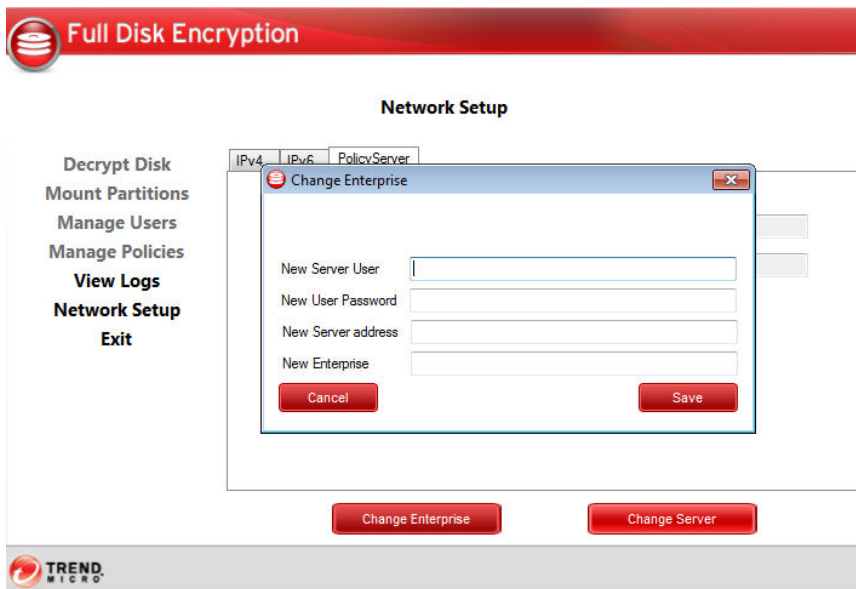


FIGURE 5-2. Recovery Console Change Enterprise

5. Specify the new server user name, password, the PolicyServer IP address (or host name), and the enterprise.
6. Click **Save**.
Full Disk Encryption validates the server and post a confirmation message.
7. At the confirmation message, click **OK**.

Changing the FileArmor PolicyServer

Procedure

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

Moving KeyArmor to a New Enterprise

Procedure

1. Log on the device with Endpoint Encryption Administrator credentials.
2. Right click the KeyArmor icon in the tray menu and select **About KeyArmor**.
3. Click the **edit** link next to the **Server Address** box and type the new server address.
4. Click **OK**.
5. Log off KeyArmor.
6. Remount device and log back in with the Administrator credentials.
7. Right click the KeyArmor icon from the tray menu and select **About KeyArmor**.
8. Click the **edit** link next to the **Enterprise** box and type the new Enterprise Name.
9. Click **OK**.
10. Click **Close**.
11. Log off KeyArmor.
12. Log on the KeyArmor device with a Group Administrator user name and password from the new target enterprise.

13. Verify the log events within the new Enterprise group that the device was added to the correct group.
-

Uninstalling Client Applications

This section explains how to uninstall Endpoint Encryption client applications.

Uninstalling Full Disk Encryption

To uninstall Full Disk Encryption, the user must have uninstall rights within their group and have Windows local administrator rights.



Tip

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

Procedure

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



Note

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

The Full Disk Encryption Uninstall opens.

3. Click **Next**.

Full Disk Encryption begins to uninstall.

4. Click **OK** to confirm drive decryption.

**Note**

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

5. When decryption completes, click **OK**.
 6. Run `TMFDEUninstall.exe` again to finish the uninstall.
 7. Reboot the device.
-

**Note**

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

Uninstalling FileArmor

Use Windows Add/Remove Programs to uninstall FileArmor.

**Note**

- Set the **Policies > FileArmor > Computer > Allow User to Uninstall** to **Yes** to allow any User or Group Authenticator to run the uninstaller in Windows.
 - Manually decrypt all encrypted files before uninstalling FileArmor. Otherwise, they will become unreadable.
 - Save and close all documents before starting the uninstall process. A reboot is required when the uninstaller completes.
-

Procedure

1. Log on FileArmor with an account that has permission to uninstall FileArmor.
 2. Open the **Windows Start Menu** and go to **Control Panel > Programs > Uninstall a Program**.
 3. Select FileArmor from the list and then click **Uninstall**.
-

Chapter 6

Getting Support

Depending on the type of support needed, there are various places to get help.

This chapter covers the following topics:

- *Trend Community on page 6-2*
- *Support Portal on page 6-2*
- *Contacting Technical Support on page 6-3*
- *TrendLabs on page 6-4*

Trend Community

Get help, share experiences, ask questions, and discuss security concerns with other fellow users, enthusiasts, and security experts.

<http://community.trendmicro.com/>

Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains thousands of helpful and easy to use technical support procedures for Trend Micro products and services. New solutions are added daily.

Procedure

1. Go to <http://esupport.trendmicro.com>.
2. Select a product or service from the appropriate drop-down menu and specify any other related information, if prompted.

The Technical Support product page displays.

3. Specify any search criteria, for example an error message, and then click the search icon.

A list of solutions displays.

4. If the solution cannot be found, submit a case and a Trend Micro support engineer will investigate the issue. Response time is typically 24 hours or less.

Submit a support case online at:

<http://esupport.trendmicro.com/srf/SRFMain.aspx>

Contacting Technical Support

Technical support, pattern downloads, and product/service updates are available for one year with all product licenses. After one year, renew the license to continue receiving Trend Micro support.

In the United States, reach Trend Micro representatives by phone, fax, or email:

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

- Get a list of the worldwide support offices at:
<http://www.trendmicro.com/us/about-us/contact/index.html>
- Get the latest Trend Micro documentation at:
<http://docs.trendmicro.com>

Resolving Issues Faster

To speed up problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional hardware connected to the endpoint
- Amount of memory and free hard disk space
- Operating system and service pack version
- Endpoint client version
- Serial number or activation code

- Detailed description of install environment
- Exact text of any error message received

TrendLabs

TrendLabs is a global network of research, development, and action centers committed to 24/7 threat surveillance, attack prevention, and timely and seamless solutions delivery. Serving as the backbone of the Trend Micro service infrastructure, TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services.

TrendLabs monitors the worldwide threat landscape to deliver effective security measures designed to detect, preempt, and eliminate attacks. The daily culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

Learn more about TrendLabs at:


<http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs>

Appendix A

Endpoint Encryption Pilot Checklist

| PILOT PROGRAM CHECK LIST | DATE | NOTES |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------|
| PolicyServer configured as required <ul style="list-style-type: none"> • Policies set • Groups created • Users created/imported | | |
| Client software installed (Full Disk Encryption and/or FileArmor) <ul style="list-style-type: none"> • Software copied locally to machine and run successfully | | |
| Administrators, Authenticators and end-users can access devices based on policy settings <ul style="list-style-type: none"> • Fixed Password • Single Sign-on • Smart Card | | |

| PILOT PROGRAM CHECK LIST | DATE | NOTES |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------|
| <p>All machines compatible with new software</p> <ul style="list-style-type: none">• Preboot authentication and/or connectivity confirmed• Encryption completes• Machine functions normally• Files/Folders encrypted per policy• USB port controlled as defined by policy• PolicyServer alerts, event logs and reports confirm Administrator and end user activity | | |
| <p>End-users can perform business as usual activities</p> <ul style="list-style-type: none">• Access windows via existing user name/password or SSO from pre-boot• Machine functions normally both on and off the network• User has access to all user data, applications and network resources | | |

| PILOT PROGRAM CHECK LIST | DATE | NOTES |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------|
| <p>System Administrators test support processes</p> <ul style="list-style-type: none">• Create Backup Administrators• Test reporting and alerts• Use Full Disk Encryption Recovery Console to back up and recover files• Use Full Disk Encryption Recovery CD to decrypt device and remove pre-boot• Test Remote Help authentication process• Test device lock and device wipe. <hr/> <p> WARNING! Do not wipe a KeyArmor device. The device cannot be restored.</p> <hr/> | | |

Appendix B

Security Infrastructure Checklist

TABLE B-1. Security Infrastructure Checklist

| CHECK | QUESTIONS |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| End-user | <ol style="list-style-type: none"><li data-bbox="512 760 1166 813">1. Does the end-user training include the new functionality that Endpoint Encryption provides?<li data-bbox="512 829 1166 911">2. Is the Acceptable Use Policy (AUP) updated to include encryption services, especially any penalties for not using or bypassing encryption?<li data-bbox="512 927 1166 980">3. Are users notified when they log on the machine that aligns with the AUP?<li data-bbox="512 997 1166 1050">4. Are all users fully trained on how to report a lost or stolen device?<li data-bbox="512 1066 1166 1120">5. Have users been trained on procedures regarding failed login attempts and password recovery?<li data-bbox="512 1136 1166 1190">6. Is there a policy regarding encryption of confidential documents that are sent outside of the organization?<li data-bbox="512 1206 1166 1239">7. Have any new password policies been added to the AUP? |

| CHECK | QUESTIONS |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Incident Response | <ol style="list-style-type: none"> 1. Has the Incident Response (IR) policy been updated to include actions taken when a device is lost or stolen? 2. Has an audit log review schedule been established for the PolicyServer logs? 3. Have the email alerts been added to the IR policy, including the recipients and the expected response when an alert is received? 4. Have specific criteria been developed to allow a device to be killed or wiped, including any audit trail documentation after the action is completed? |
| Risk Assessment | <ol style="list-style-type: none"> 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 | <ol style="list-style-type: none"> 1. Has PolicyServer been added to the Critical Services list? 2. Is the DR/BC plan updated to include the restoration of the Policy Server service? 3. Is a process developed to allow user data to be recovered from a device? |
| Human Resources | <ol style="list-style-type: none"> 1. Is the New Employee checklist updated to include any new process for Endpoint Encryption? 2. Is the termination processes updated to include any new process for Endpoint Encryption - especially device kill/wipe? |
| Compliance | <ol style="list-style-type: none"> 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? |

Appendix C

Full Disk Encryption Pre-installation Checklist

Before installing Full Disk Encryption, the Full Disk Encryption installer launches and automatically checks the target device that all necessary system requirements are met. The installer closes if these are not met.

Use the checklist to determine missing requirements. Check the `PreInstallCheckReport.txt` file for details. `PreInstallCheckReport.txt` is located in the same folder as the Full Disk Encryption installation files.

TABLE C-1. Conditions Checked by the Installer

| SYSTEM CHECK | REQUIREMENT | NOTES |
|-----------------|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Fixed media | Internal hard drive | Full Disk Encryption cannot be installed on removable drives running Windows. For file and folder encryption on removable media, use FileArmor. |
| Free space | 256MB minimum | |
| Memory | 1GB minimum | |
| Partition count | Fewer than 25 partitions | Partitions with extended MBRs are not available. |

| SYSTEM CHECK | REQUIREMENT | NOTES |
|----------------------------|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Partition type | Only MBR is supported | GPT (necessary for disks larger than 2TB) is not currently supported. |
| Physical drive is bootable | A bootable partition is required. | Full Disk Encryption must be installed on a bootable table. |
| SCSI disk | ATA, AHCI or IRRT drive controller. SCSI is not supported. | <ul style="list-style-type: none"> • Check only provides a warning; Windows may report a SATA drive as SCSI. • If the disk is not a true SCSI, Full Disk Encryption can be installed. If unsure, physically check the drive. |
| .Net Framework | .Net 2.0 SP1 or newer required for Windows XP and above. | Skipped for Windows Vista or newer operating systems. |
| SED hardware compatibility | Hardware encryption is enabled if present. | Full Disk Encryption supports Seagate™ DriveTrust™, OPAL, and OPAL 2 drives. |
| BitLocker is not installed | BitLocker cannot be installed on the device. | If BitLocker is installed, it must be removed before Full Disk Encryption can be installed. |

**Note**

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

Index

A

- about
 - client-server architecture, 1-2
 - Endpoint Encryption, 1-2
 - Full Disk Encryption, 4-2
 - KeyArmor, 4-16
 - PolicyServer, 3-2
- Active Directory, 3-12, 4-9
 - configuration, 3-13
 - overview, 3-12
- AHCI, 4-6
- ATA, 4-6
- authentication, 1-8
- automated installation, 4-8

B

- BIOS, 4-6
- BitLocker, 4-5

C

- central administration, 1-8
- central management, 1-9
- change management, 2-9
 - Active Directory, 2-9
- changing PolicyServers, 5-12
- client-server architecture, 1-2
- Command Line Helper, 4-22, 5-9
 - for FileArmor, 4-24
 - for Full Disk Encryption, 4-23
- Command Line Installer Helper, 4-19, 4-21
- community, 6-2
- cryptography, 1-2

D

- DAAutoLogin, 5-9

- DataArmor SP7, 4-6
- database requirements, 1-5, 3-4
- data protection, 1-2
- decryption, 5-16
- deployment
 - change management, 2-9
 - considerations, 2-1, 2-6
 - end-users, 2-5
 - FileArmor, 4-12
 - KeyArmor, 4-17
 - pilot program, 2-8
 - planning, 2-5
 - policies, 2-8
 - project team, 2-7
 - scaling, 2-11
 - security infrastructure, 2-7
 - supported platforms
 - FileArmor, 2-3
 - Full Disk Encryption, 2-3
 - KeyArmor, 2-3
 - PolicyServer, 2-3
- deployment requirements, 2-1
- device management, 1-8
- disk controller, 4-6

E

- encryption, 1-9
 - BitLocker, 4-5
 - features, 1-8
 - file and folder, 1-10
 - FIPS, 1-11
 - full disk, 1-10
 - hardware-based, 1-9, 1-10
 - installation scripts, 4-20

- project planning, 2-1
- software-based, 1-9, 1-10
- endpoint clients
 - installation, 4-1
 - scripted installations, 4-22
 - supported platforms, 2-3

Endpoint Encryption

- about, 1-2
- pilot checklist, A-1

F

FileArmor

- change PolicyServer, 5-15
- deployment, 4-12
- file encryption, 1-10
- installation, 4-12, 4-14
 - manual, 4-15
 - other requirements, 4-15
 - scripts, 4-16
- policies, 4-13
- supported operating systems, 1-7, 4-14
- system requirements, 1-7, 4-14
- uninstalling, 5-17
- upgrades, 5-7

FIPS, 1-2

- about, 1-11
- FIPS 140-2, 1-2, 1-11
- security levels, 1-11

FIPS 140-2, 1-2

Full Disk Encryption, 4-2

- change enterprise, 5-12
- change PolicyServer, 5-12
- changing enterprises, 5-13
- device encryption, 4-2
- hard disk preparation, 4-4
- installation, 4-7
 - automated, 4-8

- managed, 4-7, 4-8
- managed requirements, 4-9
- scripts, 4-8
- unmanaged, 4-7
- installation types, 4-7
- patching, 5-10
- policies, 4-2
- pre-installation checklist, 4-3, C-1
- preparing device, 4-5
- replacing another product, 5-10
- supported operating systems, 1-6, 4-3
- system requirements, 1-6, 4-3
- uninstalling, 5-16
- upgrades, 5-6

G

- GPO, 4-21

H

hard drives

- installation preparation, 4-4
- hardware based encryption, 1-6, 4-3

I

installation

- automated, 4-8
- FileArmor, 4-12
 - other requirements, 4-15
- hard drive preparation, 4-4
- managed, 4-8
- managed client, 4-9, 4-11
- manual, 4-8
- methods, 4-8
- pilot checklist, A-1
- PolicyServer, 3-1
- PolicyServer databases, 3-7
- PolicyServer MMC, 3-10

- PolicyServer web services, 3-7
- security infrastructure checklist, B-1
- installation scripts, 4-16
- Intel Matrix Manager, 4-7
- Intel Rapid Recovery Technology, 4-6

K

- KeyArmor, 4-16
 - changing enterprises, 5-15
 - deployment, 4-17
 - device components, 4-17
 - end-users, 4-18
 - key management, 1-11
 - safe removal, 4-18
 - SECURE DRIVE, 4-17
 - system requirements, 1-7, 4-17
- key features, 1-8
- key management, 1-11, 4-16

L

- LANDesk, 4-21
- LDAP proxy
 - hardware checklist, 3-18
 - requirements, 3-17
- LDAP Proxy, 3-17
- license file, 3-2
- License file, 3-5

M

- managed client
 - installation, 4-9, 4-11
- managed installation, 4-7, 4-8
 - requirements, 4-9
- manual installation, 4-8
- Microsoft .NET, 2-3
- Microsoft SMS, 4-19
- migration

- KeyArmor, 5-15
- migrations, 5-1
 - migrating endpoint clients, 5-12
- Mobile Armor cryptographic, 4-22

O

- online
 - community, 6-2
- OPAL, 1-6, 4-3

P

- passwords, 1-9
- patch management, 5-9
- Phased rollout, 2-10
- pilot program, 2-8
- policies, 1-9
 - security planning, 2-8
 - synchronization, 1-10
- policy control, 1-10
- PolicyServer
 - AD synchronization, 3-1, 3-12
 - changing, 5-12
 - client web service, 1-2
 - installation
 - database, 3-7
 - Microsoft SQL DB, 3-6
 - MMC, 3-10
 - order, 3-6
 - web services, 3-7
 - installation files, 3-2
 - installation process, 3-1
 - installation requirements, 3-1
 - introduction, 3-2
 - LDAP proxy, 3-17
 - requirements, 3-3
 - accounts, 3-5
 - files, 3-5

- SQL, 1-5, 3-3
- scaling, 2-11
- scripted installation, 4-21
- setup files, 3-5
- software requirements, 1-5, 3-4
- SQL accounts, 3-5
- SQL requirements, 1-5, 3-3
- system requirements
 - hardware, 1-5, 3-3
- upgrades
 - database, 5-2
 - web services, 5-2
- upgrading, 5-2
- upgrading MMC, 5-5
- web service, 1-2

PolicyServer installation scripts, 4-21

PolicyServer MMC, 1-2, 3-9

- applications, 3-9
- policies, 3-9
- users and groups, 3-9

pre-installation checklist, 4-3

pre-installation considerations, 4-2

pre-install check report, C-1

product components, 1-2

product definitions, viii, ix

product overview, 1-1

R

Recovery Console

- changing enterprise or server, 5-12
- changing enterprises, 5-13

reporting, 1-2, 1-8

S

SATA, 4-7

scaling

- server and database requirements, 2-11

- scaling requirements, 2-1
- SCCM, 4-21
- scripted installations, 4-19
- scripts
 - arguments, 4-20
 - encryption, 4-20
 - FileArmor, 4-20, 4-24
 - Full Disk Encryption, 4-20, 4-23
 - requirements, 4-19
- Seagate DriveTrust drives, 1-6, 4-3
- security
 - anti-malware/antivirus protection, 1-2
- security infrastructure, 2-7
- security infrastructure checklist, B-1
- single sign-on, 4-9
- software, 1-5, 3-4
- support
 - knowledge base, 6-2
 - resolve issues faster, 6-3
 - TrendLabs, 6-4
- system architecture, 1-2
- system requirements
 - FileArmor, 1-7, 4-14
 - Full Disk Encryption, 1-6, 4-3
 - KeyArmor, 1-7, 4-17
 - PolicyServer, 1-5, 3-3, 3-4

T

terminology, viii, ix

tools

- Command Line Helper, 4-22, 5-9
- Command Line Installer Helper, 4-21
- DAAutoLogin, 4-22, 5-9
- Recovery Console, 5-13, 5-15

TrendLabs, 6-4

trial license, 3-7, 3-10, 5-2

Trivoli, 4-21

U

UEFI, 4-5

understanding

- file encryption, 1-10

- FIPS, 1-11

- full disk encryption, 1-10

- key management, 1-11

uninstall, 5-1

- client applications, 5-16

- FileArmor, 5-17

- Full Disk Encryption, 5-16

unmanaged installation, 4-7

upgrade

- PolicyServer web services, 5-2

upgrades, 5-1

- FileArmor, 5-7

- Full Disk Encryption, 5-6

- PolicyServer, 5-2

- PolicyServer databases, 5-2

- PolicyServer MMC, 5-5

V

VMware Virtual Infrastructure, 1-5, 3-3

W

Windows 8, 1-6, 4-3, 4-5

- upgrading to, 5-8

Windows Server 2008 considerations, 1-5, 3-4



TREND MICRO INCORPORATED

10101 North De Anza Blvd. Cupertino, CA., 95014, USA

Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: APEM35671/120920