TREND MICRO™

# 6.0 TREND MICRO™ Endpoint Encryption

## Patch 1

## PolicyServer MMC Guide

Comprehensive Endpoint Encryption for Data at Rest

Endpoint Security

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

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

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

Copyright © 2018. Trend Micro Incorporated. All rights reserved.

Document Part No.: APEM68337/180626

Release Date: August 2018

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

## Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Endpoint Encryption collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Policy:

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

# Table of Contents


## Chapter 1: Introduction

## Chapter 2: About Trend Micro Endpoint Encryption

Features and Benefits ..... 2-3

What's New ..... 2-4

About PolicyServer ..... 2-8

Management Consoles ..... 2-9
- Trend Micro Control Manager ..... 2-10
- About PolicyServer MMC ..... 2-11

Endpoint Encryption Agents ..... 2-11

Authentication Methods ..... 2-13
- ColorCode ..... 2-14
- Domain Authentication ..... 2-14
- Fixed Password ..... 2-15
- PIN ..... 2-15
- Remote Help ..... 2-15
- Self Help ..... 2-16
- Smart Card ..... 2-16

## Chapter 3: Getting Started with PolicyServer MMC

Logging on to PolicyServer MMC ..... 3-3

PolicyServer MMC Interface ..... 3-4

Working with Groups and Users ..... 3-6
- Defining Users and Groups ..... 3-6
- Adding a Top Group ..... 3-7
- Adding a New User to a Group ..... 3-8
- Adding a New Enterprise User ..... 3-11
- Adding an Existing User to a Group ..... 3-13

Understanding Policy Controls ..... 3-15
Policy Visual Indicators ..... 3-15
Policy Fields and Buttons ..... 3-16
Modifying Policies ..... 3-17

Disabling Agents ..... 3-19

Active Directory Synchronization ..... 3-20
Active Directory Overview ..... 3-21
Configuring Active Directory ..... 3-22
Importing Active Directory Users ..... 3-24

## Chapter 4: Policies in PolicyServer MMC

Authentication Overview ..... 4-2
Groups ..... 4-2
Users ..... 4-3
Devices ..... 4-5

Policy Overview ..... 4-5
Policy Visual Indicators ..... 4-6
Policy Fields and Buttons ..... 4-7
Accessing Policies ..... 4-7
Selecting a Policy for Modification ..... 4-8
Editing Policies with Ranges ..... 4-8
Editing Policies with True/False or Yes/ No Responses ..... 4-10
Editing Policies with Multiple-choice / Single-selection ..... 4-12
Editing Policies with Text String Arguments ..... 4-15
Editing Policies with Multiple Options ..... 4-16

Policy Synchronization ..... 4-18

PolicyServer Policies ..... 4-18
Admin Console Policies ..... 4-19
Administrator Policies ..... 4-19
Authenticator Policies ..... 4-20
Log Alert Policies ..... 4-21
Service Pack Download Policies ..... 4-22
Welcome Message Policies ..... 4-22

Full Disk Encryption Policies ..... 4-23
Agent Policies ..... 4-24

Encryption Policies ..... 4-26
Login Policies ..... 4-26
Password Policies ..... 4-32

File Encryption Policies ..... 4-33
Agent Policies ..... 4-33
Encryption Policies ..... 4-33
Login Policies ..... 4-35
Password Policies ..... 4-36

Common Policies ..... 4-37
Agent Policy ..... 4-37
Authentication Policies ..... 4-38

## Chapter 5: Groups in PolicyServer MMC

Group Management ..... 5-2
Adding a Top Group ..... 5-2
Adding a Subgroup ..... 5-4
Modifying a Group ..... 5-5
Removing a Group ..... 5-5
Adding a New User to a Group ..... 5-5
Adding an Existing User to a Group ..... 5-8
Removing Users From a Group ..... 5-9
Removing All Users From a Group ..... 5-10
Adding a Device to a Group ..... 5-11
Removing a Device from a Group ..... 5-12

Offline Groups ..... 5-12
Creating an Offline Group ..... 5-13
Updating an Offline Group ..... 5-15

## Chapter 6: Users in PolicyServer MMC

Adding Users to Endpoint Encryption ..... 6-2
Adding a New Enterprise User ..... 6-2
Importing Users from a CSV File ..... 6-4
Importing Active Directory Users ..... 6-5

Managing Users in Endpoint Encryption ..... 6-7
Finding a User ..... 6-8

Modifying a User ..... 6-9
Viewing a User's Group Membership ..... 6-9
Adding a New User to a Group ..... 6-10
Adding an Existing User to a Group ..... 6-12
Changing a User's Default Group ..... 6-14
Allowing User to Install to a Group ..... 6-15
Removing Users From a Group ..... 6-16
Removing All Users From a Group ..... 6-17
Restoring a Deleted User ..... 6-17

Working with Passwords ..... 6-18
Resetting an Enterprise Administrator/Authenticator Password . 6-19
Resetting a Group Administrator/Authenticator Password ..... 6-20
Resetting User Passwords ..... 6-20
Smart Card ..... 6-22
Using Self Help Password Reset ..... 6-25
Remote Help Assistance ..... 6-27
Managing Password Setting Objects from Active Directory ..... 6-31

## Chapter 7: Devices in PolicyServer MMC

Adding a Device to a Group ..... 7-3
Add/Remove Search Result Icons ..... 7-4

Removing a Device from a Group ..... 7-4

Deleting a Device from the Enterprise ..... 7-5

Getting a Software Token ..... 7-6

Using the Recovery Key ..... 7-7

Viewing Device Attributes ..... 7-8
Device Attributes ..... 7-8

Viewing Directory Listing ..... 7-11

Viewing Group Membership ..... 7-11

Killing a Device ..... 7-12

Locking a Device ..... 7-13

Resetting a Device ..... 7-13

Restoring a Deleted Device ..... 7-14

## Chapter 8: Advanced Enterprise Features

Enterprise Maintenance ..... 8-2
Purge Inactive Users ..... 8-2
Purge Inactive Devices ..... 8-4
Log Purge ..... 8-6

Restoring Deleted Users and Devices ..... 8-8
Restoring a Deleted User ..... 8-8
Restoring a Deleted Device ..... 8-9

Enterprise Log Events ..... 8-9
Managing Log Events ..... 8-10
Alerts ..... 8-10
Enabling PolicyServer to relay SMS and Email Delivery ..... 8-12

Enterprise Reports ..... 8-14
Report Options ..... 8-14
Report Icons ..... 8-15
Report Types ..... 8-15
Displaying Reports ..... 8-19
Scheduling Reports ..... 8-19
Displaying Report Errors ..... 8-20

Maintenance Tools ..... 8-20
Using the Diagnostics Monitor ..... 8-21
Using the Log Server Tool ..... 8-24
Using the PolicyServer Change Settings Tool ..... 8-25
Using the License Renewal Tool ..... 8-26
Using the Command Line Helper ..... 8-30

## Chapter 9: Technical Support

Troubleshooting Resources ..... 9-2
Using the Support Portal ..... 9-2
Threat Encyclopedia ..... 9-2

Contacting Trend Micro ..... 9-3
Speeding Up the Support Call ..... 9-4

Sending Suspicious Content to Trend Micro ..... 9-4
Email Reputation Services ..... 9-4

File Reputation Services ..... 9-5
Web Reputation Services ..... 9-5

Other Resources ..... 9-5
Download Center ..... 9-5
Documentation Feedback ..... 9-6

# Appendices

## Appendix A: PolicyServer Message IDs

## Appendix B: Endpoint Encryption Services

## Appendix C: Policy Mapping Between Management Consoles

## Appendix D: Glossary

## Index

Index ..... IN-1

# Chapter 1

## Introduction

This guide is intended to help security administrators and IT administrators manage Endpoint Encryption users, devices, policies, logs, and reports using the PolicyServer Microsoft Management Console (MMC). This documentation assumes general knowledge about encryption methods, device formatting and partitioning, and client-server architecture.

This help is a supplementary guide for administrators who require advanced policy setup. For general Endpoint Encryption management and help using Trend Micro Control Manager, see the *Endpoint Encryption Administrator's Guide*.

# Chapter 2

# About Trend Micro Endpoint Encryption

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

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

Topics include:


- *Features and Benefits on page 2-3*

- *What's New on page 2-4*
- *About PolicyServer on page 2-8*
- *Management Consoles on page 2-9*
- *Endpoint Encryption Agents on page 2-11*
- *Authentication Methods on page 2-13*

# Features and Benefits

The following table explains Endpoint Encryption key features and benefits.

**TABLE 2-1. Endpoint Encryption Key Features**

| FEATURE | BENEFITS |
|---|---|
| Encryption | • Protection for the full disk, including the master boot record (MBR), operating system, and all system files<br>• Hardware-based and software-based encryption for mixed environments<br>• Comprehensive data protection of files, folders, and removable media |
| Authentication | • Flexible authentication methods, including both single and multi-factor<br>• Control password strength and regularity for password changes<br>• Policy updates before authentication and system boot<br>• Configurable actions on failed password attempt threshold |
| Device management | • Policies to protect data on endpoints and removable media<br>• Ability to remotely lock, reset, wipe, or kill a device |

| FEATURE | BENEFITS |
|---|---|
| Central administration | • Flexibly use either PolicyServer MMC or Control Manager to manage PolicyServer<br>• Deploy Endpoint Encryption agents to endpoints already managed by OfficeScan<br>• Enforce security policies to individual users and policy groups from a single policy server<br>• Instantly protect end user data by sending lock or erase commands to lost or stolen Endpoint Encryption devices<br>• Automate policy enforcement with remediation of security events<br>• Update security policies in real-time, before authentication, to revoke user credentials before booting the operating system |
| Record keeping, reports, and auditing | • Advanced real-time reporting and auditing to ensure security compliance<br>• Analyze usage statistics with scheduled reports and alert notifications |

# What's New

Trend Micro Endpoint Encryption 6.0 Patch 1 offers the following new features and enhancements.

**TABLE 2-2. What's New in Endpoint Encryption 6.0 Patch 1**

| FEATURES / ENHANCEMENTS | DESCRIPTION |
|---|---|
| Option to update PolicyServer setting in agents after installation | For endpoints that have Encryption Management for Microsoft Bitlocker and Encryption Management for Apple FileVault installed, Endpoint Encryption adds the option to update the PolicyServer settings in agents, even after installation. |

| Features / Enhancements | Description |
|---|---|
| AES Encryption key size used by Microsoft Bitlocker | For easier deployment, Endpoint Encryption adds the option to configure the Microsoft Bitlocker AES Encryption key size based on the Full Disk Encryption policy setting. |
| Full Disk Encryption enhancements | Endpoint Encryption adds the following enhancements:<br>• Support for Intel and Toshiba self-encrypting drives<br>• Remote retrieval of the encryption status of each disk from the device by directly querying the agent via system management software<br>• To streamline the Window update process, disks already encrypted by Full Disk Encryption can be configured to repeatedly skip the Full Disk Encryption Preboot |
| File Encryption support for new authentication types | For File Encryption, Endpoint Encryption adds support for the following authentication types:<br>• User Principal Name (UPN) and domain password<br>• Single Sign On by UPN format |
| Logon user information | Endpoint Encryption updates the PolicyServer MMC and Control Manager widgets to show logon user information for Endpoint Encryption agents. |

**Table 2-3. What's New in Endpoint Encryption 6.0**

| Features / Enhancements | Description |
|---|---|
| Support for UEFI firmware | Endpoint Encryption now supports booting on endpoints with UEFI firmware. |
| Improved drive performance using AES-XTS encryption mode | For new installations, Endpoint Encryption uses the AES-XTS method by default. However, existing agents upgraded to this version will retain the existing AES-CBC encryption mode. Moreover, Endpoint Encryption can manage endpoints where both AES-XTS and AES-CBC encryption modes are used. |

| Features / Enhancements | Description |
|---|---|
| Support for systems with more than one physical drive | Endpoint Encryption encrypts all fixed drives during installation. Additionally, users have the option of manually encrypting any fixed drives attached after installation. |
| Wi-Fi preboot policies | Wi-Fi settings can be further customized via new policies available in PolicyServer. These policy settings allow or restrict access to the Wi-Fi settings during preboot. |
| Preboot screen customization | PolicyServer now supports customization of the preboot screen. |
| Encryption of used disk space for Full Disk Encryption | Full Disk Encryption will only encrypt the used disk space, resulting in a faster encryption process. |
| Safety check | Endpoint Encryption runs a safety check after installation to verify if the installation was successfully completed. If successful, Endpoint Encryption loads the preboot screen and starts encrypting. However, if the installation was unsuccessful, (or a force shut down is detected), Endpoint Encryption will not load the preboot screen. |
| Multiple Active Directory Domain Synchronization to PolicyServer | Endpoint Encryption supports synchronization of multiple Active Directory domains to PolicyServer |
| Installation enhancements for Encryption Management for Microsoft Bitlocker | Encryption Management for Microsoft BitLocker successfully installs even if Microsoft BitLocker is installed and enabled. In previous versions, the installer stops if MicrosoftBitLocker is installed and enabled. |

| Features / Enhancements | Description |
|---|---|
| Support for multiple languages | Supported languages for Full Disk Encyrption, File Encryption, Encryption Management for Microsoft BitLocker, Encryption Management for Apple File Vault:<br>• `de` (German)<br>• `en` (English)<br>• `fr` (French)<br>• `es` (Spanish)<br>• `pl` (Polish)<br>• `it` (Italian)<br>• `cs` (Czech)<br>Supported languages for PolicyServer:<br>• `de` (German)<br>• `en` (English)<br>• `fr` (French)<br>• `es` (Spanish)<br>Supported languages for the OfficeScan Plug-in Service (PLS) Add-on:<br>• `de` (German)<br>• `en` (English)<br>• `fr` (French)<br>• `es` (Spanish)<br>• `pl` (Polish, but will display English)<br>• `it` (Italian, but will display English) |

# About PolicyServer

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

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

**TABLE 2-4. PolicyServer Components**

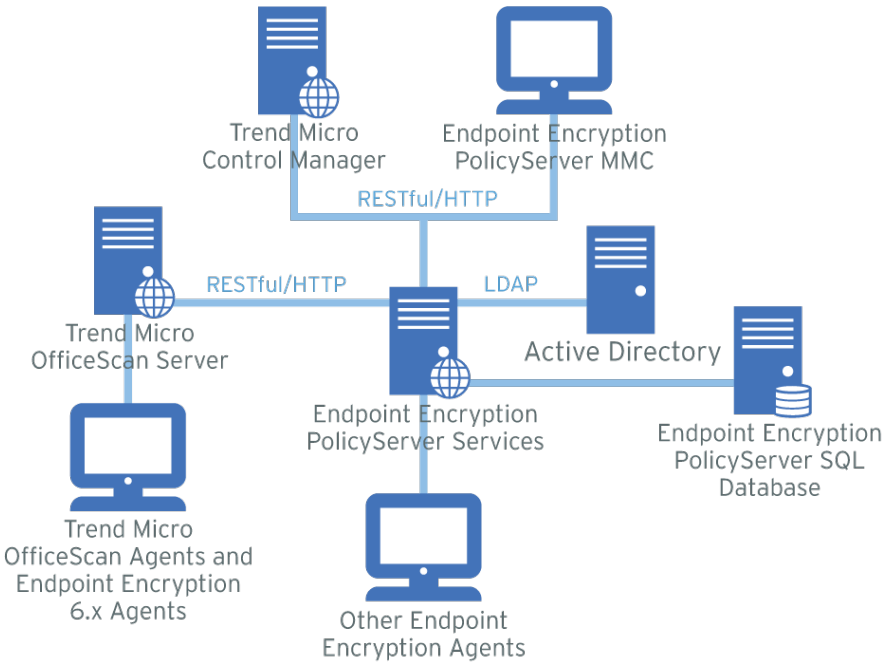
| COMPONENT | DESCRIPTION |
|---|---|
| Enterprise | The Endpoint Encryption Enterprise is the unique identifier about the organization in the PolicyServer database configured during PolicyServer configuration. One PolicyServer database may have one Enterprise configuration. |
| Database | The PolicyServer Microsoft SQL database securely stores all user, device, and log data. The database is either configured on a dedicated server or added to an existing SQL cluster. The log and other databases can reside separately. |
| PolicyServer Windows Service | PolicyServer Windows Service manages all communication transactions between the host operating system, Endpoint Encryption Service, Legacy Web Service, Client Web Proxy, and SQL databases. |
| Endpoint Encryption Service | Starting from Endpoint Encryption 5.0, all agents use Endpoint Encryption Service to communicate with PolicyServer. Endpoint Encryption Service uses a Representational State Transfer web API (RESTful) with an AES-GCM encryption algorithm. After a user authenticates, PolicyServer generates a token related to the specific policy configuration. Until the Endpoint Encryption user authenticates, the service denies all policy transactions. |

| Component | Description |
|---|---|
| Legacy Web Service | All Endpoint Encryption 3.1.3 and earlier agents use Simple Object Access Protocol (SOAP) to communicate with PolicyServer. Under certain situations, SOAP may allow insecure policy transactions without user authentication. Legacy Web Service filters SOAP calls by requiring authentication and limiting the commands that SOAP accepts. This service is optional, and can be installed on the same endpoint as the Endpoint Encryption Service using the Endpoint Encryption proxy installer. |

# Management Consoles

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

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




**Note**

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

## Trend Micro Control Manager

Trend Micro™ Control Manager™ is a central management console that manages Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. The Control Manager web-based management console provides a single monitoring point for managed products and services throughout the network.

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

## About PolicyServer MMC

The PolicyServer Microsoft Management Console plug-in (PolicyServer MMC) is the native management console for Endpoint Encryption policy, user, and device administration.

Use PolicyServer MMC to centrally manage:

- All Endpoint Encryption users, devices, and groups
- All policies including encryption, password complexity and authentication
- Remote device actions, including killing a device, erasing data, or delaying authentication
- Event logs about authentication events, management events, device encryption status, and security violations
- Remote Help password reset process
- Auditing and reporting options

# Endpoint Encryption Agents

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

| AGENT | DESCRIPTION |
|---|---|
| Full Disk Encryption | The Endpoint Encryption agent for hardware and software encryption with preboot authentication. Full Disk Encryption secures data files, applications, registry settings, temporary files, swap files, print spoolers, and deleted files on any Windows endpoint. Strong preboot authentication restricts access vulnerabilities until the user is validated.<br><br>The Full Disk Encryption agent may be installed on the same endpoint as the File Encryption agent. The Full Disk Encryption agent cannot be installed on the same endpoint as either the Encryption Management for Microsoft BitLocker agent or the Encryption Management for Apple FileVault agent. |
| Encryption Management for Microsoft BitLocker | The Endpoint Encryption Full Disk Encryption agent for Microsoft Windows environments that simply need to enable Microsoft BitLocker on the hosting endpoint.<br><br>The Encryption Management for Microsoft BitLocker agent may be installed on the same endpoint as the File Encryption agent. |
| Encryption Management for Apple FileVault | The Endpoint Encryption Full Disk Encryption agent for Mac OS environments that simply need to enable Apple FileVault on the hosting endpoint. |
| File Encryption | The Endpoint Encryption agent for file and folder encryption on local drives and removable media. File Encryption protects files and folders located on virtually any device that appears as a drive within the host operating system.<br><br>The File Encryption agent may be installed on the same endpoint as either the Full Disk Encryption agent or the Encryption Management for Microsoft BitLocker agent. |

# Authentication Methods

Endpoint Encryption administrators and users have several authentication methods to log on to Endpoint Encryption devices. The methods available are determined by the PolicyServer policy configuration.

**Note**

You must use PolicyServer MMC to configure the authentication methods available to Endpoint Encryption users. It is not possible to use Control Manager to configure the allowed authentication methods. However, you can configure Control Manager for domain authentication.

**TABLE 2-5. Supported Authentication Methods**

| AUTHENTICATION METHOD | DESCRIPTION |
|---|---|
| *ColorCode on page 2-14* | A unique sequence of colors. |
| *Domain Authentication on page 2-14* | Active Directory LDAP synchronization for single sign-on (SSO). |
| *Fixed Password on page 2-15* | A string of characters, numbers, and symbols. |
| *PIN on page 2-15* | A standard Personal Identification Number (PIN). |
| *Remote Help on page 2-15* | Interactive authentication for users who forget their credentials or devices that have not synchronized policies within a predetermined amount of time. |
| *Self Help on page 2-16* | Question and answer combinations that allow users to reset a forgotten password without contacting Technical Support. |
| *Smart Card on page 2-16* | A physical card used in conjunction with a PIN or fixed password. |

## ColorCode

ColorCode™ is a unique authentication method designed for quick access and easy memorization. Rather than alphanumeric characters or symbols for the password, ColorCode authentication consists of a user-created color sequence (example: red, red, blue, yellow, blue, green).

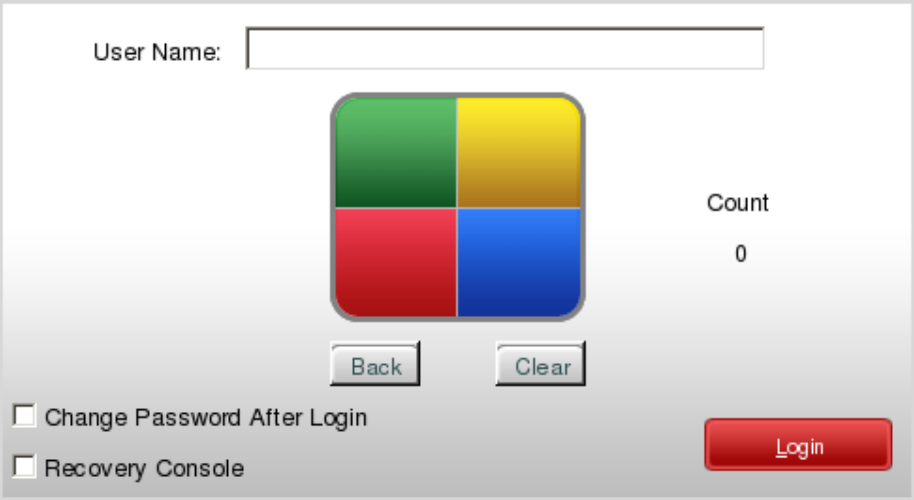



**FIGURE 2-1. ColorCode Authentication Screen**

## Domain Authentication

Endpoint Encryption integrates with Active Directory using LDAP configured in PolicyServer. Endpoint Encryption domain authentication allows Endpoint Encryption users to use single sign-on (SSO) between the operating system and the Endpoint Encryption agent. For example, Endpoint Encryption users with domain authentication must only provide their credentials once to authenticate to the Full Disk Encryption preboot, log on to Windows, and access the files protected by File Encryption.

For seamless Active Directory integration, make sure that the following requirements are met:

- PolicyServer has joined the domain.
- All Endpoint Encryption devices are in the same Active Directory and domain as PolicyServer.
- The user names configured in Active Directory exactly match the user names configured in PolicyServer (including case).
- The user names are located within a PolicyServer group and the Domain Authentication policy is enabled.
- The host name and domain name are configured correctly based on the LDAP or Active Directory server settings.

**Note**

For information about configuring LDAP and Active Directory settings, see the *Endpoint Encryption Installation Guide* available at:

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

## Fixed Password

Fixed password authentication is the most common authentication method. The fixed password is created by the user and can be almost any string of numbers, characters, or symbols. You can place restrictions on fixed passwords to ensure that they are not easily compromised.

## PIN

A Personal Identification Number (PIN) is common identification method requiring a unique sequences numbers. The PIN is created by the user and can be almost anything. Similar to fixed passwords, you may place restrictions on the PIN combination.

## Remote Help

Remote Help allows Group or Enterprise Authenticators to assist Endpoint Encryption users who are locked out and cannot log on to Endpoint Encryption devices after too

many unsuccessful log on attempts, or when the period between the last PolicyServer synchronization has been too long.

**Note**

Remote Help authentication is triggered by Endpoint Encryption device policy rules. Remote Help policy rules are configurable in both PolicyServer MMC and Control Manager.

## Self Help

Self Help authentication allows Endpoint Encryption users who have forgotten the credentials to answer security questions and log on to Endpoint Encryption devices without getting Technical Support assistance. Self Help requires the Endpoint Encryption user to respond with answers to predefined personal challenge questions. Self Help can replace fixed password or other authentication methods.

Consider the following when choosing your authentication method or when configuring Self Help:

- Self Help is not available for Administrator and Authenticator accounts.
- Self Help is not available for accounts that use domain authentication. PolicyServer is unable to change or retrieve previous domain passwords.
- Self Help has a maximum of six questions for each user account. Users may be unable to log on using Self Help if more than six questions are configured.
- Self Help is only configurable with PolicyServer MMC.

## Smart Card

Smart card authentication requires both a PIN and a physical token to confirm the user identity. Smart card certificates are associated with the user account and the user's assigned group. Once registered, the user can use smart card authentication from any Endpoint Encryption device in that group. Users are free to use any Endpoint Encryption device in their group and do not need to ask for another one-time password.

To use smart card authentication, make sure that the following requirements are met:

- The smart card reader is connected to the endpoint and the smart card is inserted into the smart card reader.
- ActivClient 6.2 with all service packs and updates installed.

**Note**

ActivClient 7.0 and later is not supported.

- Specify the smart card PIN in the password field.

**WARNING!**

Failure to provide a correct password sends a password error and may result in locking the smart card.

**Note**

- Smart card authentication is only configurable with PolicyServer MMC.
- Switching the authentication method from smart card to domain authentication may cause issues for domain users added through ADSync or Active Directory User Import. To resolve this issue, remove the domain user account from the enterprise, and then restart the PolicyServer services to start synchronization with the AD server. The synchronization process adds the user back with domain authentication as the authentication method. Alternatively, you can also add the domain user account back via Active Directory User Import.

# Chapter 3

# Getting Started with PolicyServer MMC

The PolicyServer Microsoft Management Console plug-in (PolicyServer MMC) is the native management console for Endpoint Encryption policy, user, and device administration.

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

Use PolicyServer MMC to centrally manage:

- All Endpoint Encryption users, devices, and groups
- All policies including encryption, password complexity and authentication
- Remote device actions, including killing a device, erasing data, or delaying authentication
- Event logs about authentication events, management events, device encryption status, and security violations
- Remote Help password reset process
- Auditing and reporting options

Before configuring PolicyServer MMC to manage PolicyServer, make sure to install and configure PolicyServer services and databases.

**Note**

For information about installing and configuring PolicyServer MMC, see the *Endpoint Encryption Installation Guide*.

Topic include:


- *Logging on to PolicyServer MMC on page 3-3*
- *PolicyServer MMC Interface on page 3-4*
- *Working with Groups and Users on page 3-6*
- *Understanding Policy Controls on page 3-15*
- *Disabling Agents on page 3-19*
- *Active Directory Synchronization on page 3-20*

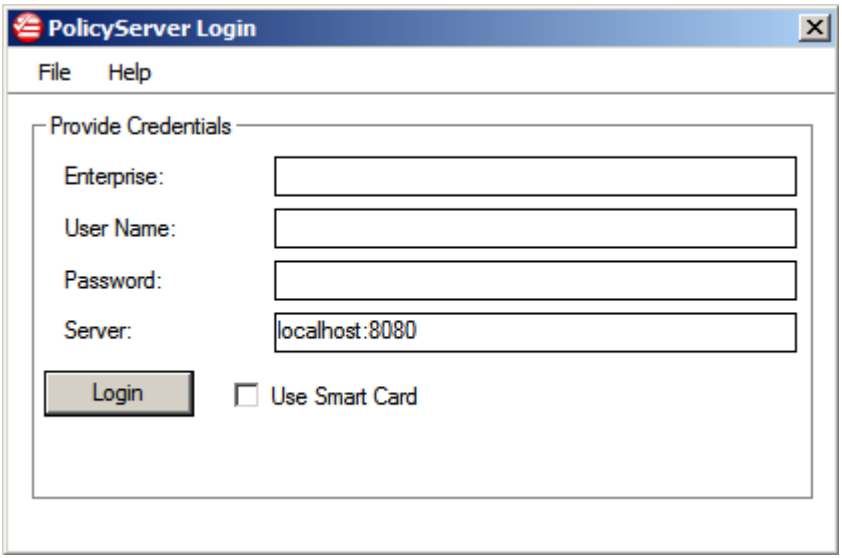
# Logging on to PolicyServer MMC

**Procedure**

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

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

   The PolicyServer MMC authentication screen appears.




2. Specify the following parameters:

| Option | Description |
|---|---|
| Enterprise | Specify the Enterprise. |
| User name | Specify the user name of an Enterprise administrator account. |

| OPTION | DESCRIPTION |
|---|---|
| Password | Specify the password for the user name. |
| Server | Specify the PolicyServer IP address or host name, and include the port number assigned to that configuration. |

3. Optional: To use a smart card to authenticate, select **Use Smart Card**.

4. Click **Login**.

The PolicyServer MMC opens.

# PolicyServer MMC Interface

The PolicyServer MMC interface contains the following panes:

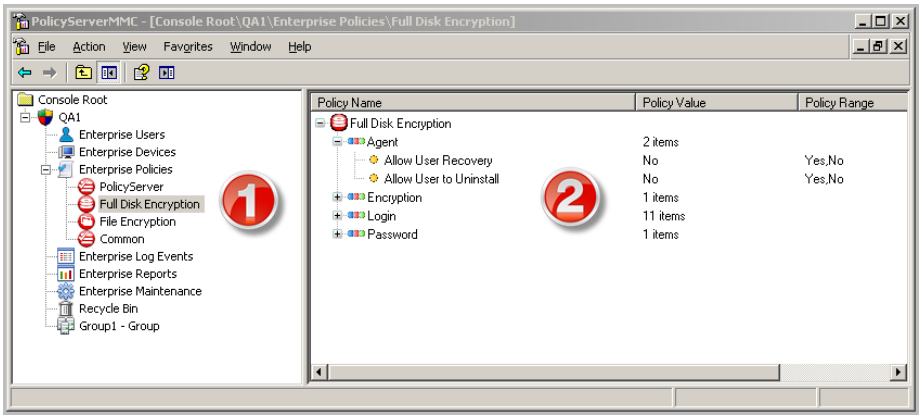



**FIGURE 3-1. PolicyServer MMC Interface**

**TABLE 3-1. PolicyServer MMC Interface Description**

| PANE | DESCRIPTION |
|---|---|
| Left (1) | Use the left pane to view users, groups, policies, devices, and agents. Expand a node to manage nested items within the tree structure. Opening an item updates the content in the right pane. |
| Right (2) | Use the right pane to modify policies, update user and group information, view reports, and maintain other functions. The exact format of the information shown in the right pane depend from the left pane. |

Within the left pane tree structure, there are a number of different nodes. The following table describes each node:

**TABLE 3-2. PolicyServer MMC Tree Description**

| NODE | DESCRIPTION |
|---|---|
| Enterprise Users | View all administrator and user accounts within the Enterprise. To see group affiliation, open the group and then click **Users**. |
| Enterprise Devices | View all instances of Endpoint Encryption agents and which Endpoint Encryption device they are connecting from. To see group affiliation, open the group and then click **Devices**. |
| Enterprise Policies | Control whether agents can connect to PolicyServer. Also, manage all enterprise policies. Group policies override enterprise policies. |
| Enterprise Log Events | View all log entries for the enterprise. |
| Enterprise Reports | Manage various reports and alerts. No group-only reports are available. |
| Enterprise Maintenance | Manage the PolicyServer MMC application plug-ins. |
| Recycle Bin | View deleted Endpoint Encryption users and devices. |
| Groups | Manage Endpoint Encryption users, devices, policies and log events for a collection of users. |

# Working with Groups and Users

This section explains how to get started with the PolicyServer MMC groups and users. First define the users and groups, and then assign users to groups. It is also possible to add new users directly to a group. At least one Top Group is required.

User and group recommendations:

- Follow the Active Directory structure.
- Create a new group whenever there is a policy difference between groups of users. If one group requires domain authentication and another requires fixed password, then two separate groups are required.
- Create multiple groups to minimize access. All members of a group are allowed access to any Endpoint Encryption device in that group.

Topics include:


- *Defining Users and Groups on page 3-6*
- *Adding a Top Group on page 3-7*
- *Adding a New User to a Group on page 3-8*
- *Adding a New Enterprise User on page 3-11*
- *Adding an Existing User to a Group on page 3-13*


## Defining Users and Groups

Define all roles and group affiliations before adding any users or groups.

1. Identify Enterprise Administrator/Authenticator accounts.
2. Create Enterprise Administrator/Authenticator accounts.
3. Identify groups.
4. Create groups.
5. Identify Group Administrator/Authenticator accounts.

6. Create Group Administrator/Authenticator accounts.
7. Identify users to be assigned to each group.
8. Import or create new users each group.

## Adding a Top Group

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

**Note**

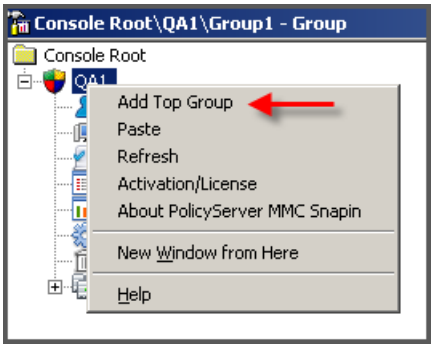
Enterprise administrators and authenticators may not be added to groups because their permissions supercede all groups. If you add an administrator or authenticator to a group, that account will be a group administrator or authenticator.

For more information, see *Modifying a User on page 6-9*.

**Procedure**

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

   The **Add New Group** screen appears.

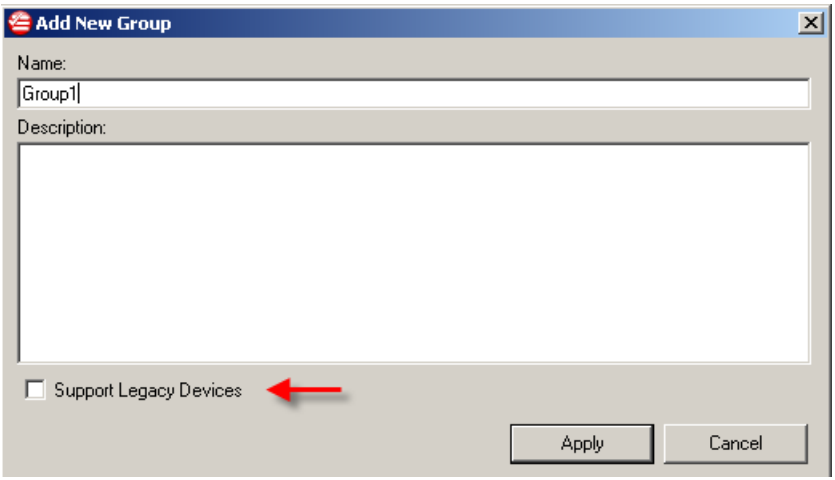



2. Specify the name and description for the group.

3. If using Endpoint Encryption devices that do not support Unicode, select **Support Legacy Devices**.

**Note**

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




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

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

## Adding a New User to a Group

**Note**

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

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

**Procedure**

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

   The **Add New User** screen appears.

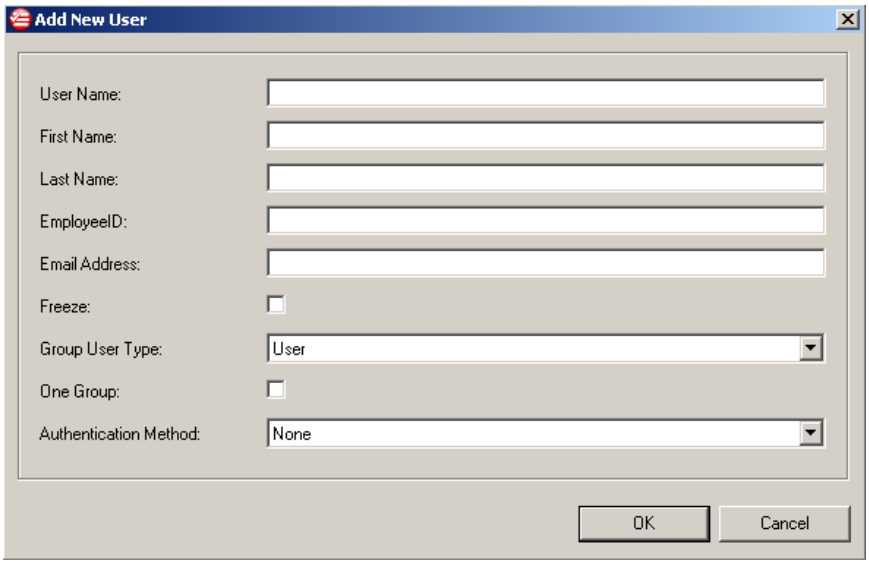



**FIGURE 3-2. Add New User Screen**

3. Specify the following options:

| OPTION | DESCRIPTION |
|---|---|
| User Nme | Specify the user name for the new user account (required). |
| First Name | Specify the first name for the new user account (required). |
| Last Name | Specify the last name for the new user account (required). |
| EmployeeID | Specify the employee ID for the new user account (optional). |

| OPTION | DESCRIPTION |
|---|---|
| Freeze | Select whether to temporarily disable the new user account (optional). While frozen, the user is unable to log on devices. |
| Group User Type | Select the privileges of the new account.<br><br>**Note**<br>For information about account roles, see *Users on page 4-3*.<br><br>Options include:<br>• User<br>• Authenticator<br>• Administrator<br><br>**Note**<br>Giving a user in a group administrator or authenticator privileges only applies those privileges within that group. That user is treated as a group administrator or group authenticator. Add an administrator or authenticator in the Enterprise, outside of the group, to give that user Enterprise-level privileges. |
| One Group | Select whether the new user account is allowed to be a member of multiple group policies. |
| Authentication method | Select the method that the new user account uses to log on to Endpoint Encryption devices. Options include:<br><br>**Note**<br>The default authentication method for users is **None**.<br><br>For information about account roles, see *Users on page 4-3*. |

4. Click **OK**.

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

## Adding a New Enterprise User

The following procedure explains how to add new Endpoint Encryption users to the Enterprise.

**Note**

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

Adding a new Endpoint Encryption user to a group adds the user to the group and to the Enterprise.

**Procedure**

1. To access Enterprise Users, do one of the following:
   - Expand the Enterprise, then open **Enterprise Users**.
   - Expand the Enterprise, expand the group, then open **Users**.
2. Right-click the white space in the right pane and select **Add User**.

The **Add New User** screen displays.

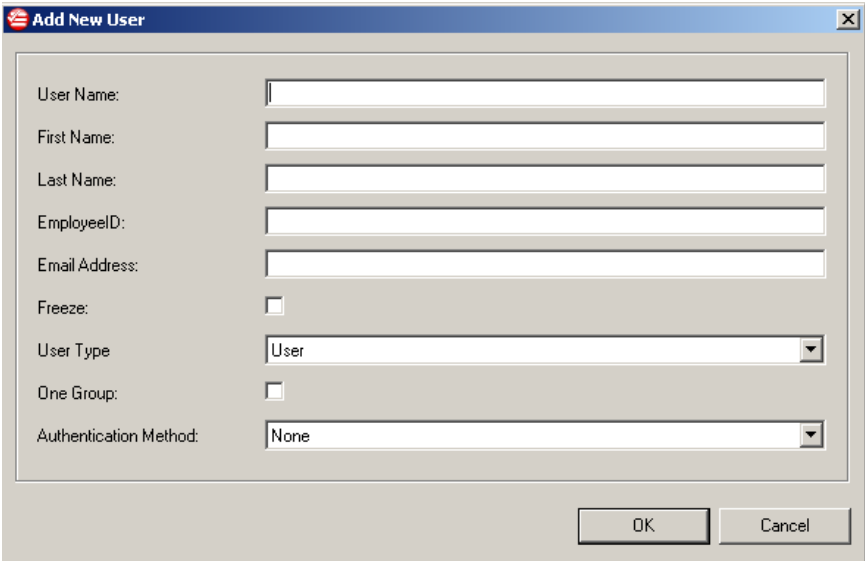



**FIGURE 3-3. Add New User screen**

3. Specify the following options:

| OPTION | DESCRIPTION |
|---|---|
| User name | Specify the user name for the new user account (required). |
| First name | Specify the first name for the new user account (required). |
| Last name | Specify the last name for the new user account (required). |
| EmployeeID | Specify the employee ID for the new user account (optional). |
| Freeze | Select whether to temporarily disable the new user account (optional). While frozen, the user is unable to log on to devices. |
| Group User Type | Select the privileges of the new account. For information about account roles, see *Authentication Overview on page 4-2*.<br><br>Options include: |

| OPTION | DESCRIPTION |
|---|---|
| | • **User**<br>• **Authenticator**<br>• **Administrator**<br><br>**Note**<br>It is not possible to add Enterprise Administrator or Authenticator accounts to groups. |
| One Group | Select whether the new user account is allowed to be a member of multiple group policies. |
| Authentication method | Select the method that the new user account uses to log on to Endpoint Encryption devices. For information about authentication methods, see *Authentication Overview on page 4-2*.<br><br>**Note**<br>The default authentication method for users is **None**. |

4. Click **OK**.

   The new Endpoint Encryption user is added the Enterprise. The user cannot log on to Endpoint Encryption devices until the user account is added to a group.

## Adding an Existing User to a Group

A user can be a member of multiple groups.

**Procedure**

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

The **Add Users To Group** screen appears.

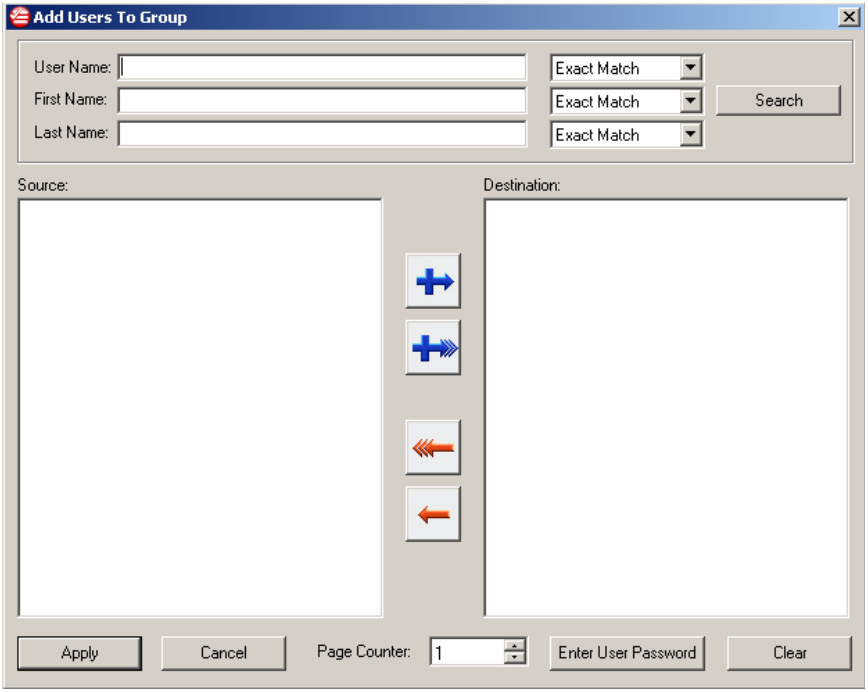



**FIGURE 3-4. Add Users To Group Screen**

3. Specify user details and then click **Search**.

   The **Source** field populates with any accounts that match the search criteria.

4. Select users from the **Source** list and click the blue arrow to add them.

   For information about search icons, see *Add/Remove Search Result Icons on page 6-14*.

   The selected user moves to the **Destination** list.

5. To change a user password:

   a. In the **Destination** list, highlight the user.

b. Click **Enter User Password** located at the bottom of the window.

c. In the window that appears, specify the user's authentication method.

d. Click **Apply** to close the **Change Password** window.

6. Click **Apply** to save changes.

   The user is added to the group. If this is the only group assignment, then the user is now able to log on to Endpoint Encryption devices.

# Understanding Policy Controls

After adding and configuring the users and groups, set policies for the Enterprise or group. Each group (whether a Top Group or a subgroup) contains a "Policies" node with policies specific to each agent and other common policies that affect all agents and authentication.

**Note**

To disable or enable policies at the Enterprise or group level, see *Accessing Policies on page 4-7*.

For information about the PolicyServer MMC interface, see *PolicyServer MMC Interface on page 3-4*.

Topics include:


- *Policy Visual Indicators on page 3-15*
- *Policy Fields and Buttons on page 3-16*
- *Modifying Policies on page 3-17*


## Policy Visual Indicators

The small circles to the left of each policy indicate one of the following states:

- Policy level
- Group modification status
- Single or multiple array of values
- Whether the policy contains sub-policies

**TABLE 3-3. Policy Indicators**

| INDICATOR | DESCRIPTION |
|---|---|
| | A single yellow circle indicates the policy value is inherited from the parent group or the Enterprise. |
| | A single blue circle indicates a policy has been modified for the group. |
| | Three blue circles indicate the policy may have multiple arrays of values. |
| | Three multi-colored (red, blue, green) circles indicate the policy will always have one or more sub-policies. |

## Policy Fields and Buttons

The following table explains the fields and buttons to control policies in PolicyServer MMC. All modified values are propagated to a group's subgroups. Only the relevant fields and buttons show in a selected policy.

**TABLE 3-4. Policy Fields and Buttons**

| FIELD/BUTTON | DESCRIPTION | CHANGEABLE? |
|---|---|---|
| OK | Saves changes to the selected policy | N/A |
| Description | Explains the selected policy | No |
| Policy Range | Displays the value range that the selected policy can fall between | Yes |

| Field/Button | Description | Changeable? |
|---|---|---|
| Policy Value | Depending on the policy, displays the actual value of the selected policy, whether it contains a string, number, or series of entries | Yes |
| Policy Multiple Value | Specifies whether this policy can be used multiple times for different settings (multiple “if found” strings) | No |
| Policy Name | Displays the name of the selected policy | No |
| Policy Type | Specifies the category for the selected policy | No |
| Enterprise controlled | Makes this policy mirror changes to the same policy at the Enterprise level | Yes |
| Save to subgroups | Pushes policy settings to the same policy in all subgroups | Yes |

## Modifying Policies

The PolicyServer MMC has a common set of windows to modify policies. Different types of input are available depending on what the policy controls and which parameters are required. This task gives a general overview about editing a policy. The steps required to edit one policy are different to modify another policy.

**Note**

For more information about modifying policies, including explanations about configuring different policy types, see *Accessing Policies on page 4-7*.

**Procedure**

1. Expand the **Enterprise**.
2. Select the policy level to modify.
   - For enterprise policies, expand **Enterprise Policies**.

- For group policies, expand the **Group Name** and then expand **Policies**.

3. Open the specific application or select **Common**.

   The policy list displays in the results windows.

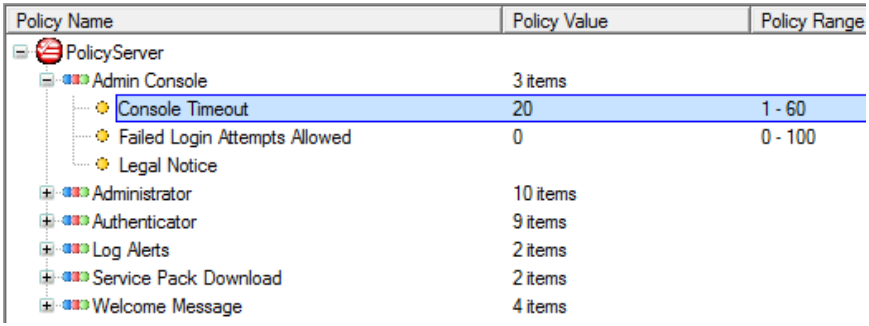



**FIGURE 3-5. Modifying a Policy**

4. Go to a policy and double-click to open the editor window.

For example, the “Console Timeout” policy:

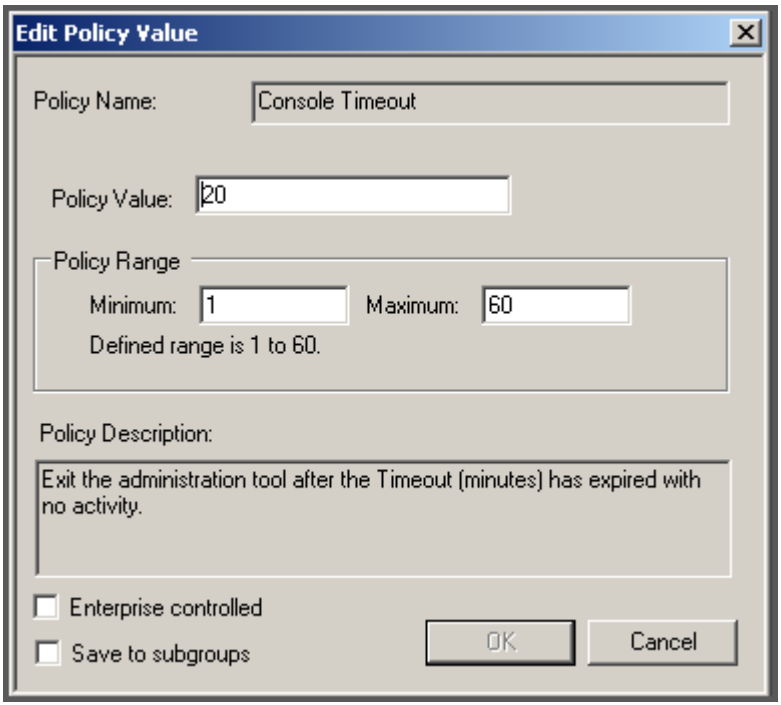



**FIGURE 3-6. “Console Timeout” Policy Editor Window**

5. Specify changes appropriate for the policy, then click **OK**.

# Disabling Agents

All Endpoint Encryption agents are enabled by default.

**Procedure**

1. Log on to PolicyServer MMC.

See *Logging on to PolicyServer MMC on page 3-3*.

2. Do one of the following:

   - To disable the agent across the Enterprise, click **Enterprise Policies**.
   - To disable the agent for users in the group only, expand the group and then click **Policies**.

   All applications appear in the right pane.

3. Right-click the application and then select **Disable**.

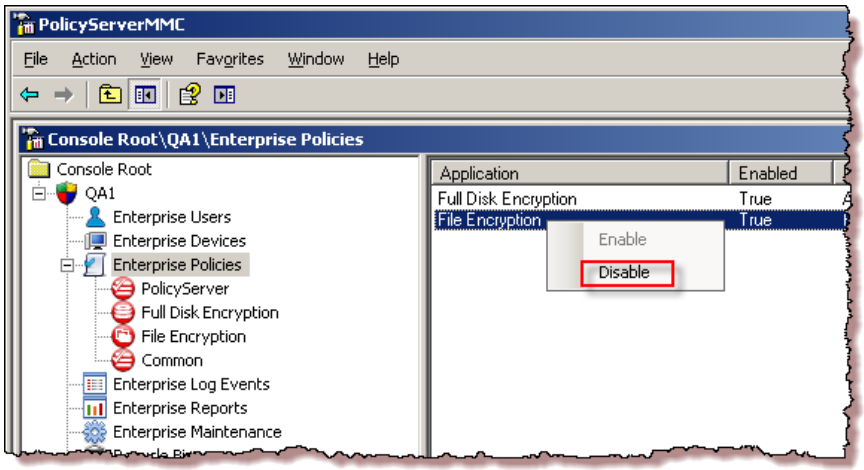



**FIGURE 3-7. Enable/Disable Agents**

The Endpoint Encryption agent is disabled. Endpoint Encryption users cannot log on devices using this agent.

# Active Directory Synchronization

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

Topics include:


- *Active Directory Overview on page 3-21*
- *Configuring Active Directory on page 3-22*
- *Importing Active Directory Users on page 3-24*


## Active Directory Overview

Three items are required to enable PolicyServer AD synchronization:

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

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

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

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

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

If you remove the Endpoint Encryption user from a paired group in PolicyServer, that domain user will not automatically be re-added by the synchronization system. This prevents overriding the your action for this Endpoint Encryption user. If you manually move a synchronized domain user back into a paired group then the synchronization system will again begin to automatically maintain the user in the group.

## Configuring Active Directory

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

**Procedure**

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

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

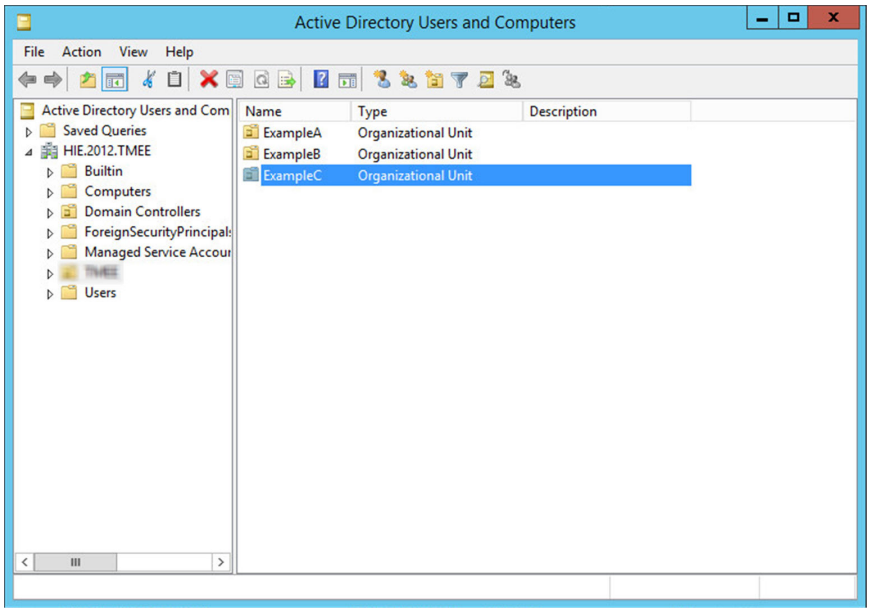



**FIGURE 3-8. Active Directory Users and Computers**

2. Create your organizational units (OUs).

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

   a. Right-click the new domain created during AD installation and then select **New**.

b. Select **Organizational Unit**.

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

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

**Important**

Endpoint Encryption supports up to 12 OUs per policy.

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

**3.** Add new users to your OUs.

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

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

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

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

**Note**

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

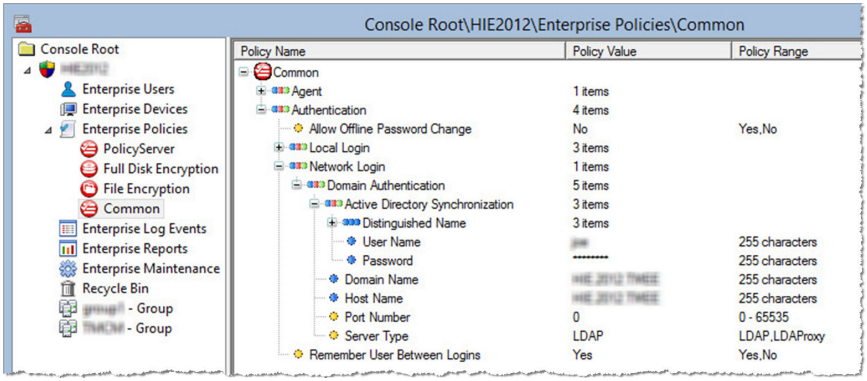
d. When prompted to complete, click **Finish**.

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

# Importing Active Directory Users

**Procedure**

1. Log on to PolicyServer MMC.
2. Set your enterprise as a top level group.
   a. Right-click the enterprise and select **Create Top level Group**.
   b. Specify the name and description for the group.
   c. Click **Apply**.
3. To configure the synchronization policy, open the group and go to **Enterprise Policies** > **Common** > **Authentication** > **Network Login** > **Domain Authentication** > **Active Directory Synchronization**.




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

   For each OU to synchronize, perform the following steps:

   a. Right-click **Distinguished Name** and click **Add**.
   b. In the **Policy Value** section, specify the OU by its sequence of relative distinguished names (RDN) separated by commas.

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

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

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

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

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

# Chapter 4

# Policies in PolicyServer MMC

This chapter explains how to manage and configure Endpoint Encryption policies with PolicyServer MMC.

**Note**

For information about the policy mapping between PolicyServer MMC and Control Manager, see *Policy Mapping Between Management Consoles on page C-1*.

Topics include:


- *Authentication Overview on page 4-2*
- *Policy Overview on page 4-5*
- *Policy Synchronization on page 4-18*
- *PolicyServer Policies on page 4-18*
- *Full Disk Encryption Policies on page 4-23*
- *File Encryption Policies on page 4-33*
- *Common Policies on page 4-37*

# Authentication Overview

The primary form of protection that Endpoint Encryption delivers is prevention of uauthorized user access to encrypted endpoints and devices. Correctly configuring Endpoint Encryption devices, users, and policy groups prevents data loss risk from accidental information release or deliberate sabotage.

| | |
|---|---|
| *Groups on page 4-2* | Groups act as a container for users for policy management. Administrators and authenticators within a group have those special privileges only within that group, but unassigned administrators and authenticators have that role throughout the Enterprise. |
| *Users on page 4-3* | Endpoint Encryption counts the amount of consecutive logon attempts by a particular user account on a device. If that user violates the policy criteria, Endpoint Encryption can reset, lock, or erase the disk. |
| *Devices on page 4-5* | Endpoint Encryption counts the amount of consecutive logon attempts on a given device or when an agent does not communicate with PolicyServer for a given length of time. If a device violates the policy criteria, Endpoint Encryption can reset, lock, or erase the disk. |

For a complete list of the configurable methods to authenticate users and devices, see *Authentication Methods on page 2-13*.

## Groups

Endpoint Encryption manages policies by user groups. Groups management differs between PolicyServer MMC and Control Manager. After modifying policies and groups, PolicyServer synchronizes groups across both consoles.

**Important**

Control Manager always takes precedence over PolicyServer MMC for policy and group assignment. Any modifications to the group assignment in PolicyServer MMC are automatically overwritten the next time that Control Manager synchronizes with PolicyServer.

| CONSOLE | GROUP MANAGEMENT |
|---|---|
| Control Manager | Endpoint Encryption automatically creates a group each time a policy with specific targets is deployed. After deployment, modify the groups a user is in from the **Endpoint Encryption Users** widget, and modify the users in the policy from the **Policy Management** screen. |
| PolicyServer MMC | Add and modify groups directly from the left pane of PolicyServer MMC. Groups in PolicyServer MMC can be assigned as follows:<br>• **Top Group**: Top Groups are the highest level of groups under the Enterprise. Each Top Group has a unique node underneath the Enterprise.<br>• **Subgroup**: Subgroups are created within Top Groups. Subgroups inherit the policies of the Top Group on creation, but do not inherit changes made to the Top Group. Subgroups may not be more permissive than the Top Group.<br>**Note**<br>You must manually assign devices and users to each subgroup. Adding Endpoint Encryption users to a subgroup does not automatically add the users to the Top Group. However, you can add users to both the Top Group and subgroup. |

**Note**

To configure users within a policy group on PolicyServer MMC, see *Groups in PolicyServer MMC on page 5-1*.

To configure the users within a policy group on Control Manager, see the *Endpoint Encryption Administrator's Guide*.

## Users

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

Endpoint Encryption has several types of account roles and authentication methods for comprehensive identity-based authentication and management. Using Control Manager

or PolicyServer MMC, you can add or import user accounts, control authentication, synchronize with the Active Directory, and manage policy group membership, as needed.

The following table describes the Endpoint Encryption user roles:

| ROLE | DESCRIPTION |
|---|---|
| Administrator | Administrators may access the management consoles and perform any configurations within their domain. This role has different rights depending on the level that the administrator role is added:<br>• Enterprise administrator: These administrators have control over all policies, groups, users, and devices in the enterprise.<br>• Group administrator: These administrators have control over users and devices that authenticate within a specific group. Control Manager makes a group for each policy, so these administrators may also be known as “policy administrators”. |
| Authenticator | Authenticators provide remote assistance when users forget their Endpoint Encryption passwords or have technical problems. This role has different rights depending on the level that the authenticator role is added:<br>• Enterprise authenticator: These authenticators can assist any users in the enterprise.<br>• Group authenticator: These authenticators can assist any users within a specific group. Control Manager makes a group for each policy, so these authenticators may also be known as “policy authenticators”. |
| User | Basic end users have no special privileges. The user role may not log on the Endpoint Encryption management consoles. Unless allowed by PolicyServer, the user role also may not use recovery tools. |

**Note**

To configure Endpoint Encryption users, see *Users in PolicyServer MMC on page 6-1*.

## Devices

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

Depending on the policy settings, too many consecutive unsuccessful authentication attempts to the Endpoint Encryption devices delays the next authentication attempt, locks the Endpoint Encryption device, or erases all data controlled by the associated Endpoint Encryption agent.

**Note**

To configure Endpoint Encryption devices, see *Devices in PolicyServer MMC on page 7-1*.

# Policy Overview

This section explains how to use various windows to change a policy, but does not explain the process to modify every policy. PolicyServer MMC has a common set of windows to use when modifying a policy. One policy may have an editor window available to edit the numbers, ranges and values associated with the policy while another policy may have a window to modify text strings.

When managing policies, note the following:

- Policies are configurable by the agent within each group.
- Policy inheritance only occurs when a subgroup exists. For information about group permissions, see *Groups on page 4-2*.
- Every policy has a default value.

Topics include:

- *Policy Visual Indicators on page 3-15*
- *Policy Fields and Buttons on page 3-16*

- *Accessing Policies on page 4-7*
- *Selecting a Policy for Modification on page 4-8*
- *Editing Policies with Ranges on page 4-8*
- *Editing Policies with True/False or Yes/ No Responses on page 4-10*
- *Editing Policies with Multiple-choice / Single-selection on page 4-12*
- *Editing Policies with Text String Arguments on page 4-15*
- *Editing Policies with Multiple Options on page 4-16*


## Policy Visual Indicators

The small circles to the left of each policy indicate one of the following states:

- Policy level
- Group modification status
- Single or multiple array of values
- Whether the policy contains sub-policies

**TABLE 4-1. Policy Indicators**

| INDICATOR | DESCRIPTION |
|---|---|
| | A single yellow circle indicates the policy value is inherited from the parent group or the Enterprise. |
| | A single blue circle indicates a policy has been modified for the group. |
| | Three blue circles indicate the policy may have multiple arrays of values. |
| | Three multi-colored (red, blue, green) circles indicate the policy will always have one or more sub-policies. |

## Policy Fields and Buttons

The following table explains the fields and buttons to control policies in PolicyServer MMC. All modified values are propagated to a group's subgroups. Only the relevant fields and buttons show in a selected policy.

**TABLE 4-2. Policy Fields and Buttons**

| FIELD/BUTTON | DESCRIPTION | CHANGEABLE? |
|---|---|---|
| OK | Saves changes to the selected policy | N/A |
| Description | Explains the selected policy | No |
| Policy Range | Displays the value range that the selected policy can fall between | Yes |
| Policy Value | Depending on the policy, displays the actual value of the selected policy, whether it contains a string, number, or series of entries | Yes |
| Policy Multiple Value | Specifies whether this policy can be used multiple times for different settings (multiple “if found” strings) | No |
| Policy Name | Displays the name of the selected policy | No |
| Policy Type | Specifies the category for the selected policy | No |
| Enterprise controlled | Makes this policy mirror changes to the same policy at the Enterprise level | Yes |
| Save to subgroups | Pushes policy settings to the same policy in all subgroups | Yes |

## Accessing Policies

Every group in PolicyServer MMC contains one or more policy folders. The right pane shows the results window, which provides controls to:

- Display a list of policies and their values

- Modify a policy using the editor window
- Run reports and other log events
- Run enterprise maintenance

**Note**

For information about the PolicyServer MMC interface, see *PolicyServer MMC Interface on page 3-4*.

## Selecting a Policy for Modification

**Procedure**

1. Go to **Group Name** > **Policies** and select the appropriate node.

   Example: **Group1** > **Policies** > **Full Disk Encryption**.

2. Go to the specific policy.

   Example: **Common** > **Client** > **Allow User to Uninstall**.

3. Right-click the policy and select **Properties**.

## Editing Policies with Ranges

Some policies have controls to set a range of policy values, such as the minimum and maximum length for a password.

An example of editing policies with ranges is the **Failed Login Attempts Allowed** policy. **Failed Login Attempts Allowed** controls whether a device locks when a user exceeds the number of failed authentication attempts allowed.

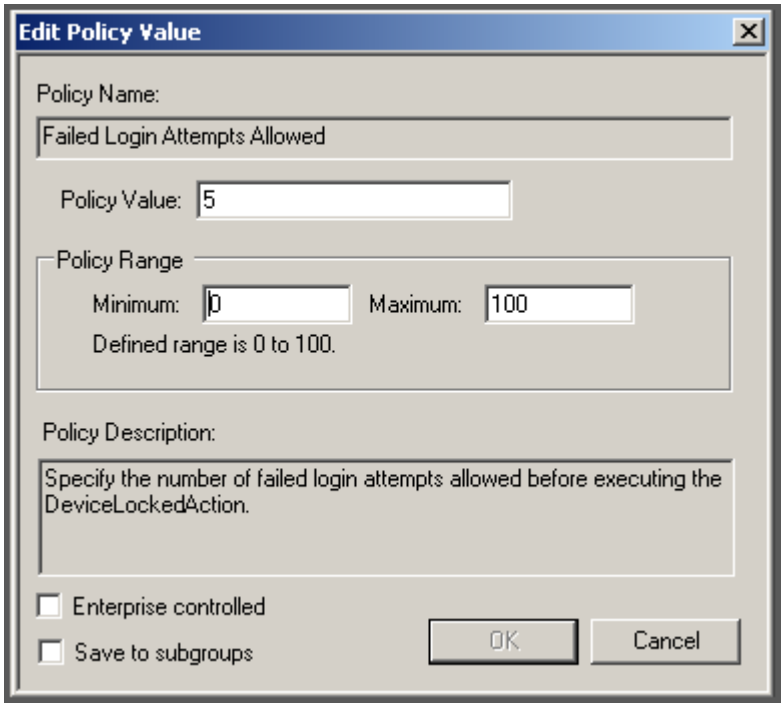



**FIGURE 4-1. Policy with Ranges Window**

Using the parameters defined in the **Policy Range** fields, indicate the number of failed authentication attempts allowed per user in the **Policy Value** field.

---

**Procedure**

1. Right-click the policy to be modified and then click **Properties**.
2. In the **Minimum** field, specify the lowest number of unsuccessful authentication attempts allowed by a user in this group before locking the device.

**Note**

The minimum and maximum values for the policy range can be the same as the parent's range, or they can be modified with unique values. It is not possible to extend the minimum and maximum values.

3. In the **Maximum** field, specify the highest number of authentication attempts that can be made by a user in this group before authentication fails and the device is locked.

4. In the **Policy Value** field, specify the number of failed authentication attempts allowed for a user in this group before the device is locked.

5. Click **OK** to save changes.

   The policy change is activated once the Endpoint Encryption agent synchronizes with PolicyServer.

## Editing Policies with True/False or Yes/ No Responses

Some policies only have True/False or Yes/No options. For this example, **Preboot Bypass** is used.

A Group Administrator can define whether the Full Disk Encryption preboot appears before Windows starts. If the parent group allows **Yes** and **No**, then the subgroup Group Authenticators have the right to set the range to **Yes** and **No**, just **Yes**, or just

**No**. If the parent group has set the range to either **Yes** or **No**, then the subgroup Group Administrator can only select that same range.

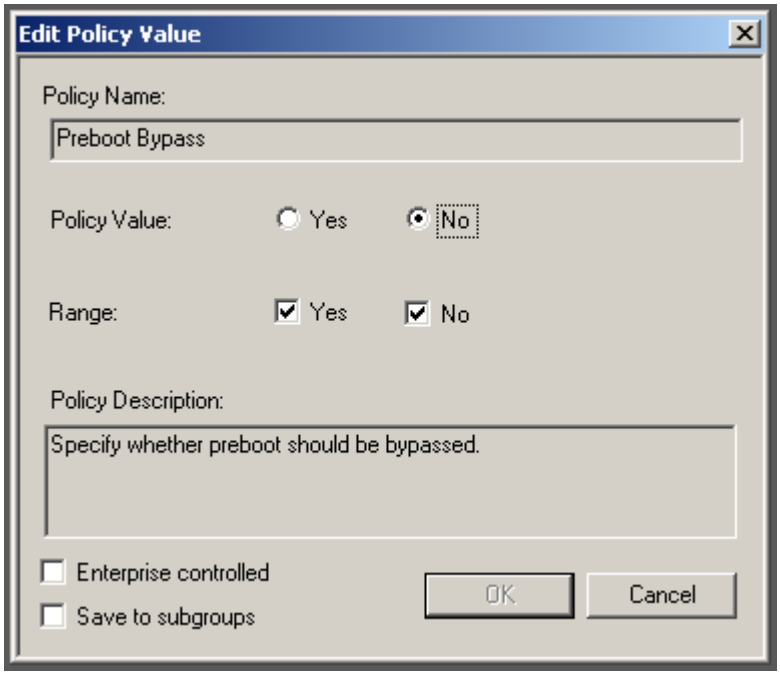



**FIGURE 4-2. Policy with Yes/No Values**

**Procedure**

1. Right-click the policy to be modified and then click **Properties**.
2. Specify policy options.
   - The **Policy Value** field sets whether the policy is turned on.
   - The **Range** field sets whether the policy is available to other users or groups.

     Example: if the policy is set to **No**, then the policy will not be available to set to **Yes**.

**Note**

Removing an option from **Policy Range** removes the value from the **Policy Value** drop-down in the current group and all subgroups.

3. Click **OK** to save changes.

   The policy change is activated once the Endpoint Encryption agent synchronizes with PolicyServer.

## Editing Policies with Multiple-choice / Single-selection

Some policies have multiple options available for selection. The **Device Locked Action** policy is edited in a multiple-choice/single-selection window. You can only select one

**Policy Value**. In this example, the Group Administrator must define the action to take when a user exceeds the allowed number of authentication attempts.

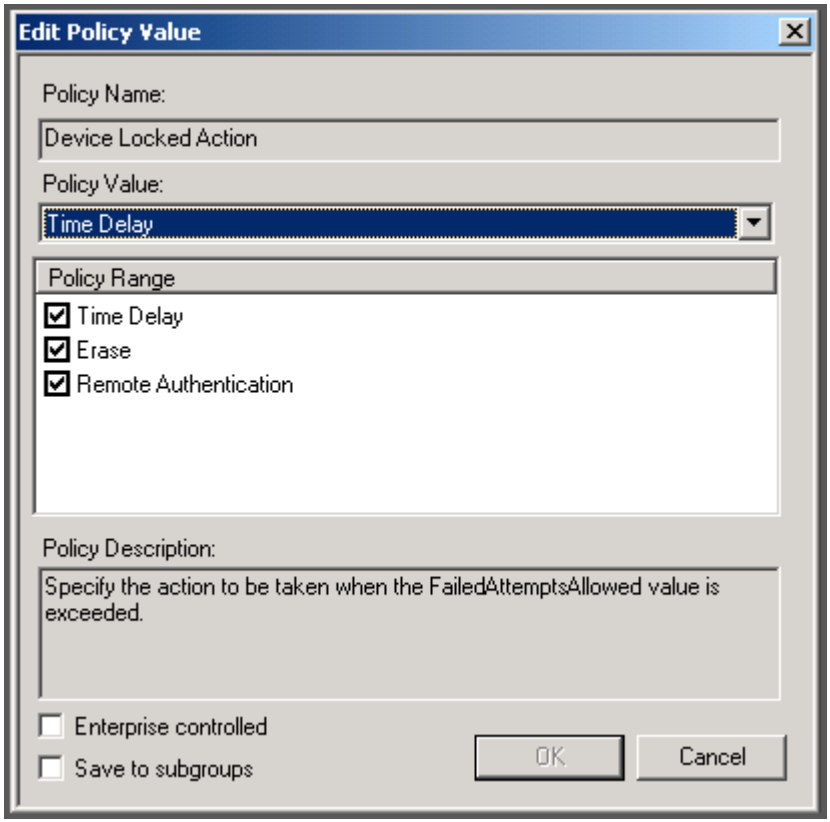



**FIGURE 4-3. Policy with Multiple Choice/Single Selection**

**Procedure**

1. Right-click the policy to be modified and then click **Properties**.
2. Select a default setting from the **Policy Value** drop-down list.
3. Select the available options for the **Policy Range** area.

**Note**

Removing an option from **Policy Range** removes the value from the **Policy Value** drop-down in the current group and all subgroups.

4. Click **OK** to save changes.

   The policy change is activated once the Endpoint Encryption agent synchronizes with PolicyServer.

## Editing Policies with Text String Arguments

Some policies have an editable text string for single array arguments. The **Dead Man Switch** policy is an example of a policy that provides the capability to specify a string of text.

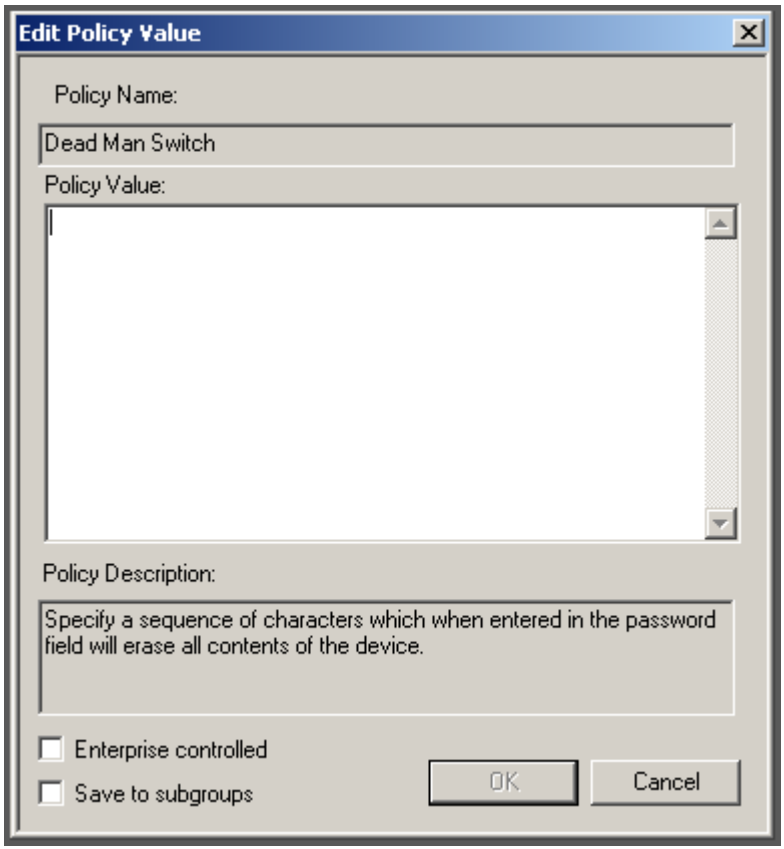



**FIGURE 4-4. Policy with Text String Argument**

**Procedure**

1. Right-click the policy to be modified and then click **Properties**.
2. Specify the sequence of characters for this policy in the **Policy Value** field, .
3. Click **OK** to save changes.

   The policy change is activated once the Endpoint Encryption agent synchronizes with PolicyServer.

## Editing Policies with Multiple Options

Some policies have multiple options stored in subpolicies affecting that policy. Multiple option policies create separate lines in a text string, and each new line in the string is a subpolicy. For example, the **IF Found** policy displays how to return a found device. A normal address format displays the name, street address, and city/state/zip on three separate lines.

**Note**

Depending on the policy, multiple options is generally limited to six subpolicies.

**Procedure**

1. Right-click the policy to modify and then click **Add**.

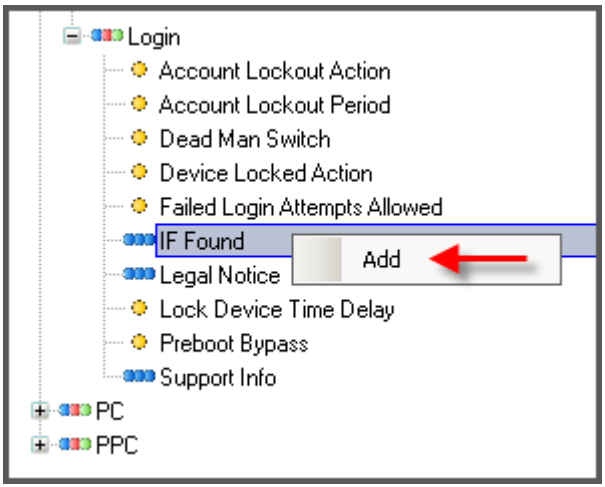



**FIGURE 4-5. If Found Policy: Adding a New Option**

2. Specify details in the **Policy Value** field.

---

**Note**

Depending on the policy, you may need to modify the added policy by right-clicking and selecting **Properties**.

---

3. Click **OK** to save changes.

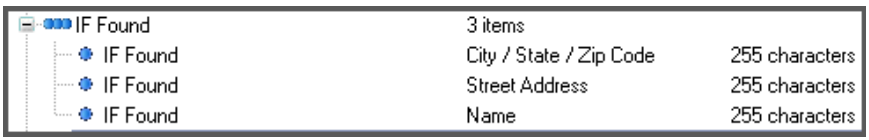



**FIGURE 4-6. If Found Policy: Results After Adding Multiple Options**

4. If needed, add a new option.

5. To make changes, right-click the child policy, then select **Properties**.

   The policy change is activated once the Endpoint Encryption agent synchronizes with PolicyServer.

---

# Policy Synchronization

The following list explains the events that initiate policy synchronization between agents and PolicyServer:

- After the operating system loads and the agent service starts

  **Note**

  For information about Endpoint Encryption services, see *Endpoint Encryption Services on page B-1*.

- At regular intervals based on the PolicyServer synchronization policy
- Manually, by clicking the **Synchronize Policies** button in the agent context menu

**Note**

Device actions initiate after the agent receives policy updates.

# PolicyServer Policies

This section explains the configurable options for policies affecting PolicyServer.

Topics include:


- *Admin Console Policies on page 4-19*
- *Administrator Policies on page 4-19*
- *Authenticator Policies on page 4-20*
- *Log Alert Policies on page 4-21*
- *Service Pack Download Policies on page 4-22*
- *Welcome Message Policies on page 4-22*

## Admin Console Policies

The following table explains the policies governing PolicyServer MMC.

**TABLE 4-3. PolicyServer Admin Console Policy Descriptions**

| POLICY NAME | DESCRIPTION | VALUE RANGE AND DEFAULT |
|---|---|---|
| **Console Timeout** | Exit the administration tool after the Timeout (minutes) has expired with no activity. | 1-60<br>Default: 20 |
| **Failed Login Attempts Allowed** | Lockout the administrator logon after this number of consecutive failed log on attempts. | 0-100<br>Default: 0 |
| **Legal Notice** | Contains the legal notice that must be displayed before the Administrator or Authenticator can use the administration tools. | 1-1024 chars<br>Default: N/A |

## Administrator Policies

The following table explains policies governing PolicyServer Group Administrator privileges.

**TABLE 4-4. PolicyServer Administrator Policy Descriptions**

| POLICY NAME | DESCRIPTION | VALUE RANGE AND DEFAULT |
|---|---|---|
| **Add Devices** | Specify whether the Group Administrator is allowed to add devices. | Yes, No<br>Default: Yes |
| **Add Users** | Specify whether the Group Administrator is allowed to add new users. | Yes, No<br>Default: Yes |
| **Add Users to Enterprise** | Specify whether the Group Administrator is allowed to add new users to the enterprise. | Yes, No<br>Default: No |

| POLICY NAME | DESCRIPTION | VALUE RANGE AND DEFAULT |
|---|---|---|
| **Add/Modify Groups** | Specify whether the Group Administrator is allowed to add/modify subgroups. | Yes, No<br>Default: Yes |
| **Change Policies** | Specify whether the Group Administrator is allowed to change policies. | Yes, No<br>Default: Yes |
| **Copy/Paste Groups** | Specify whether the Group Administrator is allowed to copy and paste subgroups. | Yes, No<br>Default: Yes |
| **Remove Devices** | Specify whether the Group Administrator is allowed to remove devices. | Yes, No<br>Default: Yes |
| **Remove Groups** | Specify whether the Group Administrator is allowed to remove subgroups. | Yes, No<br>Default: Yes |
| **Remove Users** | Specify whether the Group Administrator is allowed to remove users. | Yes, No<br>Default: Yes |
| **Remove Users from Enterprise** | Specify whether the Group Administrator is allowed to remove users from the enterprise. | Yes, No<br>Default: No |

## Authenticator Policies

The following table explains policies governing Enterprise and Group Authenticator rights and privileges.

**TABLE 4-5. PolicyServer Administrator Policy Descriptions**

| POLICY NAME | DESCRIPTION | VALUE RANGE AND DEFAULT |
|---|---|---|
| **Add Devices** | Specify whether Enterprise and Group Authenticators are allowed to add devices. | Yes, No<br>Default: No |

| Policy Name | Description | Value Range and Default |
|---|---|---|
| **Add Users** | Specify whether Enterprise and Group Authenticators are allowed to add new users. | Yes, No<br>Default: No |
| **Add Users to Enterprise** | Specify whether Enterprise and Group Authenticators are allowed to add new users to the enterprise. | Yes, No<br>Default: No |
| **Add/Modify Groups** | Specify whether Enterprise and Group Authenticators are allowed to add/modify subgroups. | Yes, No<br>Default: No |
| **Copy/Paste Groups** | Specify whether Enterprise and Group Authenticators are allowed to copy and paste subgroups. | Yes, No<br>Default: No |
| **Remove Devices** | Specify whether Enterprise and Group Authenticators are allowed to remove devices. | Yes, No<br>Default: No |
| **Remove Groups** | Specify whether Enterprise and Group Authenticators are allowed to remove subgroups. | Yes, No<br>Default: No |
| **Remove Users** | Specify whether Enterprise and Group Authenticators are allowed to remove users. | Yes, No<br>Default: No |
| **Remove Users from Enterprise** | Specify whether Authenticators are allowed to remove users from the enterprise. | Yes, No<br>Default: No |

## Log Alert Policies

The following table explains policies governing email messages sent for important PolicyServer log events.

**TABLE 4-6. PolicyServer Log Alerts Policy Description**

| POLICY NAME | DESCRIPTION | VALUE RANGE AND DEFAULT |
|---|---|---|
| **From Email Address** | Specify the email address that is used as the source email address for the alerts email message. | 1-255 characters<br>Default: N/A |
| **SMTP Server Name** | Specify the SMTP server responsible for sending alert email messages. | 1-255 characters<br>Default: N/A |

## Service Pack Download Policies

The following table explains policies governing when agents automatically download service packs.

**TABLE 4-7. PolicyServer Service Pack Download Policy Descriptions**

| POLICY NAME | DESCRIPTION | VALUE RANGE AND DEFAULT |
|---|---|---|
| **Service Pack Download Begin Hour** | Set the time to download service packs. | 0-23<br>Default: 0 |
| **Service Pack Download End Hour** | Set the time to stop downloading any service pack. | 0-23<br>Default: 0 |

## Welcome Message Policies

The following table explains policies governing whether to send a welcome message to users when they have been added to a group.

**TABLE 4-8. PolicyServer Welcome Message Policy Descriptions**

| POLICY NAME | DESCRIPTION | VALUE RANGE AND DEFAULT |
|---|---|---|
| **Message** | Contains the welcome message file. | 1-1024 characters<br>Default: N/A |
| **SMTP Server Name** | Specify the SMTP server responsible for sending welcome email messages. | 1-255 characters<br>Default: N/A |
| **Source Email** | Specify the email address that is used as the source email address for welcome email message. | 1-255 characters<br>Default: N/A |
| **Subject** | The Welcome message subject line. | 1-255 characters<br>Default: N/A |

# Full Disk Encryption Policies

This section explains the configurable options for policies affecting the following Full Disk Encryption agents:

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

Topics include:


- *Agent Policies on page 4-24*
- *Encryption Policies on page 4-26*
- *Login Policies on page 4-26*

- *Password Policies on page 4-32*

## Agent Policies

The following table explains the policies affecting Wi-Fi configuration, Full Disk Encryption Recovery Console access, and agent uninstallation.

**Note**

Encryption Management for Apple FileVault and Encryption Management for Microsoft BitLocker do not require authentication and are not affected by authentication policies. Client, login, password, and authentication policies, or allowing the user to uninstall the Endpoint Encryption agent software only affects the Full Disk Encryption and File Encryption agents.

**TABLE 4-9. Full Disk Encryption Client Policy Descriptions**

| POLICY NAME | DESCRIPTION | VALUE RANGE AND DEFAULT |
|---|---|---|
| **Allow User to Configure Wi-Fi** | Specify whether users are allowed to configure Wi-Fi policies on the device. | Yes, No<br>Default: Yes |
| **Allow User to Recover** | Specify whether users are allowed to access system recovery utilities on the device. | Yes, No<br>Default: No |
| **Allow User to Uninstall** | Specify whether users are allowed to uninstall Full Disk Encryption. | Yes, No<br>Default: No |
| **Wi-Fi Settings** | Specify the Wi-Fi settings | N/A |
| **Wi-Fi Settings** > **Network Name** | Specify the name or SSID of the network. | 1-255 characters |

| Policy Name | Description | Value Range and Default |
|---|---|---|
| **Wi-Fi Settings** > **Password** | Specify the network password.<br><br>**Note**<br>Ensure that the password meets the following length requirements:<br>• WEP password length:<br>5 to 10 characters, or 10 to 26 hexadecimal [0-9][a-f] characters<br>• WPA PSK password length:<br>8 to 63 characters, or 64 hexadecimal [0-9][a-f] characters<br>• WPA Enterprise user name and password length:<br>Less than 128 characters | 1-255 characters |
| **Wi-Fi Settings** > **Priority** | Specify the priority of the network. | 0-16<br><br>Default: 1 |
| **Wi-Fi Settings** > **Security Type** | Specify the security type for network authentication. | No authentication, WEP, WEP Open, WEP Shared, WPA2 Enterprise, WPA2 Personal, WPA Enterprise, WPA Personal<br><br>Default: WEP Open |

| Policy Name | Description | Value Range and Default |
|---|---|---|
| **Wi-Fi Settings** > **User Name** | Specify the user name if the network requires user-based authentication. | 1-255 characters |

## Encryption Policies

The following table explains the Full Disk Encryption encryption policy. The encrypt device policy affects the Full Disk Encryption, Encryption Management for Apple FileVault, and Encryption Management for Microsoft BitLocker agents.

**Table 4-10. Full Disk Encryption Policy Descriptions**

| Policy Name | Description | Value Range and Default |
|---|---|---|
| **Encrypt Device** | Specify whether to encrypt the device. | Yes, No<br>Default: Yes |
| **Encrypt Only Used Space** | Specify whether to encrypt only the used space. | Yes, No<br>Default: Yes |
| **Select Encryption Key Size** | Specify the device encryption key size in bits. | 128, 256<br>Default: 256 |

## Login Policies

The following table explains the policies that govern logging on to the Full Disk Encryption agent.

**Note**

Encryption Management for Apple FileVault and Encryption Management for Microsoft BitLocker do not require authentication and are not affected by authentication policies. Client, login, password, and authentication policies, or allowing the user to uninstall the Endpoint Encryption agent software only affects the Full Disk Encryption and File Encryption agents.

**TABLE 4-11. Full Disk Encryption Login Policy Descriptions**

| POLICY NAME | DESCRIPTION | VALUE RANGE AND DEFAULT |
|---|---|---|
| **Account Lockout Action** | Specify the action to be taken when the device has failed to communicate with the PolicyServer as specified in the policy Account Lockout Period.<br>• Erase: All content on the device is wiped.<br>• Remote Authentication: Require user to perform remote authentication. | Erase, Remote Authentication<br>Default: Remote Authentication |
| **Account Lockout Period** | Specify the number of days that the client may be out of communication with the PolicyServer. | 0-999<br>Default: 360 |
| **Dead Man Switch** | Specify a sequence of characters, when entered will erase all contents on the device. | 1-255 characters<br>Default: N/A |

| Policy Name | Description | Value Range and Default |
|---|---|---|
| **Device Locked Action** | Specify the action to be taken when the device locks.<br>• Time Delay: The amount of time that must elapse before the user can retry logging on.<br>• Erase: All content on the device is wiped.<br>• Remote Authentication: Require user to perform remote authentication. | Time Delay, Erase, Remote Authentication<br>Default: Time Delay |
| **Failed Login Attempts Allowed** | Specify the number of failed Login attempts before using Lock Device Time Delay. | 0-100<br>Default: 5 |
| **If Found** | Specify information to be displayed. | 1-255 characters<br>Default: N/A |
| **Legal Notice** | Specify whether a legal notice should be displayed. | Enable/Disable<br>Default: Disabled |
| **Legal Notice Display Time** | Specify when the configured legal notice should be displayed to the user. | Installation, Startup<br>Default: Startup |
| **Legal Notice Text** | Specify the body of the legal notice. | Insert File<br>Default: N/A |
| **Lock Device Time Display** | Lock device for X minutes if user exceeds Failed Attempts Allowed. | 1-999,999 minutes<br>Default: 1 |
| **Preboot Bypass** | Specify if the preboot should be bypassed. | Yes, No<br>Default: No |
| **Logon Background Color** | Specify the background color during logon. | Enable, Disable<br>Default: Disable |

| Policy Name | Description | Value Range and Default |
|---|---|---|
| **Logon Background Color** > **Blue Value** | Specify the blue value of the RGB color code. | 0-255<br>Default: 63 |
| **Logon Background Color** > **Green Value** | Specify the green value of the RGB color code. | 0-255<br>Default: 59 |
| **Logon Background Color** > **Red Value** | Specify the red value of the RGB color code. | 0-255<br>Default: 57 |
| **Logon Banner** | Specify if a banner image should be shown during logon. | Enable, Disable<br>Default: Disable |
| **Logon Banner** > **Logon Banner Image** | Specify the logon banner image. | Maximum size: 128 KB<br>Resolution: 512 x 64 pixels<br>File formats: PNG with transparency (recommended), JPG and GIF |
| **Support Info** | Display Help Desk information or Administrator contact. | Default: N/A |
| **Token Authentication** | Policy related to physical tokens including smart cards and USB tokens. All sub-policies are visible only when Token Authentication is enabled. | Enable, Disable<br>Default: Disable |

| Policy Name | Description | Value Range and Default |
|---|---|---|
| **OCSP Validation** | Verifying certificates via OCSP allows for the revocation of invalid certificates via the CA.<br><br>**Note**<br>All sub-policies are visible only when OCSP Validation is Enabled. | Enable, Disable<br><br>Default: Disable |
| **OCSP CA Certificates** | Certificate Authority certificates.<br><br>**Note**<br>This is a sub-policy of OCSP Validation. | 0-1024 characters<br><br>Default: N/A |
| **OCSP Expired Certificate Status Action** | Defines the action to take if the OCSP certificate status is expired.<br><br>**Note**<br>This is a sub-policy of OCSP Validation. | Time Delay, Erase, Remote Authentication, Denial of Login, Allow Access<br><br>Default: Denial of Login |
| **OCSP Grace** | A grace period in days that allows authentication to occur even if the OCSP server has not verified the certificate in this number of days.<br><br>**Note**<br>This is a sub-policy of OCSP Validation. | 0-365<br><br>Default: 7 |

| Policy Name | Description | Value Range and Default |
|---|---|---|
| **OCSP Responders** | Certificate Authority certificates.<br><br>**Note**<br>This is a sub-policy of OCSP Validation. | Yes, No<br><br>Default: Yes |
| **OCSP Responder Certificate** | Certificate Authority Certificate<br><br>**Note**<br>This is a sub-policy of OCSP Responders. | 0-1024 characters<br><br>Default: N/A |
| **OCSP Responder URL** | Certificate Authority certificates.<br><br>**Note**<br>This is a sub-policy of OCSP Responders. | 0-1024 characters<br><br>Default: N/A |
| **OCSP Revoked Certificate Status Action** | Defines the action to take if the OCSP certificate status is revoked.<br><br>**Note**<br>This is a sub-policy of OCSP Responders. | Time Delay, Erase, Remote Authentication, Denial of Login, Allow Access<br><br>Default: Denial of Login |
| **OCSP Show Success** | Whether success of OCSP reply should be displayed.<br><br>**Note**<br>This is a sub-policy of OCSP Responders. | Yes, No<br><br>Default: Yes |

| POLICY NAME | DESCRIPTION | VALUE RANGE AND DEFAULT |
|---|---|---|
| **OCSP Unknown Certificate Status Action** | Specify the action when an OCSP certificate status is unknown.<br><br>This is sub-policy of OCSP Responders. | Time Delay, Erase, Remote Authentication, Denial of Login, Allow Access<br><br>Default: Denial of Login |
| **Token Passthru** | Pass the token to the desktop GINA for further processing during the boot process.<br><br>This is sub-policy of OCSP Responders. | Yes, No<br><br>Default: No |

## Password Policies

The following table explains Full Disk Encryption password policies.

**Note**

Encryption Management for Apple FileVault and Encryption Management for Microsoft BitLocker do not require authentication and are not affected by authentication policies. Client, login, password, and authentication policies, or allowing the user to uninstall the Endpoint Encryption agent software only affects the Full Disk Encryption and File Encryption agents.

**TABLE 4-12. Full Disk Encryption Password Policy Descriptions**

| POLICY NAME | DESCRIPTION | VALUE RANGE AND DEFAULT |
|---|---|---|
| **Authentication Methods Allowed** | Specify the allowed type(s) of authentication methods that can be used. | Fixed, ColorCode, Pin, Remote<br><br>Default: Fixed |

# File Encryption Policies

This section explains the configurable options for policies affecting File Encryption agents.

Topics include:


- *Agent Policies on page 4-33*
- *Encryption Policies on page 4-33*
- *Login Policies on page 4-35*
- *Password Policies on page 4-36*


## Agent Policies

The following table explains the policies governing installation privileges on devices with File Encryption installed.

**TABLE 4-13. File Encryption Agent Policy Descriptions**

| POLICY NAME | DESCRIPTION | VALUE RANGE AND DEFAULT |
|---|---|---|
| **Allow User to Uninstall** | This policy specifies whether a user other than an Administrator can uninstall the endpoint application. | Yes, No<br>Default: Yes |

## Encryption Policies

The following table explains the policies governing how encryption is handled on File Encryption devices.

**TABLE 4-14. File Encryption Encryption Policy Descriptions**

| POLICY NAME | DESCRIPTION | VALUE RANGE AND DEFAULT |
|---|---|---|
| **Allow Secure Delete** | Specify whether to allow the user to delete files. | Yes, No<br>Default: Yes |
| **Disable Optical Drive** | Disable access to CD or DVD drives. | Yes, No<br>Default: No |
| **Encryption Key Used** | • User Key: choose a key unique to the user.<br>• Group Key: choose a key unique to the group, so all users in the group will also have access to files.<br>• Enterprise Key: choose a key unique to the enterprise, so all users in the enterprise will also have access to files. | User Key, Group Key, Enterprise Key<br>Default: Group Key |
| **Encryption Method Allowed** | Choose which allowable ways to encrypt files are allowed:<br>• User Key<br>• Group Key<br>• User-created password<br>• Digital Certificates | User's Unique Key, Group Unique Key, Encrypt With Static Password, Encrypt With Certificate<br>Default: All |
| **Removable Media** | Specify settings for USB devices. | Enable, Disable<br>Default: Disable |
| **Allowed USB Devices** | Specify permitted USB devices. | Any, KeyArmor<br>Default: Any |
| **Disable USB Drive** | Disable the USB drive when not logged in, always disable, and never disable drive. | Always, Logged Out, Never<br>Default: Logged Out |

| Policy Name | Description | Value Range and Default |
|---|---|---|
| **Folders to Encrypt on Removable Media** | The drive letter is given and the policy value corresponds to a valid removable media device. Non-existent folders are created. If no drive letter is given then all removable media devices attached to the device at login will use the policy values. | 1-255 characters<br>Default: N/A |
| **Fully Encrypt Device** | Specify whether all files/folders on removable media are encrypted. | Yes, No<br>Default: No |
| **Specify Folders to Encrypt** | List the folders that will be encrypted on the hard drive. Non-existent folders are created. A valid drive letter to the hard drive must also be supplied. A valid policy value is: C:\EncryptedFolder. | 1-255 characters<br>Default: `%DESKTOP%\Encrypted Files` |

## Login Policies

The following table explains the policies that govern logging on to the File Encryption agent.

**Table 4-15. File Encryption Login Policy Descriptions**

| Policy Name | Description | Value Range and Default |
|---|---|---|
| **Authentication Methods Allowed** | Specify the allowed type(s) of authentication that can be used. | Fixed, ColorCode, Pin, Smart Card<br>Default: Fixed |
| **Device Locked Action** | Action to be taken when the device is locked. | Time Delay, Remote Authentication<br>Default: Time Delay |

| Policy Name | Description | Value Range and Default |
|---|---|---|
| **Failed Login Attempts Allowed** | Number of failed logon attempts before using Lock Device Time Delay. 0 allows for unlimited attempts. | 0-100<br>Default: 5 |
| **Legal Notice Display Time**<br>**Note**<br>This is a sub-policy of the Legal Notice. | Specify when the configured legal notice is displayed to the user.<br>**Note**<br>The legal notice does not appear for File Encryption 3.1.3 or older agents. | Installation, Startup<br>Default: Startup |
| **Legal Notice Text**<br>**Note**<br>This is a sub-policy of the Legal Notice. | Specify the body of the legal notice.<br>**Note**<br>The legal notice does not appear for File Encryption 3.1.3 or older agents. | Insert File<br>Default: N/A |
| **Lock Device Time Delay** | Lock device for X minutes if user exceeds Failed Attempts Allowed. | 0-999,999<br>Default: 1 |

## Password Policies

The following table explains policies governing File Encryption passwords.

**TABLE 4-16. File Encryption Password Policy Descriptions**

| POLICY NAME | DESCRIPTION | VALUE RANGE AND DEFAULT |
|---|---|---|
| **Force Talking to Server** | Forces the File Encryption agent to communicate with to the server after X amount of days. 0 makes File Encryption agent standalone. | 0-999<br>Default: 360 |
| **Physical Token Required** | Require a physical token (smart cards) to log on to Endpoint Encryption devices. | Yes, No<br>Default: No |

# Common Policies

This section explains the configurable options for all enterprise policies affecting all Endpoint Encryption agents.

Topics include:


- *Agent Policy on page 4-37*
- *Authentication Policies on page 4-38*


## Agent Policy

The following table explains the sync interval policy.

**TABLE 4-17. Endpoint Encryption Common Agent Policy Descriptions**

| POLICY NAME | DESCRIPTION | VALUE RANGE AND DEFAULT |
|---|---|---|
| **Sync Interval** | Specify how often (in minutes) the application communicates to PolicyServer from the device to receive updated information. | 1-1440<br>Default: 30 |

## Authentication Policies

The following table explains policies that govern authenticating local and domain user accounts.

**Note**

Encryption Management for Apple FileVault and Encryption Management for Microsoft BitLocker do not require authentication and are not affected by authentication policies. Client, login, password, and authentication policies, or allowing the user to uninstall the Endpoint Encryption agent software only affects the Full Disk Encryption and File Encryption agents.

**TABLE 4-18. Endpoint Encryption Common Authentication Policy Descriptions**

| CATEGORY | POLICY NAME | DESCRIPTION | VALUE RANGE AND DEFAULT |
|---|---|---|---|
| **Local Login** | Admin Password | Specify policies regarding authenticating to the local device only. | N/A |
| **Local Login** > **Admin Password** | Allowed Character Types | Specify whether passwords can contain alpha, numeric, special or a combination. | Alpha, Numeric, Special<br>Default: All |
| **Local Login** > **Admin Password** | Can Contain User Name | Specify if the user name can be contained in the password. | Yes, No<br>Default: Yes |
| **Local Login** > **Admin Password** | Consecutive Characters Allowed | Specify the number of consecutive characters allowed in a password. | 0-255<br>Default: 3 |
| **Local Login** > **Admin Password** | Minimum Length | Specify the minimum length allowed for passwords. | 0-255<br>Default: 6 |
| **Local Login** > **Admin Password** | Password History Retention | Specify the number of past passwords the user is not allowed to use. | 0-255<br>Default: 0 |

| Category | Policy Name | Description | Value Range and Default |
|---|---|---|---|
| **Local Login** > **Admin Password** | Require How Many Characters | Specify the number of alpha characters that must be used in a password. | 0-255<br>Default: 0 |
| **Local Login** > **Admin Password** | Require How Many Lower Case Characters | Specify the number of lower case characters that must be used in a password. | 0-255<br>Default: 0 |
| **Local Login** > **Admin Password** | Require How Many Numbers | Specify the number of numeric characters that must be used in a password. | 0-255<br>Default: 0 |
| **Local Login** > **Admin Password** | Require How Many Special Characters | Specify the number of special characters that must be used in a password. | 0-255<br>Default: 0 |
| **Local Login** > **Admin Password** | Require How Many Upper Case Characters | Specify the number of upper case characters that must be used in a password. | 0-255<br>Default: 0 |
| **Local Login** | Self Help | Specify the policies that are used for Self Help. | N/A |
| **Local Login** > **Self Help** | Number of Questions | Specify the number of questions required to be answered correctly to authenticate the user. | 1-6<br>Default: 1 |
| **Local Login** > **Self Help** | Personal Challenge | Specify the personal challenge question(s) used for Self Help. | 1-1024<br>Default: N/A |
| **Local Login** | User Password | Specify the policies that are used for User Passwords. | N/A |
| **Local Login** > **User Password** | Allowed Character Types | Specify whether passwords can contain alpha, numeric, special or a combination. | Alpha, Numeric, Special<br>Default: All |

| Category | Policy Name | Description | Value Range and Default |
|---|---|---|---|
| **Local Login** > **User Password** | Can Contain User Name | Specify if the user name can be contained in the password. | Yes, No<br>Default: Yes |
| **Local Login** > **User Password** | Change Password Every | Specify (in days) when to force a user to change their password. | 1-1000000<br>Default: 60 |
| **Local Login** > **User Password** | Consecutive Characters Allowed | Specify the number of consecutive characters allowed in a password. | 0-255<br>Default: 3 |
| **Local Login** > **User Password** | Minimum Length | Specify the minimum length allowed for passwords. | 0-255<br>Default: 6 |
| **Local Login** > **User Password** | Password History Retention | Specify the number of past passwords the user is not allowed to use. | 0-255<br>Default: 0 |
| **Local Login** > **User Password** | Require How Many Characters | Specify the number of alpha characters that must be used in a password. | 0-255<br>Default: 0 |
| **Local Login** > **User Password** | Require How Many Lower Case Characters | Specify the number of lower case characters that must be used in a password. | 0-255<br>Default: 0 |
| **Local Login** > **User Password** | Require How Many Numbers | Specify the number of numeric characters that must be used in a password. | 0-255<br>Default: 0 |
| **Local Login** > **User Password** | Require How Many Special Characters | Specify the number of special characters that must be used in a password. | 0-255<br>Default: 0 |
| **Local Login** > **User Password** | Require How Many Upper Case Characters | Specify the number of upper case characters that must be used in a password. | 0-255<br>Default: 0 |

| Category | Policy Name | Description | Value Range and Default |
|---|---|---|---|
| **Local Login** > **User Password** | User Name Case Sensitive | Specify if the user name is case sensitive | Yes, No<br>Default: No |
| **Network Login** | Domain Authentication | Specify settings for Domain Authentication | Enable, Disable |
| **Network Login** > **Domain Authentication** | Active Directory Synchronization | Specify settings for Active Directory Synchronization | Enable, Disable |
| **Network Login** > **Domain Authentication** > **Active Directory Synchronization** | Distinguished Name | Optional: Specify the distinguished name of the authentication server. If no Distinguished Name is specified, this will default to the LDAP server Default Naming Convention. | 1-255<br>Default: N/A |
| **Network Login** > **Domain Authentication** > **Active Directory Synchronization** | User Name | Specify the user name that will be connected to Active Directory. | 1-255<br>Default: N/A |
| **Network Login** > **Domain Authentication** > **Active Directory Synchronization** | Password | Specify the password that will be connected to Active Directory. | 1-255<br>Default: N/A |
| **Network Login** > **Domain Authentication** | Domain Name | NetBIOS name of the domain for Single Sign On. Default is NetBIOS value used by the PolicyServer. | 1-255<br>Default: N/A |
| **Network Login** > **Domain Authentication** | Host Name | Specify the host name. The host name can be a domain name. | 1-255<br>Default: N/A |

| CATEGORY | POLICY NAME | DESCRIPTION | VALUE RANGE AND DEFAULT |
|---|---|---|---|
| **Network Login** > **Domain Authentication** | Port Number | Optional: 0 = use default. Specifies the port to be used for the connection. If no port number is specified, the LDAP provider uses the default port number. | 0-65535<br>Default: 0 |
| **Network Login** | Server Type | Type of server used to authenticate client user requests. | LDAP, LDAProxy<br>Default: LDAP |
| **Network Login** > **Authentication** | Remember User Between Login | Remember last used user name and display it in the authentication screen. | Yes, No<br>Default: Yes |

# Chapter 5

# Groups in PolicyServer MMC

Endpoint Encryption utilizes both role-based and identity-based authentication to secure data. Correctly configuring Endpoint Encryption groups ensures that data remains encrypted from unauthorized users, thus preventing data loss risk from accidental information release or deliberate sabotage.

Topics include:


- *Group Management on page 5-2*
- *Offline Groups on page 5-12*

# Group Management

This section explains how to use PolicyServer MMC to add new groups, add or remove Endpoint Encryption users and devices, and modify groups.

Topics include:


- *Adding a Top Group on page 3-7*
- *Adding a Subgroup on page 5-4*
- *Modifying a Group on page 5-5*
- *Removing a Group on page 5-5*
- *Adding a New User to a Group on page 3-8*
- *Adding an Existing User to a Group on page 3-13*
- *Removing Users From a Group on page 5-9*
- *Removing All Users From a Group on page 5-10*
- *Adding a Device to a Group on page 5-11*
- *Removing a Device from a Group on page 5-12*


## Adding a Top Group

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

**Note**

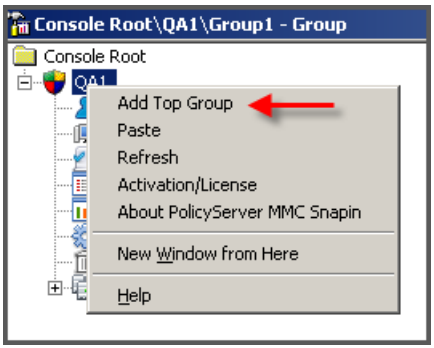
Enterprise administrators and authenticators may not be added to groups because their permissions supercede all groups. If you add an administrator or authenticator to a group, that account will be a group administrator or authenticator.

For more information, see *Modifying a User on page 6-9*.

**Procedure**

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

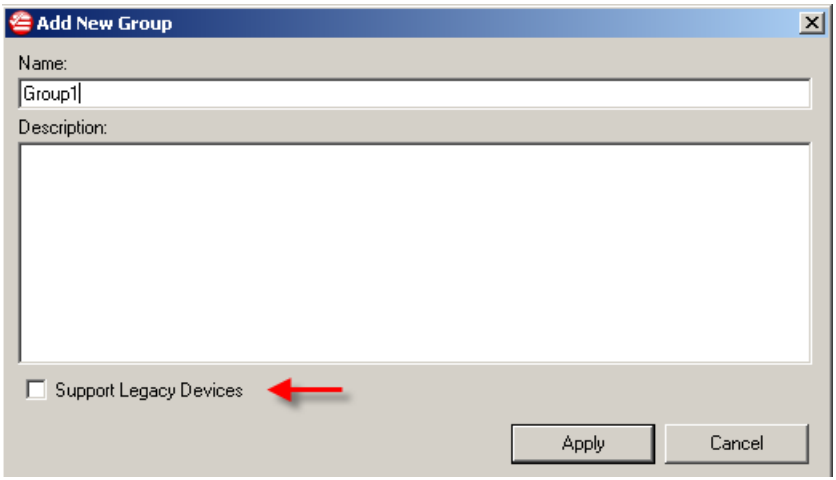
   The **Add New Group** screen appears.




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

**Note**

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




4. Click **Apply**.

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

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

## Adding a Subgroup

Although subgroups inherit all existing policies of the parent group, you must separately add users and devices to the subgroup.

**Procedure**

1. Right-click a group in the left pane tree structure, and then click **Add**.

   The **Add New Group** window appears.

2. Follow the steps in *Adding a Top Group on page 3-7*.

   The new group is added to the tree structure inside the Top Group.

## Modifying a Group

**Procedure**

1. Right-click a group in the left pane tree structure, then click **Modify**.

   The **Modify Group** screen appears.

2. Specify changes.

3. Click **Apply**.

## Removing a Group

Use the tree structure to remove a group. Removing a Top Group removes all subgroups.

**Procedure**

1. Right-click a group in the left pane tree structure, then click **Remove**.

   A warning message appears.

2. Click **Yes** to remove the group.

   The selected group no longer appears in the tree structure.

## Adding a New User to a Group

**Note**

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

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

**Procedure**

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

   The **Add New User** screen appears.

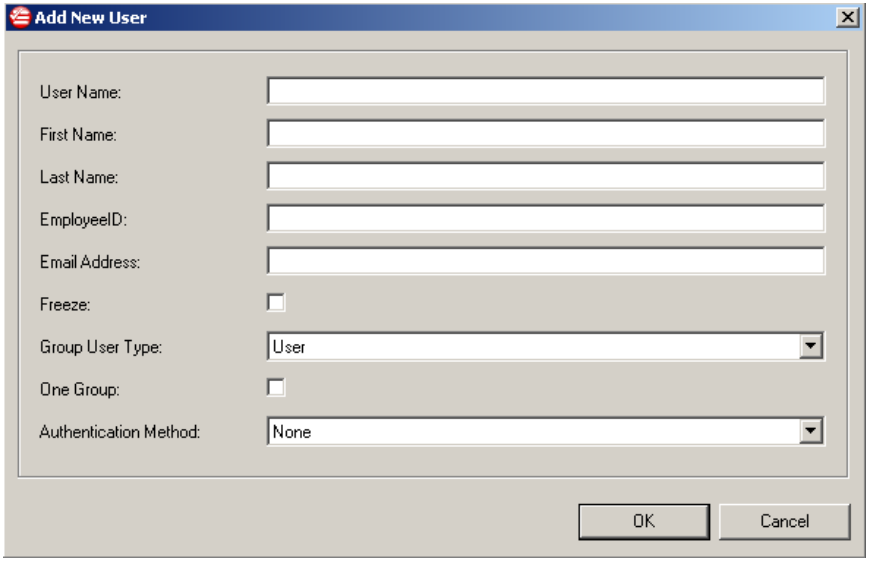



**FIGURE 5-1. Add New User Screen**

3. Specify the following options:

| OPTION | DESCRIPTION |
|---|---|
| User Nme | Specify the user name for the new user account (required). |
| First Name | Specify the first name for the new user account (required). |
| Last Name | Specify the last name for the new user account (required). |
| EmployeeID | Specify the employee ID for the new user account (optional). |

| OPTION | DESCRIPTION |
|---|---|
| Freeze | Select whether to temporarily disable the new user account (optional). While frozen, the user is unable to log on devices. |
| Group User Type | Select the privileges of the new account.<br><br>**Note**<br>For information about account roles, see *Users on page 4-3*.<br><br>Options include:<br>• User<br>• Authenticator<br>• Administrator<br><br>**Note**<br>Giving a user in a group administrator or authenticator privileges only applies those privileges within that group. That user is treated as a group administrator or group authenticator. Add an administrator or authenticator in the Enterprise, outside of the group, to give that user Enterprise-level privileges. |
| One Group | Select whether the new user account is allowed to be a member of multiple group policies. |
| Authentication method | Select the method that the new user account uses to log on to Endpoint Encryption devices. Options include:<br><br>**Note**<br>The default authentication method for users is **None**.<br><br>For information about account roles, see *Users on page 4-3*. |

4. Click **OK**.

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

## Adding an Existing User to a Group

A user can be a member of multiple groups.

**Procedure**

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

   The **Add Users To Group** screen appears.

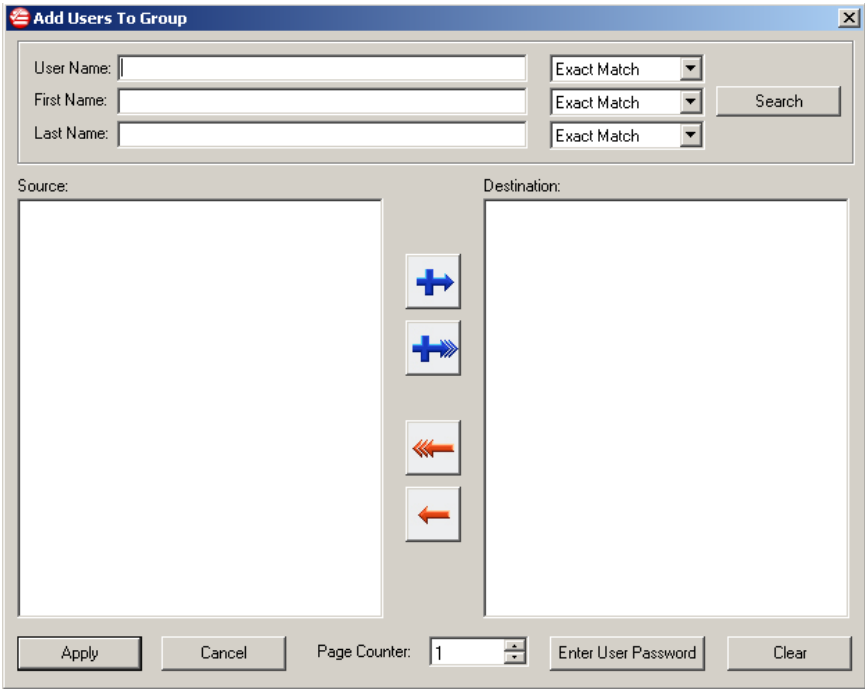



**FIGURE 5-2. Add Users To Group Screen**

3. Specify user details and then click **Search**.

The **Source** field populates with any accounts that match the search criteria.

4. Select users from the **Source** list and click the blue arrow to add them.

   For information about search icons, see *Add/Remove Search Result Icons on page 6-14*.

   The selected user moves to the **Destination** list.

5. To change a user password:

   a. In the **Destination** list, highlight the user.

   b. Click **Enter User Password** located at the bottom of the window.

   c. In the window that appears, specify the user's authentication method.

   d. Click **Apply** to close the **Change Password** window.

6. Click **Apply** to save changes.

   The user is added to the group. If this is the only group assignment, then the user is now able to log on to Endpoint Encryption devices.

## Removing Users From a Group

**WARNING!**

Before removing a Group Administrator or Group Authenticator account, reassign this role to another user account. Otherwise, only the Enterprise Administrator or Enterprise Authenticator accounts can make changes to the group.

Removing a user from a group restricts the user from accessing any Endpoint Encryption device assigned to that group. Before removing Endpoint Encryption users, make sure that the users have backed up and unencrypted their data.

**Procedure**

1. Expand the group, then click **Users**.
2. In the right pane, right-click the user and select **Remove User**.

   A warning message appears.

3. To remove the user from the Enterprise as well, select **Remove from Enterprise**.

**Note**

Removing a user from the Enterprise also removes that user from all groups and subgroups.

4. Click **Yes**.

   The user is removed.

## Removing All Users From a Group

**WARNING!**

Before removing a Group Administrator or Group Authenticator account, reassign this role to another user. Otherwise, only Enterprise Administrator and Enterprise Authenticator accounts can make group-level changes.

**Procedure**

1. Expand the group, then click **Users**.
2. In the right pane, right-click the user and select **Remove All Users**.

   A warning message displays.
3. To remove all users from the Enterprise as well, select **Remove from Enterprise**.

**Note**

Removing a user from the Enterprise also removes that user from all groups and subgroups.

4. Click **Yes.**

# Adding a Device to a Group

**Note**

Each Endpoint Encryption device can belong to only one group.

**Procedure**

1. In the left pane, expand the desired policy group and click **Devices**.
2. In the right pane, right-click the whitespace and select **Add Device**.

   The **Add Devices to Group** screen appears.

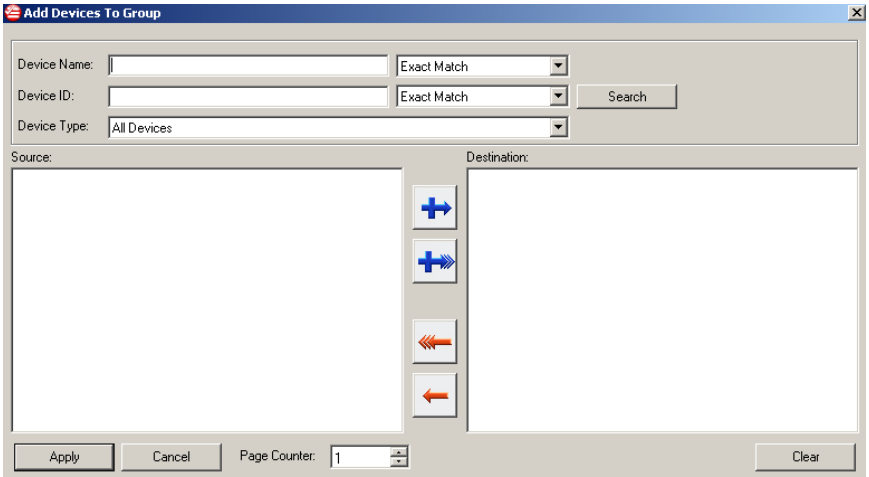



**FIGURE 5-3. Add Devices to Group Screen**

3. Type the device details, then click **Search**.

   If there is a match, the **Source** field populates with Endpoint Encryption devices.

4. Select applicable Endpoint Encryption devices from the **Source** field, then click the **blue arrow** to add them.

   For information about search icons, see *Add/Remove Search Result Icons on page 6-14*.

5. Click **Apply** to add the Endpoint Encryption device to the selected group.

   The Endpoint Encryption device is added to the group.

## Removing a Device from a Group

Removing a device from a group removes the device from the selected group only.

**WARNING!**

To remove a device from all groups, remove it from the Enterprise. Before deleting a device from the Enterprise, verify that the device has been unencrypted and that all Endpoint Encryption agents were uninstalled. Failure to do so may result in irreversible data loss.

**Procedure**

1. Expand the group, then open **Devices**.
2. In the right pane, right-click the device and select **Remove Device**.

   A warning message appears.
3. Click **Yes**.

   The device is removed.

# Offline Groups

An offline group is a group of endpoints that did not connect to PolicyServer when the File Encryption agent was installed. Export the policies, users, and devices for that group to a file and install them on each endpoint. When the group requires changes, export a new file and repeat the import.

Policies are automatically updated when the agent connects to PolicyServer.

Topics include:

- *Creating an Offline Group on page 5-13*
- *Updating an Offline Group on page 5-15*


## Creating an Offline Group

Offline groups allow agents that do not need to or cannot communicate with PolicyServer to get updated policies. The Endpoint Encryption agent installation files must be available to the server where PolicyServer is installed.

**Note**

Exported groups must contain at least one user. The group name must also be alphanumeric only.

**Procedure**

1. From the left pane, right-click the group and then select **Export**.

   The **PolicyServer Export Group Wizard** appears.

**FIGURE 5-4. PolicyServer Exporting Group Wizard**

2. Select **Create off-line devices**.
3. Specify the export location.
4. Specify and confirm the export password.

> **Note**
>
> The export password is used to authenticate the executable on the agent.

5. Click **Next**
6. Click **Add** to browse to and upload Endpoint Encryption client installers.

**TABLE 5-1. Endpoint Encryption Installation Filename**

| INSTALLATION FILE | PURPOSE |
|---|---|
| `FileEncryptionIns.exe` | Installs the File Encryption agent. |

**Note**

For older Endpoint Encryption product versions, see the supporting documentation.

7. Click **Next**.
8. Depending on the license type, specify the number of devices to be installed on. The number of licenses available is reduced with every device.
9. Optionally specify a **Device Name Prefix**. PolicyServer uses the device prefix number to generate a unique Device ID and device encryption key for each device in this group.
10. Click **Next**.

    The offline group build begins.
11. Click **Done** to generate the export file at the specified location.

    A generated executable file named "Export" is created on the desktop. Use this to distribute policy changes to offline groups.

## Updating an Offline Group

The following procedure explains how to create an update for an offline group.

**Procedure**

1. From the left pane, right-click the group, then select **Export**.

   The **PolicyServer Export Group Wizard** opens.
2. Select **Update off-line devices**.

3. Specify the export password.

**Note**

Use the export password to authenticate the executable on the Endpoint Encryption agent.

4. Click **Browse** to specify a location to store the export file.
5. Click **Next**

   The offline group build begins.
6. Click **Done**.

   The export file is generated at the specified location.
7. Install the software on the device using the generated executable or script.

**Note**

See the *Endpoint Encryption Installation and Migration Guide*.

# Chapter 6

# Users in PolicyServer MMC

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

**Note**

For a description of Endpoint Encryption user roles, see *Users on page 4-3*.

This chapter explains account roles and authentication methods, how to administer PolicyServer MMC to manage policies affecting Endpoint Encryption users, and how to control information access by using the **Users** policy node in PolicyServer MMC. This chapter also explains how to restore deleted Endpoint Encryption users.

Topics include:


- *Adding Users to Endpoint Encryption on page 6-2*
- *Managing Users in Endpoint Encryption on page 6-7*
- *Working with Passwords on page 6-18*

# Adding Users to Endpoint Encryption

Endpoint Encryption has several options to add users to Endpoint Encryption:

- Add users manually, one at a time
- Bulk import numerous users with a CSV file
- Use the External Directory Browser with Active Directory

Topics include:


- *Adding a New Enterprise User on page 3-11*
- *Importing Users from a CSV File on page 6-4*
- *Importing Active Directory Users on page 6-5*


## Adding a New Enterprise User

The following procedure explains how to add new Endpoint Encryption users to the Enterprise.

**Note**

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

Adding a new Endpoint Encryption user to a group adds the user to the group and to the Enterprise.

**Procedure**

1. To access Enterprise Users, do one of the following:
   - Expand the Enterprise, then open **Enterprise Users**.
   - Expand the Enterprise, expand the group, then open **Users**.
2. Right-click the white space in the right pane and select **Add User**.

The **Add New User** screen displays.

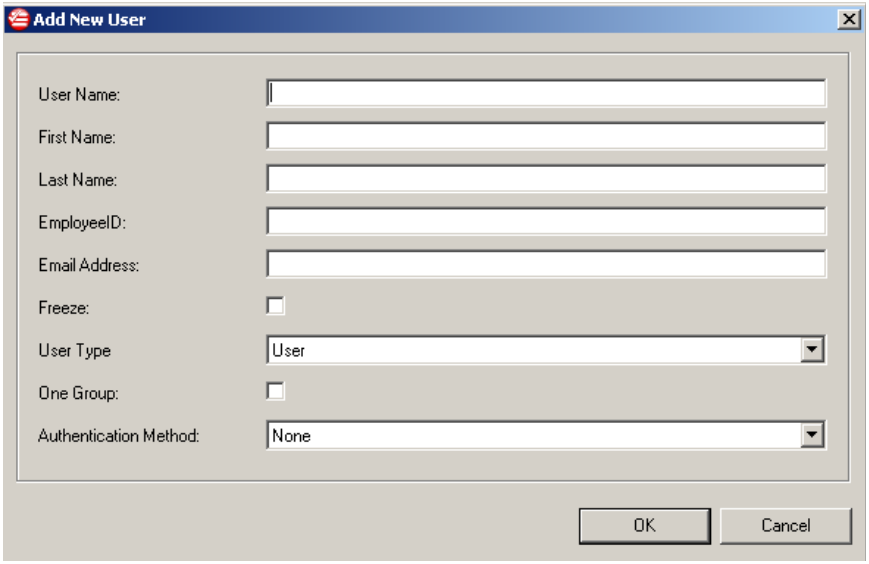



**FIGURE 6-1. Add New User screen**

3. Specify the following options:

| OPTION | DESCRIPTION |
|---|---|
| User name | Specify the user name for the new user account (required). |
| First name | Specify the first name for the new user account (required). |
| Last name | Specify the last name for the new user account (required). |
| EmployeeID | Specify the employee ID for the new user account (optional). |
| Freeze | Select whether to temporarily disable the new user account (optional). While frozen, the user is unable to log on to devices. |
| Group User Type | Select the privileges of the new account. For information about account roles, see *Authentication Overview on page 4-2*.<br><br>Options include: |

| OPTION | DESCRIPTION |
|---|---|
| | • **User**<br>• **Authenticator**<br>• **Administrator**<br><br>**Note**<br>It is not possible to add Enterprise Administrator or Authenticator accounts to groups. |
| One Group | Select whether the new user account is allowed to be a member of multiple group policies. |
| Authentication method | Select the method that the new user account uses to log on to Endpoint Encryption devices. For information about authentication methods, see *Authentication Overview on page 4-2*.<br><br>**Note**<br>The default authentication method for users is **None**. |

4. Click **OK**.

   The new Endpoint Encryption user is added the Enterprise. The user cannot log on to Endpoint Encryption devices until the user account is added to a group.

## Importing Users from a CSV File

Use a Comma Separated Values (CSV) file to simultaneously import multiple users.

Format: user name (required), first name, last name, employee ID, email address

**Note**

- Importing users from a CSV file is supported only for users using fixed password authentication.
- Include a comma for fields with no data.
- Create one CSV file for each group of users to import. All users in the CSV file are added to the same group.

**Procedure**

1. Expand the group in the left pane, then click **Users**.
2. Right-click whitespace in the right pane, then select **Bulk Import Add Users**.

   The open file window appears.
3. Go to the CSV file and click **Open**.
4. At the confirmation, click **OK**.

   The users in the CSV file are added to the group and the Enterprise.

## Importing Active Directory Users

PolicyServer maintains a user directory separate from the Active Directory database. This allows PolicyServer absolute security over access to all Endpoint Encryption devices, user rights, and authentication methods.

For information about configuring Active Directory integration, see the *Endpoint Encryption Installation and Migration Guide*.

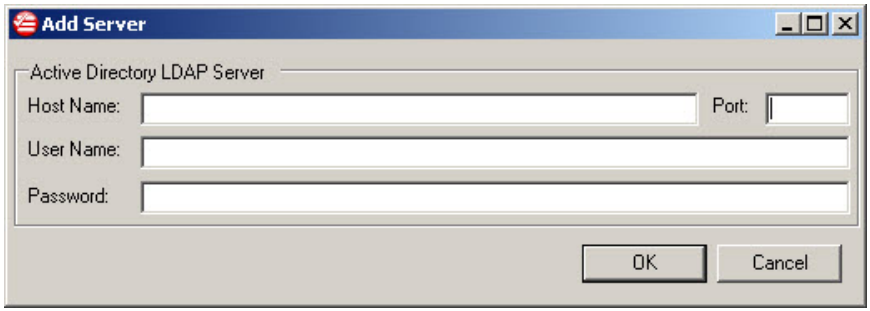
**Procedure**

1. Log on to PolicyServer MMC.
2. Open **Enterprise Users**, right-click the right pane (whitespace) and then select **External Directory Browser**.

   The **Active Directory User Import** screen appears.

3. Go to **Edit** > **Connect to Domain**.

   The **Add Server** screen appears.




4. Specify the following parameters for the Active Directory LDAP Server:
   - **Host name**
   - **Port**
   - **User name**
   - **Password**
5. Click **OK**.
6. Wait for the specified Active Directory domain to populate.

   The Active Directory tree for the specified domain appears in the left pane.
7. From the left pane, use the navigation tree to select the container from which to add users.

   The available users populate in the right pane.
8. Select applicable users, right-click the selection and then select:
   - **Add to Enterprise**
   - **Add to Group**
     a. Expand the Enterprise.

b. Select the appropriate group.

c. Click **OK**.

9. Click **OK** to add the users to the specified location.

   A confirmation window appears.

10. Click **OK** to confirm.

    An import status message displays.

11. Click **OK** to finish, or repeat the procedure to select more users to import

---

# Managing Users in Endpoint Encryption

Manage users in Endpoint Encryption from the **Enterprise Users** screen.

Topics include:


- *Finding a User on page 6-8*
- *Modifying a User on page 6-9*
- *Viewing a User's Group Membership on page 6-9*
- *Adding a New User to a Group on page 3-8*
- *Adding an Existing User to a Group on page 3-13*
- *Changing a User's Default Group on page 6-14*
- *Allowing User to Install to a Group on page 6-15*
- *Removing Users From a Group on page 5-9*
- *Removing All Users From a Group on page 5-10*
- *Restoring a Deleted User on page 6-17*

## Finding a User

It is faster to search for users at the group level; however, this is at the cost of searching the entire Enterprise.

---

**Procedure**

1. From the left pane, click **Enterprise Users** or expand the group and then click **Users**.

2. At the upper corner of the right pane, click **Search**.

   The **User Search Filter** window appears.

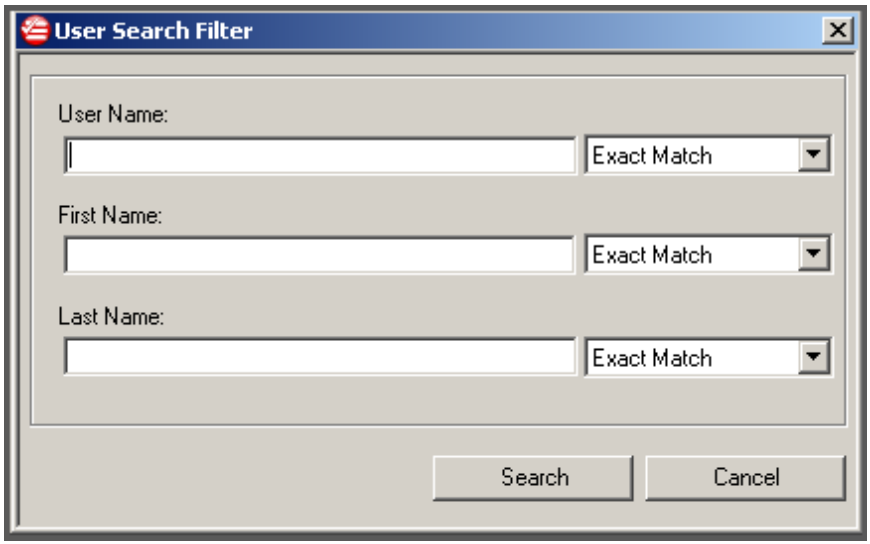



**FIGURE 6-2. User Search Filter window**

3. Specify search details and then click **Search**.

   All accounts matching the search criteria appear.

**Note**

If there are many users, use **Page Counter** to go from one page to another or click **Clear** to remove all results.

## Modifying a User

Any Group Administrator can change a user's profile information.

**Note**

- Enterprise-level changes are applied to the user universally, but group-level changes apply only to that group.

**Procedure**

1. Open **Enterprise Users**.
2. In the right pane, right-click the user and then select **Modify User**.

   The **Modify User** screen appears.
3. Make the necessary changes. If the authentication method changes to **Fixed Password**, provide the default user password.
4. Click **OK**.
5. At the confirmation message, click **OK**.

## Viewing a User's Group Membership

List groups to view the Endpoint Encryption user's group membership. If a user belongs to multiple groups, you can also change the priority of assigned groups. For information about the default group, see *Changing a User's Default Group on page 6-14*.

**Procedure**

1. Open **Enterprise Users**.
2. Right-click the user, then select **List Groups**.

   The **Group Membership** list appears.

## Adding a New User to a Group

**Note**

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

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

**Procedure**

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

The **Add New User** screen appears.

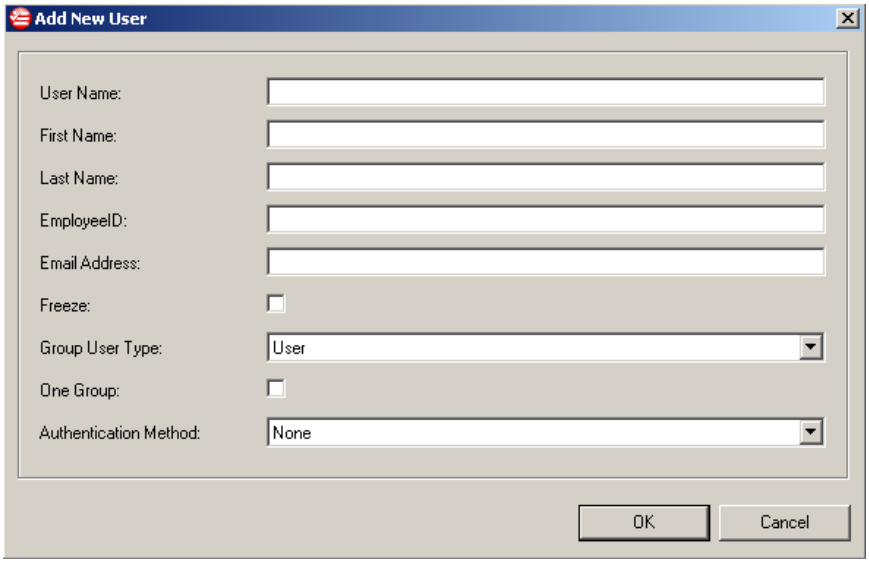



**FIGURE 6-3. Add New User Screen**

3. Specify the following options:

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

| OPTION | DESCRIPTION |
|---|---|
| | **Note**<br>For information about account roles, see *Users on page 4-3*.<br><br>Options include:<br>• User<br>• Authenticator<br>• Administrator<br><br>**Note**<br>Giving a user in a group administrator or authenticator privileges only applies those privileges within that group. That user is treated as a group administrator or group authenticator. Add an administrator or authenticator in the Enterprise, outside of the group, to give that user Enterprise-level privileges. |
| One Group | Select whether the new user account is allowed to be a member of multiple group policies. |
| Authentication method | Select the method that the new user account uses to log on to Endpoint Encryption devices. Options include:<br><br>**Note**<br>The default authentication method for users is **None**.<br>For information about account roles, see *Users on page 4-3*. |

4. Click **OK**.

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

## Adding an Existing User to a Group

A user can be a member of multiple groups.

**Procedure**

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

   The **Add Users To Group** screen appears.

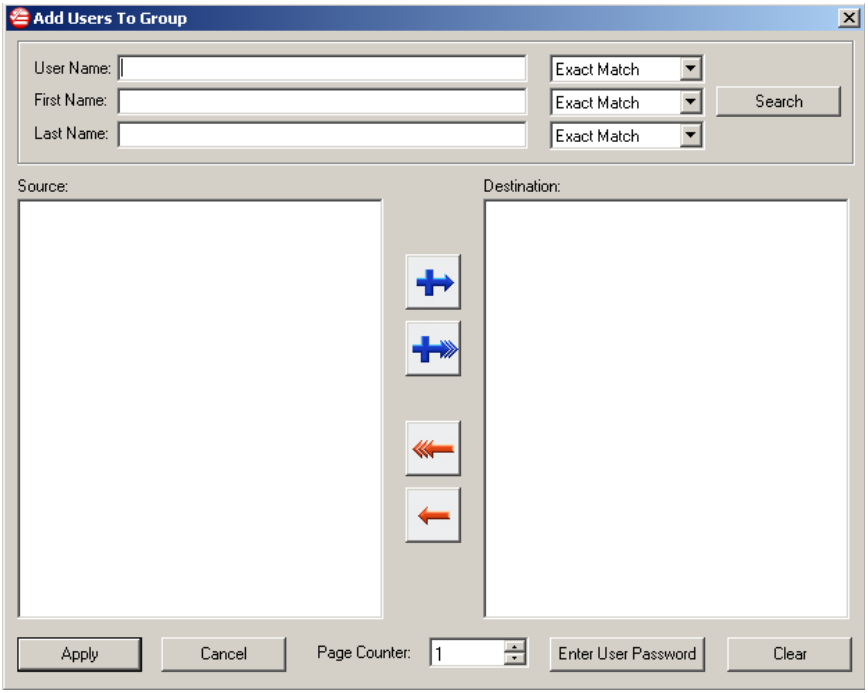



**FIGURE 6-4. Add Users To Group Screen**

3. Specify user details and then click **Search**.

   The **Source** field populates with any accounts that match the search criteria.
4. Select users from the **Source** list and click the blue arrow to add them.

   For information about search icons, see *Add/Remove Search Result Icons on page 6-14*.

The selected user moves to the **Destination** list.

5. To change a user password:

   a. In the **Destination** list, highlight the user.

   b. Click **Enter User Password** located at the bottom of the window.

   c. In the window that appears, specify the user's authentication method.

   d. Click **Apply** to close the **Change Password** window.

6. Click **Apply** to save changes.

   The user is added to the group. If this is the only group assignment, then the user is now able to log on to Endpoint Encryption devices.

## Add/Remove Search Result Icons

| CENTER ICONS | DESCRIPTION |
|---|---|
| | Add a single selected item to **Destination** field. |
| | Add all found items based on search criteria to **Destination** field. |
| | Remove a single selected item from **Destination** field. |
| | Remove all items from **Destination** field. |

## Changing a User's Default Group

Endpoint Encryption users can belong to any number of groups while Endpoint Encryption devices can only belong to one group. The default group is the group that

controls the user's policies. The first group listed in the group membership is the default group for the user.

**Note**

The user must be allowed to install to the default group. For more information, see *Allowing User to Install to a Group on page 6-15*.

**Procedure**

1. Open **Enterprise Users**.
2. Right-click the user and then select **List Groups**.

   The **Group Membership** list appears.
3. Right-click the user and then select **Move to top**.

   The user's default group is changed.

## Allowing User to Install to a Group

Allowing a user to install to a group allows users to install Endpoint Encryption devices to a group that they are a member, without requiring the additional privileges of the Administrator or Authenticator role.

**Note**

The default setting is **Disallow User To Install To This Group**.

**Procedure**

1. Open **Enterprise Users**.
2. Right-click the user and then select **List Groups**.

   The **Group Membership** list appears.

3. Right-click the user and then select **Allow User To Install To This Group**.

   The user can now install devices to this group.

## Removing Users From a Group

**WARNING!**

Before removing a Group Administrator or Group Authenticator account, reassign this role to another user account. Otherwise, only the Enterprise Administrator or Enterprise Authenticator accounts can make changes to the group.

Removing a user from a group restricts the user from accessing any Endpoint Encryption device assigned to that group. Before removing Endpoint Encryption users, make sure that the users have backed up and unencrypted their data.

**Procedure**

1. Expand the group, then click **Users**.
2. In the right pane, right-click the user and select **Remove User**.

   A warning message appears.
3. To remove the user from the Enterprise as well, select **Remove from Enterprise**.

   **Note**

   Removing a user from the Enterprise also removes that user from all groups and subgroups.
4. Click **Yes**.

   The user is removed.

## Removing All Users From a Group

**WARNING!**

Before removing a Group Administrator or Group Authenticator account, reassign this role to another user. Otherwise, only Enterprise Administrator and Enterprise Authenticator accounts can make group-level changes.

**Procedure**

1. Expand the group, then click **Users**.
2. In the right pane, right-click the user and select **Remove All Users**.

   A warning message displays.
3. To remove all users from the Enterprise as well, select **Remove from Enterprise**.

   **Note**

   Removing a user from the Enterprise also removes that user from all groups and subgroups.
4. Click **Yes.**

## Restoring a Deleted User

For both Control Manager and PolicyServer MMC environments, use the PolicyServer MMC Recycle Bin node to restore a deleted Endpoint Encryption user.

**Procedure**

1. Log on to PolicyServer MMC.
2. Expand the **Recycle Bin**.
3. Open **Deleted Users**.

   The right pane loads all deleted users.

4. Right-click the user account, then select **Restore User**.

   The user is added back to the Enterprise, but does not belong to any policy groups.

# Working with Passwords

When a user forgets the password or misplaces an endpoint, the user can reset the password using methods defined by policies. The following password reset methods are available:

- Microsoft Windows Active Directory
- Control Manager
- PolicyServer MMC
- Remote Help
- Self Help

All of these options involve setting the policy at the Enterprise or at the group/policy level, if necessary. Use the Support Information policy to provide support-related information to users about password resets.

Topics include:


- *Resetting an Enterprise Administrator/Authenticator Password on page 6-19*
- *Resetting a Group Administrator/Authenticator Password on page 6-20*
- *Resetting User Passwords on page 6-20*
- *Smart Card on page 2-16*
- *Using Self Help Password Reset on page 6-25*
- *Remote Help Assistance on page 6-27*
- *Managing Password Setting Objects from Active Directory on page 6-31*

## Resetting an Enterprise Administrator/Authenticator Password

Only Enterprise Administrator accounts can reset an Enterprise Administrator password. An Authenticator within the same group permissions or higher, can reset an Administrator or Authenticator password within that group.

**Tip**

As a safeguard against password loss, Trend Micro recommends having at least three Enterprise Administrator accounts at all times. If an Enterprise Administrator account password is lost, use Self Help authentication to reset the password.

**Procedure**

1. Log on to PolicyServer MMC using an Enterprise Administrator account.
2. Open **Enterprise Users**.
3. Right-click the Enterprise Administrator or Authenticator account with the lost password, then select **Change Password**.

   The **Change Password** window appears.
4. Select an authentication method.
5. Specify the password (if requested).
6. Click **Apply**.

   The account password is reset.

**Note**

The **User must change password at next logon** option is only available after the agent updates policies.

## Resetting a Group Administrator/Authenticator Password

Changes to passwords only affect the selected group. To reduce the number of passwords, assign Group Administrator accounts to only one Top Group.

**Procedure**

1. Log on to PolicyServer MMC using a Group Administrator account.
2. Expand the group, then click **Users**.
3. Right-click the Group Administrator or Group Authenticator account with the lost password, then select **Change Password**.

   The **Change Password** window appears.
4. Select an authentication method.
5. Specify and confirm the password (if requested).
6. Click **Apply**.

   The account password is reset.

**Note**

The **User must change password at next logon** option is only available after the client updates.

## Resetting User Passwords

When resetting a user's password, select the **User must change password at next logon** check box to require a user to change the password at next logon. The user will be required to change the password after logging on any Endpoint Encryption device.

**Tip**

Trend Micro recommends using domain authentication.

Topics include:


- *Resetting to a Fixed Password on page 6-21*
- *Resetting a User Password with Active Directory on page 6-21*


## Resetting to a Fixed Password

**Procedure**

1. Open **Enterprise Users** or expand the group, then click **Users**.
2. Select the user accounts from the right pane.

   **Note**

   Hold SHIFT to select multiple users. Multiple selection is only available at the group level.

3. Right-click and select **Change Password**.

   The **Change Password** window appears.

4. For the **Authentication Method**, select **Fixed Password**.
5. Specify and confirm the password.
6. Click **Apply**.

   The user must change his/her password after successfully logging on Endpoint Encryption devices.

## Resetting a User Password with Active Directory

Trend Micro recommends using Active Directory to reset the user password, especially if the user has access to the company Help Desk, has network connectivity, or if Windows Single Sign-on (SSO) is enabled.

Refer to the appropriate operating system user guide for more information about resetting a domain user password using Active Directory.

## Smart Card

Smart card authentication requires both a PIN and a physical token to confirm the user identity. Smart card certificates are associated with the user account and the user's assigned group. Once registered, the user can use smart card authentication from any Endpoint Encryption device in that group. Users are free to use any Endpoint Encryption device in their group and do not need to ask for another one-time password.

To use smart card authentication, make sure that the following requirements are met:

- The smart card reader is connected to the endpoint and the smart card is inserted into the smart card reader.
- ActivClient 6.2 with all service packs and updates installed.

**Note**

ActivClient 7.0 and later is not supported.

- Specify the smart card PIN in the password field.

**WARNING!**

Failure to provide a correct password sends a password error and may result in locking the smart card.

**Note**

- Smart card authentication is only configurable with PolicyServer MMC.
- Switching the authentication method from smart card to domain authentication may cause issues for domain users added through ADSync or Active Directory User Import. To resolve this issue, remove the domain user account from the enterprise, and then restart the PolicyServer services to start synchronization with the AD server. The synchronization process adds the user back with domain authentication as the authentication method. Alternatively, you can also add the domain user account back via Active Directory User Import.

## Smart Card Registration

Smart card certificates are associated with the user account and the user's assigned group. Once registered, the user can use smart card authentication from any Endpoint Encryption device in that group. Users are free to use any Endpoint Encryption device in their group and do not need to ask for another one-time password.

## Configuring Smart Card Authentication in PolicyServer MMC

Registering a smart card allows a user to log on with smart card authentication. For information about Full Disk Encryption Preboot smart card authentication, see *Smart Card on page 2-16*.

**Procedure**

1. Log on to PolicyServer MMC.
2. Go to **Full Disk Encryption** > **Login**.
3. Right-click **Token Authentication** and select **Enable**.
4. Go to **Full Disk Encryption** > **Password**.
5. Right-click **Authentication Methods Allowed**, then select **Properties**.

   The **Edit Policy Value** window appears.
6. Select **PIN**, then click **OK** to confirm the policy change.

Smart card authentication is enabled.

## Registering a Smart Card in PolicyServer MMC

Before proceeding, make sure to configure smart card authentication. For information about configuring smart card authentication, see *Configuring Smart Card Authentication in PolicyServer MMC on page 6-23*.

Smart card certificates are associated with the user account and the user's assigned group. Once registered, the user can use smart card authentication from any Endpoint Encryption device in that group. Users are free to use any Endpoint Encryption device in their group and do not need to ask for another one-time password.

After assigning a smart card PIN to the user, the user can log on the Full Disk Encryption agent directly with the smart card from the smart card authentication screen in the Full Disk Encryption preboot.

---

**Procedure**

1. Log on to PolicyServer MMC.
2. Insert the smart card in the reader.
3. Connect the reader to the PolicyServer endpoint.
4. Expand the specific group and then click **Users**.
5. Right-click a user and then select **Change Password**.

   The **Change Password** window appears.
6. In the **Authentication Method** drop-down, select **Smart Card**.
7. Specify and confirm the **PIN**.
8. In the **Select a slot** drop-down, select the smart card type.
9. Click **Apply** to confirm token authentication.
10. Click **OK** to confirm the user account changes.

---

The smart card is registered to all users in the same group as the selected user.

### Registering a Smart Card in Full Disk Encryption Preboot

**Procedure**

1. Follow the instructions to change passwords, then select **Smart Card**.

   See the *Administrator's Guide for PolicyServer MMC*.

2. Insert the smart card in the reader.
3. Connect the reader to the endpoint.
4. Specify the user name and fixed password.
5. Click **Continue**.
6. At the confirmation message, click **Continue**.
7. At the **Register Token** window, do the following:
   a. Type the new PIN provided by the Group or Enterprise Administrator.
   b. Confirm the new PIN.
   c. Select the smart card type from the **Token** drop-down list.
   d. Click **Continue** to finish registering the smart card token.

## Using Self Help Password Reset

Users who have forgotten their passwords can use Self Help to authenticate without Help Desk assistance. Use the Number of Questions and the Personal Challenge policies to set the number of personal challenge questions and the questions that the user must answer, respectively. Self Help questions are answered during the initial user authentication and when users change their passwords.

For information about using Self Help, see *Self Help on page 2-16*.

**Note**

Self Help requires that the Endpoint Encryption agent has network connectivity to PolicyServer.

**Procedure**

1. Expand **Enterprise Policies** or expand the group and then expand **Policies**.
2. Go to **Common** > **Authentication** > **Local Login** > **Self Help**.

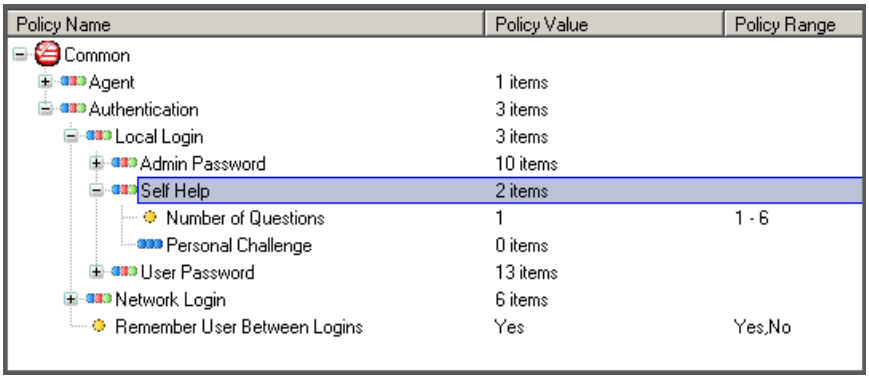



**FIGURE 6-5. Self Help Policy**

3. Open **Number of Questions** to set the required number of questions that users must answer.

**WARNING!**

Do not set **Number of Questions** greater than six. Otherwise, users are unable to authenticate using Self Help.

4. Right-click **Personal Challenge** and select **Add** to set a question that the user must answer. Repeat until all personal challenge questions are defined.

   The user will be prompted to set the personal challenge question answers the next time that the user logs on any Endpoint Encryption device.

## Remote Help Assistance

Remote Help allows users to reset a forgotten password or locked account. Any Endpoint Encryption user who has a locked account or forgot the account password must reset the password before being able to log on to any Endpoint Encryption device. Remote Help requires that the user contact the Help Desk for a Challenge Response. Remote Help does not require network connectivity to PolicyServer.

---

**Procedure**

1. Log on to PolicyServer MMC using any account with Group Administrator permissions in the same policy group as the user.
2. Ask the user to go to **Help** > **Remote Help** from the Endpoint Encryption agent.
3. Ask the user for the **Device ID**.

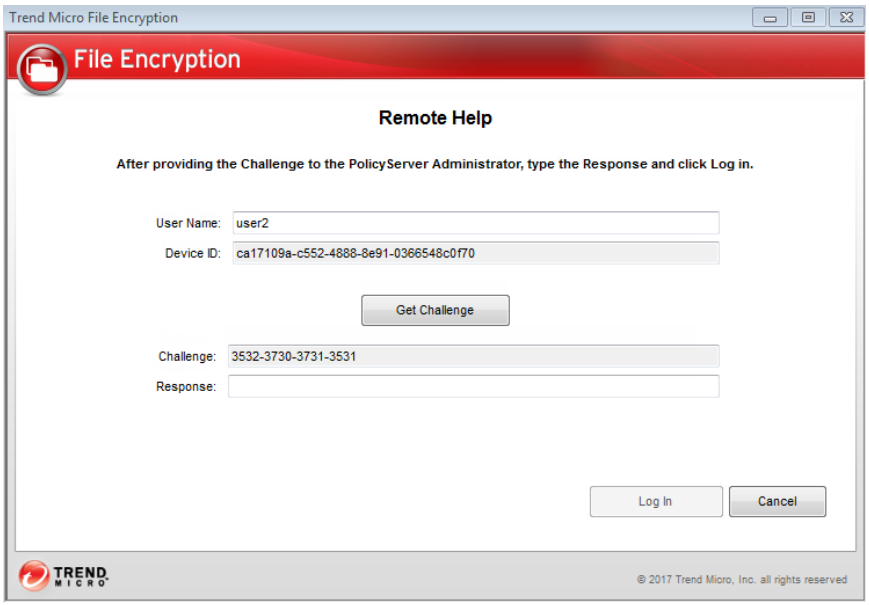



**FIGURE 6-6. Remote Help Assistance**

4. In PolicyServer MMC, open **Enterprise Devices** or expand the user's group and open **Devices**.

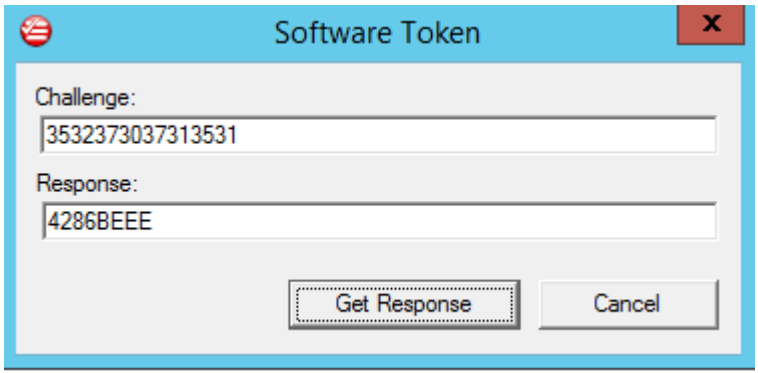
5. In the right pane, right-click the user's device and then select **Soft Token**.

   The **Software Token** window appears.

6. Get the16-digit challenge code from the user, and type it into the **Challenge** field of the **Software Token** window.

7. Click **Get Response**.

   The **Response** field loads with an 8-character string.




8. Tell the user the 8-character string from the **Response** field.

9. The user inputs the string in the **Response** field on the endpoint and clicks **Login**.

10. The user must specify a new password.

## Support Information Setup

The Support Information policy specifies information about the organization's Support Help Desk. You can uniquely configure the Support Information policy for each group.

**Procedure**

1. Log on to PolicyServer MMC with either an Enterprise Administrator/Authenticator account or a Group Administrator/Authenticator account within the same policy group as the user.
2. Expand the user's group and go to **Policies** > **Full Disk Encryption** > **Login**.
3. Right-click the **Support Info** policy and select **Add**.
4. Specify support information.
5. Click **OK**.

## Using Remote Help to Unlock Full Disk Encryption Devices

**Important**

- Restarting the Endpoint Encryption device resets the challenge code.
- Manually synchronizing policies with PolicyServer also resets the challenge code.
- The challenge code and response code are not case sensitive.

**Procedure**

1. From the Full Disk Encryption preboot, go to **Menu** > **Authentication** > **Remote Help**.
2. Provide the **Challenge Code** to the Policy/Group Administrator.
3. Specify the **Response Code** provided by the Policy/Group Administrator.
4. Click **Login**.

   The **Change Password** screen appears.

**Note**

If the account uses domain authentication, the endpoint boots directly into Windows.

5. Specify and confirm new password, then click **Next**.

   The device boots into Windows.

## Using Remote Help to Unlock a File Encryption Device

If a user exceeds the number of authentication attempts and policies are set to enact Remote Authentication, File Encryption locks Endpoint Encryption folders and notifies the user that Remote Help is required. Using Remote Help to unlock File Encryption requires assistance from the Enterprise Authenticator or Group Authenticator.

**Note**

For information about using Remote Help, see *Remote Help on page 2-15*.

**Procedure**

1. Right-click the File Encryption tray icon, then select **Remote Help**.

The **Remote Help** screen appears.

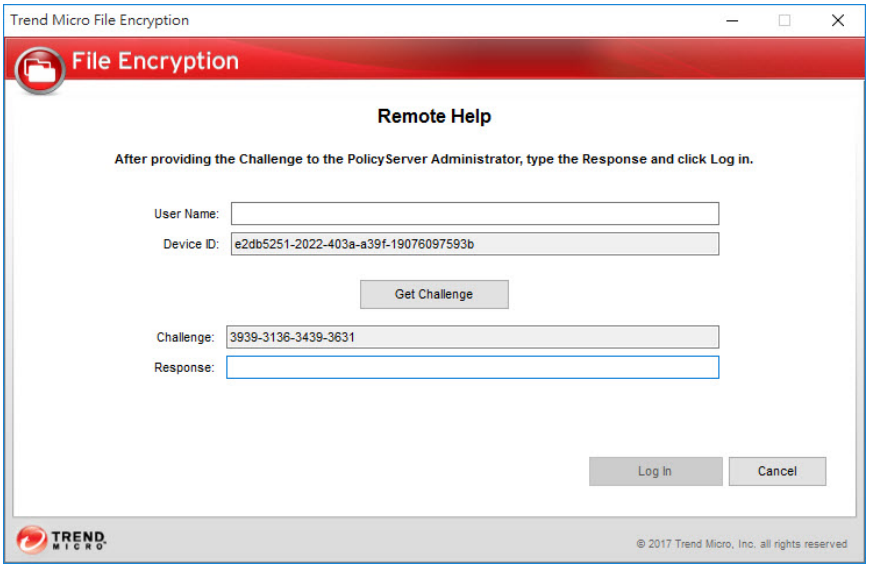



**FIGURE 6-7. File Encryption Remote Help**

2. Specify the user name.
3. Click **Get Challenge**.
4. Type the **Response** provided by the Enterprise/Group Authenticator.
5. Click **Log In**.

   The user is authenticated to File Encryption and a notification displays.

## Managing Password Setting Objects from Active Directory

Endpoint Encryption supports fine-grained password policies through Active Directory. If PolicyServer is in the Active Directory computer list, password policies in Active

Directory supersede PolicyServer policy settings from both Control Manager and PolicyServer MMC.

The following procedure shows how to add PolicyServer to the Active Directory computer list.

**Procedure**

1. Open your Password Settings object (PSO) Security settings.
    a. Go to **Start** > **Administrative Tools** > **Active Directory Users and Computers**.
    b. In the **View** menu, verify that **Advanced Features** are enabled.
    c. Locate your domain node in **Active Directory Users and Computers**
    d. Go to **System** > **Password Settings Container**.
    e. Select the PSO Property that you intend to use for password policy management.
    f. Go to the **Security** tab.
2. Add the PolicyServer endpoint to the **Group or user names** list.
    a. Under the **Group or user names** list, click **Add...**.
    b. In the **Object Types** window, select **Computers**.
    c. Select the PolicyServer endpoint.
3. Verify and confirm your changes.

# Chapter 7

# Devices in PolicyServer MMC

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

This chapter explains how to administer PolicyServer MMC to manage policies affecting Endpoint Encryption devices, and how to ensure data security by using the specialized Endpoint Encryption devices widget. This chapter also explains how to restore deleted Endpoint Encryption devices.

Topics include:


- *Adding a Device to a Group on page 5-11*
- *Removing a Device from a Group on page 5-12*
- *Deleting a Device from the Enterprise on page 7-5*
- *Getting a Software Token on page 7-6*
- *Using the Recovery Key on page 7-7*
- *Viewing Device Attributes on page 7-8*
- *Viewing Directory Listing on page 7-11*

- *Viewing Group Membership on page 7-11*
- *Killing a Device on page 7-12*
- *Locking a Device on page 7-13*
- *Resetting a Device on page 7-13*
- *Restoring a Deleted Device on page 7-14*

# Adding a Device to a Group

**Note**

Each Endpoint Encryption device can belong to only one group.

**Procedure**

1. In the left pane, expand the desired policy group and click **Devices**.
2. In the right pane, right-click the whitespace and select **Add Device**.

   The **Add Devices to Group** screen appears.

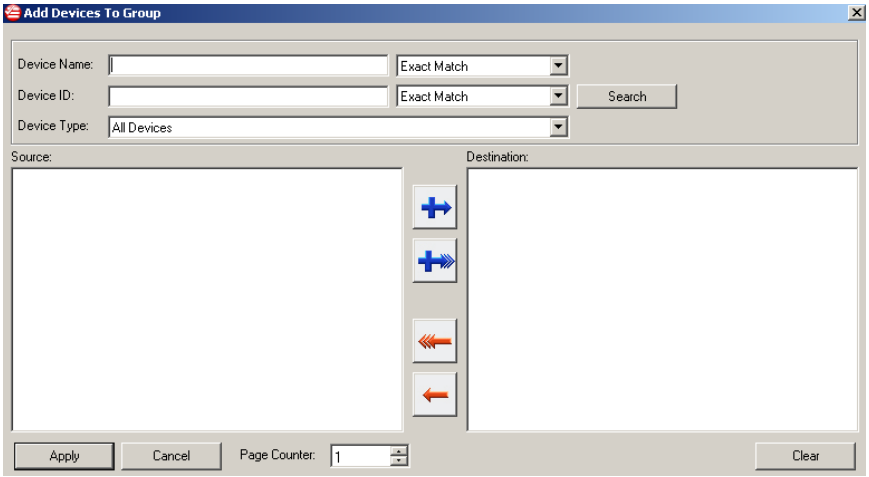



**FIGURE 7-1. Add Devices to Group Screen**

3. Type the device details, then click **Search**.

   If there is a match, the **Source** field populates with Endpoint Encryption devices.
4. Select applicable Endpoint Encryption devices from the **Source** field, then click the **blue arrow** to add them.

   For information about search icons, see *Add/Remove Search Result Icons on page 6-14*.

5. Click **Apply** to add the Endpoint Encryption device to the selected group.

   The Endpoint Encryption device is added to the group.

## Add/Remove Search Result Icons

| CENTER ICONS | DESCRIPTION |
|---|---|
| | Add a single selected item to **Destination** field. |
| | Add all found items based on search criteria to **Destination** field. |
| | Remove a single selected item from **Destination** field. |
| | Remove all items from **Destination** field. |

# Removing a Device from a Group

Removing a device from a group removes the device from the selected group only.

**WARNING!**

To remove a device from all groups, remove it from the Enterprise. Before deleting a device from the Enterprise, verify that the device has been unencrypted and that all Endpoint Encryption agents were uninstalled. Failure to do so may result in irreversible data loss.

**Procedure**

1. Expand the group, then open **Devices**.
2. In the right pane, right-click the device and select **Remove Device**.

   A warning message appears.
3. Click **Yes**.

   The device is removed.

# Deleting a Device from the Enterprise

Deleting any Endpoint Encryption device from the Enterprise also removes the device from all policy groups. The deleted Endpoint Encryption device continues functioning as long as connectivity and password policies are current on the device. However, Endpoint Encryption users cannot recover files if the Endpoint Encryption device has a critical hardware failure after it has been removed from the Enterprise. To mitigate this risk, immediately decrypt the Endpoint Encryption device and uninstall the Endpoint Encryption agent software.

For information about removing a device from a specific group, but not the Enterprise, see *Removing a Device from a Group on page 5-12*.

**Procedure**

1. Uninstall the Endpoint Encryption agent from the endpoint.

   **Note**

   For information about uninstalling Endpoint Encryption agents, see the *Endpoint Encryption Installation and Migration Guide*.
2. Open **Enterprise Devices**.
3. In the right pane, right-click the device and select **Delete Device**.

4. At the warning message, click **Yes** to confirm.

   The Endpoint Encryption device is deleted from the Enterprise.

> **Note**
>
> For information about adding the Endpoint Encryption device back the Enterprise, see *Restoring a Deleted Device on page 7-14*.

# Getting a Software Token

Generating a "software token" creates a unique string that you can use to unlock Endpoint Encryption devices and to remotely help Endpoint Encryption users reset forgotten passwords.

> **Note**
>
> The software token is only available in the full version of Full Disk Encryption, not Encryption Management for Apple FileVault or Encryption Management for Microsoft BitLocker.

For information about resetting passwords or unlocking a user account, see *Remote Help Assistance on page 6-27*.

**Procedure**

1. Open **Enterprise Devices** or expand a group and open **Devices**.

   All devices in the Enterprise or group appear in the right pane.

2. Right-click the device and select **Soft Token**.

   The **Software Token** screen appears.

3. Get the16-digit challenge code from the user, and type it into the **Challenge** field of the **Software Token** window.

4. Click **Get Response**.

   The **Response** field loads with an 8-character string.

5. Tell the user the 8-character string from the **Response** field.

   The Endpoint Encryption device is unlocked and the Endpoint Encryption user can log on to the device.

## Using the Recovery Key

Generating a "recovery key" allows the user to decrypt a hard disk when the user has forgotten the original password or key. The recovery key is only available to Encryption Management for Apple FileVault and Encryption Management for Microsoft BitLocker agents because they do not use the other recovery methods available in Full Disk Encryption.

**Note**

The recovery key is used for encrypted devices and is only available as an option when applicable devices are selected.

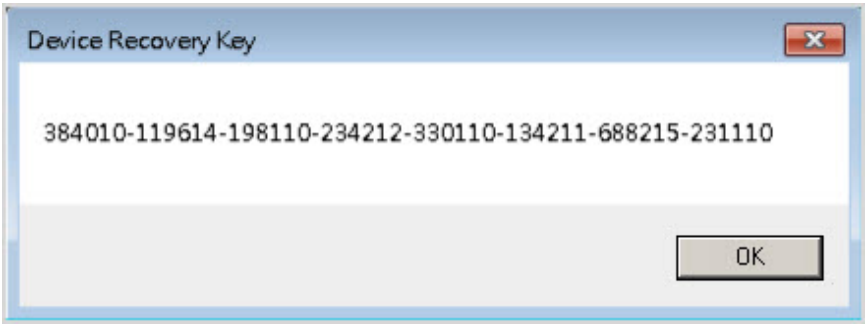
**Procedure**

1. Open **Enterprise Devices** or expand a group and open **Devices**.

   All devices in the Enterprise or group appear in the right pane.

2. In the right pane, right-click the device, then select **Recovery Key**.

The **Recovery Key** screen appears.




3. Copy the recovery key for use on the locked device.
4. Click **OK**.

# Viewing Device Attributes

Use **Device Attributes** to view a current snapshot of the selected device.

**Procedure**

1. Open **Enterprise Devices** or expand a group and open **Devices**.

   All devices in the Enterprise or group appear in the right pane.

2. In the right pane, right-click the device and select **Device Attributes**.

   The **Device Attributes** screen appears.

## Device Attributes

The following table describes the Endpoint Encryption device attributes.

| Attribute Name | Example | Description |
|---|---|---|
| AD NetBIOS Name | Enterprise | The name assigned to the AD NetBIOS. |
| AD Object GUID | 6629bdeb-99a8-456b-b7c5-dbbc50ad13d0 | The GUID assigned to the AD object. |
| Battery Count | 2 | The number of batteries installed. |
| .NET Version | 2.0.50727.3620 | The version and build number for the installed .NET framework. |
| Common Framework Build Number | 5.0.0.84 | The Endpoint Encryption agent uses a common framework for encryption. The build number is used to tell whether the agent is up-to-date. |
| Disk Model | VMware Virtual IDE | The hard disk model. |
| Disk Name | \\.\PHYSICALDRIVE0 | The name of the hard disk. |
| Disk Serial Number | | The serial number of the hard disk. |
| Disk Partitions | 1 | The number of partitions on the disk with the agent installed. |
| Disk Size | 10733990400 | The total capacity of the hard disk (in bytes). |
| Domain Name | WORKGROUP | The domain that the endpoint is a member. |
| Endpoint ID | 85b1e3e2a3c25d882540ef6e4818c3e4 | The unique ID of the endpoint used for Control Manager integration. |
| File Encryption Version | 6.0.0.1039 | The version of File Encryption installed on the endpoint. |
| Hostname | TREND-4136D2DB3 | The endpoint's host name. |
| IP Address | 10.1.152.219 | The endpoint's IP address. |
| Language | English (United States) | The language used by the endpoint. |

| Attribute Name | Example | Description |
|---|---|---|
| Locale | en-US | The regional settings used by the endpoint. |
| MAC Address | 00-50-56-01-xx-xx | The endpoint's MAC address. |
| Machine Name | TREND-4136D2DB3 | The computer name that the endpoint used. |
| Manufacturer | VMware, Inc. | The manufacturer of the hard disk. |
| Model | VMware Virtual Platform | The model of the hard disk. |
| Operating System | Microsoft Windows NT 5.1.2600 Service Pack 3 | The operating system installed on the same hard disk as the agent. |
| Operating System Name | Microsoft Windows XP Professional | The common name of the operating system installed on the same hard disk as the agent. |
| Operating System Service Pack | Service Pack 3 | The service pack number of the operating system installed on the same hard disk as the agent. |
| Operating System Version | 5.1.2600.196608 | The version number of the operating system installed on the same hard disk as the agent. |
| Partition Scheme | Classical MBR | The partition scheme for the hard disk. |
| Processor | x86 Family 6 Model 30 Stepping 5, Genuine Intel | The processor make and model of the endpoint. |
| Processor Count | 2 | The number of processors in the endpoint. |
| Processor Revision | 1e05 | The processor revision number. |
| Time Zone | Taipei Standard Time | The time zone that the endpoint resides. |
| Total Physical Memory | 2047MB | The total RAM installed in or allocated to the endpoint. |

| ATTRIBUTE NAME | EXAMPLE | DESCRIPTION |
|---|---|---|
| Type | X86-based PC | The endpoint processor type. |
| Windows User Name | TREND-4136D2DB3\admin | The user name of the Windows account that last logged on the endpoint. |
| <Agent> User | john_smith | The user name for the last logged on used. |
| <Agent> Version | 5.0.0.260 | The version and build number for the agent installation. |

# Viewing Directory Listing

**Note**

Use Directory Listing to view the directory structure of KeyArmor devices. Directory Listing is only available in environments that have upgraded from a previous PolicyServer version that had registered KeyArmor devices.

**Procedure**

1. Open **Enterprise Devices** or expand a group and open **Devices**.

   All devices in the Enterprise or group appear in the right pane.

2. In the right pane, right-click the device and select **Directory Listing**.

   The **Device Directory Snapshot** screen appears.

# Viewing Group Membership

**Note**

A device can belong to only one group.

**Procedure**

1. Open **Enterprise Devices** or expand a group and open **Devices**.

   All devices in the Enterprise or group appear in the right pane.

2. In the right pane, right-click the device and select **List Groups**.

   The **Group Membership** screen appears.

# Killing a Device

Initiating a "kill" command deletes all Endpoint Encryption device data. The deleted data is different depending on the scope of data that the associated Endpoint Encryption agent manages. For example, initiating a "kill" command to a Full Disk Encryption device deletes all data from the endpoint, while initiating a "kill" command to a File Encryption device deletes all files and folders in local or removable storage protected by the File Encryption agent. The "kill" command is issued when the Endpoint Encryption agent communicates with PolicyServer.

**WARNING!**

Killing a device cannot be undone. Back up all the data before initiating a kill command.

**Procedure**

1. Open **Enterprise Devices** or expand a group and open **Devices**.

   All devices in the Enterprise or group appear in the right pane.

2. In the right pane, right-click the device and select **Kill Device**.

3. At the warning message, click **Yes**.

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

# Locking a Device

Initiating a "lock" command to the Endpoint Encryption device prevents Endpoint Encryption user access until after performing a successful Remote Help authentication. Locking a device reboots the endpoint and forces it into a state that requires Remote Help. The lock command is issued when the Endpoint Encryption agent communicates with PolicyServer.

---

**Procedure**

1. Open **Enterprise Devices** or expand a group and open **Devices**.

   All devices in the Enterprise or group appear in the right pane.

2. In the right pane, right-click the Endpoint Encryption device and select **Lock Device**.

3. At the warning message, click **Yes**.

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

---

# Resetting a Device

Initiating a "soft reset" command reboots the endpoint. The command issues the next time that the agent communicates with PolicyServer.

---

**Procedure**

1. Open **Enterprise Devices** or expand a group and open **Devices**.

   All devices in the Enterprise or group appear in the right pane.

2. In the right pane, right-click the Endpoint Encryption device and select **Soft Reset**.

3. At the warning message, click **Yes**.

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

# Restoring a Deleted Device

For both Control Manager and PolicyServer MMC environments, use the PolicyServer MMC Recycle Bin node to restore a deleted Endpoint Encryption device.

**Procedure**

1. Log on to PolicyServer MMC.
2. Expand the Enterprise, then go to **Enterprise Maintenance**.
3. Expand the **Recycle Bin**.
4. Open **Deleted Devices**.

   The right pane loads all deleted Endpoint Encryption devices.
5. Right-click the Endpoint Encryption device and select **Restore Device**.

   The Endpoint Encryption device is added back to the Enterprise, but does not belong to any policy groups.

# Chapter 8

# Advanced Enterprise Features

In environments primarily managed by Control Manager, use PolicyServer MMC for advanced options including certain reports, logs, and maintenance. Endpoint Encryption keeps comprehensive logs and generates reports about events and updates. Use logs and reports to assess policy controls and to verify component updates. Enterprise maintenance provides a way to purge inactive users, inactive devices, and logs matching specific criteria from the database.

Topics include:


- *Enterprise Maintenance on page 8-2*
- *Restoring Deleted Users and Devices on page 8-8*
- *Enterprise Log Events on page 8-9*
- *Enterprise Reports on page 8-14*
- *Maintenance Tools on page 8-20*

# Enterprise Maintenance

PolicyServer records system activities (changes made to policies, successful authentication attempts, devices locked due to too many unsuccessful logon attempts) and maintains those records as log events. You can generate reports on an as-needed or scheduled basis.

PolicyServer MMC has a variety of built-in reports to verify device encryption status, user/device activity, and PolicyServer integrity.

**Note**

Only Enterprise Administrator accounts can use reports.

Topics include:


- *Purge Inactive Users on page 8-2*
- *Purge Inactive Devices on page 8-4*
- *Log Purge on page 8-6*


## Purge Inactive Users

An inactive user is a user account that has not logged on any Endpoint Encryption devices for a specified time period.

The Enterprise Maintenance node in PolicyServer MMC allows you to purge inactive Endpoint Encryption users and devices, then view the purged user or device log events in a report. Additionally, you can set specific criteria to purge the log database at a specific time or on a schedule.

**WARNING!**

Purged user accounts cannot authenticate to any Endpoint Encryption devices.

## Purging Inactive Users

**Procedure**

1. Log on to PolicyServer MMC.
2. Expand the Enterprise, then go to **Enterprise Maintenance**.
3. Click **Purge Inactive Users**.
4. Specify the number of days to purge all user accounts that have not logged on a device for period of time.

   **Note**

   Specify a range between 7 and 999 days.

5. Click **Purge**.
6. Click **OK** to confirm the purge.

Anything meeting the purge criteria is deleted from the database.

## Viewing the Purge Inactive Users Log Event

**Procedure**

1. Log on to PolicyServer MMC.
2. Click **Enterprise Log Events**.

   All current log events appear in the right pane.

3. At the bottom of the page, click **Filter**.

   The **Search Filter** window appears.

4. From the **Message ID** drop-down list, select **200105, Inactive Users Removed from Enterprise**.

5. Click **Search**.

   All log event matching the specified criteria appear.

6. Double-click a log event.

   The **Log Record** window appears displaying all log data for the selected event.

### Viewing the Purge Inactive Users Report

**Procedure**

1. Log on to PolicyServer MMC.
2. Expand the Enterprise, then go to **Enterprise Maintenance**.
3. Click **Enterprise Scheduled Reports**.
4. Do one of the following in the right pane:
   - To view the report in tabular format, double-click **Purged Inactive Users**.
   - To view the report in HTML format, right-click a report and then select **Display Report**.

## Purge Inactive Devices

An inactive device is any Endpoint Encryption device that has not been logged on for a specified time period.

The Enterprise Maintenance node in PolicyServer MMC allows you to purge inactive Endpoint Encryption users and devices, then view the purged user or device log events in a report. Additionally, you can set specific criteria to purge the log database at a specific time or on a schedule.

**WARNING!**

Users cannot log on to purged Endpoint Encryption devices.

## Purging Inactive Devices

**Procedure**

1. Log on to PolicyServer MMC.
2. Expand the Enterprise, then go to **Enterprise Maintenance**.
3. Click **Purge Inactive Devices**.
4. Specify the number of days to purge all user accounts that have not logged on any Endpoint Encryption device for period of time.
5. Click **Purge**.
6. Click **OK** to confirm the purge.

Anything meeting the purge criteria is deleted from the database.

## Viewing the Purge Inactive Devices Log Event

**Procedure**

1. Log on to PolicyServer MMC.
2. Click **Enterprise Log Events**.

   All current log events appear in the right pane.
3. At the bottom of the page, click **Filter**.

   The **Search Filter** window appears.
4. From the **Message ID** drop-down list, select **200303, Inactive Devices Removed from Enterprise**.
5. Click **Search**.

   All log event matching the specified criteria appear.
6. Double-click a log event.

The **Log Record** window appears displaying all log data for the selected event.

### Viewing the Purged Inactive Devices Report

**Procedure**

1. Log on to PolicyServer MMC.
2. Expand the Enterprise, then go to **Enterprise Maintenance**.
3. Click **Enterprise Scheduled Reports**.
4. Do one of the following in the right pane:
   - To view the report in tabular format, double-click **Purged Inactive Devices**.
   - To view the report in HTML format, right-click a report and then select **Display Report**.

The report appears.

## Log Purge

The Enterprise Maintenance node in PolicyServer MMC allows you to purge inactive Endpoint Encryption users and devices, then view the purged user or device log events in a report. Additionally, you can set specific criteria to purge the log database at a specific time or on a schedule.

### Purging the Log Database

**Procedure**

1. Log on to PolicyServer MMC.
2. Expand the Enterprise, then go to **Enterprise Maintenance**.
3. Click **Purge Log Database**.

4. Select **Enable scheduled purge**.
5. Configure the following options:

| OPTION | DESCRIPTION |
|---|---|
| Purge logs older than <X> days | Specify the number of days to keep logs. Anything older than the specified number of days is purged. |
| Interval type | Select to purge the log database daily, weekly, biweekly, or monthly. |
| Start date | Select when to start the scheduled purge. |
| Time | Specify the time of day for the scheduled purge. |

6. Click **Apply**.
7. At the confirmation message, click **OK**.

Anything meeting the purge criteria is deleted from the database.

## Viewing the Log Database Purge Event

**Note**

The log database purge only occurs once the schedule criteria has been met. If no data matches the search criteria, verify that the schedule is correctly set. For details, see *Purging the Log Database on page 8-6*.

**Procedure**

1. Log on to PolicyServer MMC.
2. Click **Enterprise Log Events**.

   All current log events appear in the right pane.
3. At the bottom of the page, click **Filter**.

   The **Search Filter** window appears.

4. From the **Message ID** drop-down list, select **103104, Log data purged from Enterprise**.
5. Click **Search**.

   All log event matching the specified criteria appear.
6. Double-click a log event.

   The **Log Record** window appears displaying all log data for the selected event.

# Restoring Deleted Users and Devices

Use the PolicyServer MMC Recycle Bin to restore a deleted Endpoint Encryption user or device. All deleted Endpoint Encryption users and devices are stored in the Recycle Bin at the Enterprise level. Groups do not have a recycle bin. Restoring a deleted Endpoint Encryption user or device does not add it back to previously assigned policy groups.

## Restoring a Deleted User

For both Control Manager and PolicyServer MMC environments, use the PolicyServer MMC Recycle Bin node to restore a deleted Endpoint Encryption user.

**Procedure**

1. Log on to PolicyServer MMC.
2. Expand the **Recycle Bin**.
3. Open **Deleted Users**.

   The right pane loads all deleted users.
4. Right-click the user account, then select **Restore User**.

   The user is added back to the Enterprise, but does not belong to any policy groups.

## Restoring a Deleted Device

For both Control Manager and PolicyServer MMC environments, use the PolicyServer MMC Recycle Bin node to restore a deleted Endpoint Encryption device.

**Procedure**

1. Log on to PolicyServer MMC.
2. Expand the Enterprise, then go to **Enterprise Maintenance**.
3. Expand the **Recycle Bin**.
4. Open **Deleted Devices**.

   The right pane loads all deleted Endpoint Encryption devices.
5. Right-click the Endpoint Encryption device and select **Restore Device**.

   The Endpoint Encryption device is added back to the Enterprise, but does not belong to any policy groups.

# Enterprise Log Events

PolicyServer records log events using predefined criteria including access attempts, system errors, modifications to users or groups, policy changes, and compliance issues. Managing log events and reports allows Enterprise Administrator and Group Administrator accounts to search for specific log events and report about server and client security.

Topics include:


- *Managing Log Events on page 8-10*
- *Alerts on page 8-10*
- *Enabling PolicyServer to relay SMS and Email Delivery on page 8-12*

## Managing Log Events

Only messages within the last seven (7) days automatically display. Use the filter to view older log events. It is useful to search the logs using the message ID. For example, searching for the message ID "400008" displays all "Device Encryption Complete" messages. For information about message IDs, see *PolicyServer Message IDs on page A-1*.

---

**Procedure**

1. Log on to PolicyServer MMC.
2. Select a log event level:
   - For enterprise-level logs, expand **Enterprise Log Events**.
   - For group-level logs, go to **Group Name** > **Log Events.**

   The log window appears. All log events for the past seven (7) days automatically display.
3. Double-click any log to view details.
4. Click **Filter** to search the log file:
   a. Specify the search criteria.
   b. Select the date range.
   c. Click **Search**.
5. Click **Refresh** to update log data.
6. Click **Previous** or **Next** to navigate through log data.

---

## Alerts

You can customize alert criteria using predefined security levels to help categorize alerts. Send log events to individual or multiple email recipients by setting alerts at the enterprise or group.

**Note**

For information about message IDs, see *PolicyServer Message IDs on page A-1*.

## Setting PolicyServer Alerts

**Procedure**

1. Log on to PolicyServer MMC.
2. Select a log event level:
   - For enterprise-level logs, expand **Enterprise Log Events**.
   - For group-level logs, go to **Group Name** > **Log Events.**

   The log window appears. All log events for the past seven (7) days automatically display.
3. Click **Alerts**.
4. In the right pane whitespace, right-click and select **Add**.

   The **Edit Alert** window appears.
5. Specify an **Alert Name**.
6. Select the severity of logs that trigger alerts.
7. Select the message IDs to trigger alerts.
8. Specify one email address per line to send the alert notification.
9. Select whether to send alerts based on the number of events in a set time.
10. Click **Done**.

## Enabling PolicyServer to relay SMS and Email Delivery

This function only works for PolicyServer installed on Windows Server 2008 or Windows Server 2008 R2.

**Procedure**

1. Log on to the Windows server.
2. Open **Server Manager**.
3. Go to **Features** > **Add Features**.
4. Mark **SMTP Server**.

   The **Add role services and features required for SMTP Server** window appears.
5. Click **Add Required Role Services**.
6. Click **Next**.
7. Click **Next** again.
8. Click **Install**.

   The Web Server IIS and SMTP Server installs.
9. Click **Close**.
10. Go to **Start** > **Administrative Tools** > **Internet Information Services (IIS) 6.0 Manager**.

    IIS 6.0 Manager opens.
11. Expand **ServerName (local device)**.
12. Right-click **[SMTP Virtual Server #1]** and click **Properties**.

    **Note**

    Mark **Enable logging** for future troubleshooting.
13. Go to **Access** > **Connection...** and select **Only the list below**, and then click **Add...**.

14. In the **IP address** field, specify `127.0.0.1`, then click **OK**.

> **Note**
>
> Repeat to specify all IP addresses on local server

15. Click **OK**.
16. Go to **Delivery** > **Advanced...** and specify the **Masquerade domain** in the following format: `psproxy.<domain>.<com/org>`.
17. Click **OK** twice to close the **SMTP Virtual Server #1 Properties** window.
18. Go to **Enterprise Policies** > **PolicyServer** > **PDA** > **Email**.
19. Open **SMTP ServerName**, specify `127.0.0.1`, then click **Apply**.

## Configuring Advanced Premise

For best results, create a Sender Policy Framework (SPF) DNS entry. To create an SPF record in other DNS Servers (BIND), consult the vendor documentation.

**Procedure**

1. On a Windows DNS Server, open **DNS Management Console**.
2. Right-click the forward lookup zone for the domain, and select **Other New Records**.
3. Scroll down and select **TEXT (TXT)**.
4. Leave **Record Name** blank, and specify:

   ```
   v=spf1 ip4:<external_PolicyServer_IP_address> -all
   ```

5. Click **OK**.

# Enterprise Reports

PolicyServer records log events using predefined criteria including access attempts, system errors, modifications to users or groups, policy changes, and compliance issues. Managing log events and reports allows Enterprise Administrator and Group Administrator accounts to search for specific log events and report about server and client security.

Enterprise Administrator accounts can generate reports on an as-needed or scheduled basis. PolicyServer MMC has a variety of built-in reports to verify Endpoint Encryption device encryption status, Endpoint Encryption user or device activity, and PolicyServer integrity.

**Note**

Only the Enterprise Administrator can use reports.

Topics include:


- *Report Options on page 8-14*
- *Report Icons on page 8-15*
- *Report Types on page 8-15*
- *Displaying Reports on page 8-19*
- *Scheduling Reports on page 8-19*
- *Displaying Report Errors on page 8-20*


## Report Options

The following table describes the options available for different reports. Right-click a report to view available options.

| Report Option | Description |
|---|---|
| Clear | Remove all information displayed in the results window; it does not delete the information. |
| Display Error | View a description of the error causing the report to be invalid. |
| Display Report | View the report. |
| Next Page | Move to the next page of the search items. |
| Previous Page | Return to the previous page of the search items. |
| Refresh | Update the status of a submitted report. |
| Remove Report | Delete the report. |
| Schedule Report | Set up a schedule for the report to be run on a specific day or time. |
| Submit Report | Generate the selected report. |

## Report Icons

The following table describes the icons that may appear next to a report.

| Icon | Description |
|---|---|
| | Standard reports can be submitted on an as-needed basis to view statistics and other usage metrics. |
| | Alert reports notify Enterprise Administrator accounts about potential security issues. |

## Report Types

Reports make log information easier to understand. PolicyServer MMC separates reports into two distinct categories:

- *Standard Reports on page 8-16*

  Standard reports capture specific log information in a report format. Submit standard reports on an as-needed basis.

- *Alert Reports on page 8-18*

  Alert reports send an alert notification to the Enterprise Administrator and capture the security incident in a report.

**Note**

Only the Enterprise Administrator can use reports.

## Standard Reports

Use the following table to understand which standard reports are available to generate as needed.

**TABLE 8-1. List of Standard Reports**

| REPORT NAME | DESCRIPTION |
|---|---|
| Device Encryption Status | Reports the encryption status for all Endpoint Encryption devices in the Enterprise. |
| Device Operating System Count | Reports all device operating systems and the count for each. |
| Device Version Count | Reports all Endpoint Encryption device versions and the count for each. |
| Devices By Last Sync Date | Reports all Endpoint Encryption devices that synchronized with PolicyServer in the last x amount of days. |
| Devices Not Communicating | Reports the Endpoint Encryption devices that have not communicated in the last <X> days. |
| Devices with Last Logged in User | Reports all Endpoint Encryption devices and the last user to have authenticated to it. |

| Report Name | Description |
|---|---|
| Enterprise Available License | Reports the days left in the license, available Endpoint Encryption devices and users, and count of used devices and users. |
| Enterprise Inactive User | Reports all Endpoint Encryption users who have not logged on to Endpoint Encryption devices for a specified time period. |
| Enterprise User Activity | Reports total Endpoint Encryption devices, total Endpoint Encryption users, and PolicyServer MMC user count along with Endpoint Encryption device activity. |
| Full Disk Encryption Device Not 100% Encrypted | Reports all Endpoint Encryption devices in the last <X> days that started encrypting but did not finish. |
| User Activity By Day | Reports the Endpoint Encryption user activity within <X> amount of days for the given user. |
| Users Added | Reports all Endpoint Encryption users added within the last <X> days. |
| Users Never Logged into a Device | Reports all Endpoint Encryption users who have never authenticated to any Endpoint Encryption device. |

## Running Standard Reports

Standard reports capture specific log information in a report format. Submit standard reports on an as-needed basis.

**Procedure**

1. Right-click the desired report, then select **Submit Report**.
2. Specify report parameters if required, then click **Apply**.

   The report appears.
3. To view the report, go to **Enterprise Reports** > **Enterprise Submitted Reports**.

## Alert Reports

Use the following table to understand when PolicyServer generates an alert report.

| ALERT NAME | DESCRIPTION |
|---|---|
| Consecutive Failed Logon Attempts on a Single Device | An alert is sent when multiple, consecutive authentication attempts to any Endpoint Encryption device have all failed. |
| Log Integrity Alert | An alert is sent when there is an indication that the PolicyServer logs have been tampered with. |
| Policy Tampering Alert | An alert is sent when PolicyServer detects that an entity has tampered with policies. |
| Primary and Secondary Action Enforced | An alert is sent when PolicyServer has had no connection, and the primary or secondary action has been enforced. |

### Running Alert Reports

To view the generated report, go to **Enterprise Reports** > **Enterprise Submitted Reports**.

---

**Procedure**

1. Right-click the desired alert report, then select **Configure Alerts**.

   The **Alerts Configuration** window appears.

2. Specify the **SMTP Server Address** and the **Sender** that will process the outgoing email message.

3. Click **Apply**.

4. Right-click the desired report and select **Submit Alert**.

---

## Displaying Reports

**Note**

Only the Enterprise Administrator can use reports.

**Procedure**

1. Go to **Enterprise Reports** > **Enterprise Submitted Reports**.
2. Right-click desired report, then select **Display Report**.

   The report appears.
3. To export the report, click the **Save** icon and then select **Excel** or **Acrobat (PDF) file**.

## Scheduling Reports

Schedule a report to automatically run at any specific date and time.

**Procedure**

1. Open **Enterprise Reports**.
2. Right-click the desired report, then select **Schedule Report**.

   The **Report Parameters** window displays.
3. Specify the report parameters, then click **Apply**.

   The **Report Scheduler** displays.
4. Specify the report interval, date and time, then click **Apply**.

   The report is scheduled.

5. To view scheduled reports, go to **Enterprise Reports** > **Enterprise Scheduled Reports**.

## Displaying Report Errors

Sometimes an error prevents a report from correctly running. To view PolicyServer message IDs, see *PolicyServer Message IDs on page A-1*.

**Procedure**

1. Go to **Enterprise Reports** > **Enterprise Submitted Reports**.
2. Right-click the report with an error, then select **Display Error**.

   The report error message displays.

# Maintenance Tools

This section describes additional utilities packaged with Endpoint Encryption that perform product maintenance tasks. Endpoint Encryption includes the following tools:

| TOOL | DESCRIPTION |
|---|---|
| Diagnostics Monitor | View Endpoint Encryption event logs in real time.<br>See *Using the Diagnostics Monitor on page 8-21*. |
| Log Server Tool | Generate a log package for all events that occur while replicating specific issues.<br>See *Using the Log Server Tool on page 8-24*. |
| PolicyServer Change Settings Tool | Modify your SQL server and Windows service user credentials without reinstalling PolicyServer.<br>See *Using the PolicyServer Change Settings Tool on page 8-25*. |

| TOOL | DESCRIPTION |
|---|---|
| License Renewal Tool | Update your Endpoint Encryption license Activation Code without reinstalling PolicyServer in environments managed by PolicyServer MMC.<br><br>See *Using the License Renewal Tool on page 8-26*. |
| Command Line Helper | Generate individual encrypted strings to use for authentication in other processes such as installation, upgrade, or patch scripts.<br><br>See *Using the Command Line Helper on page 8-30*. |

## Using the Diagnostics Monitor

The Diagnostic Monitor allows administrators to view events related to Endpoint Encryption in real time.

**Procedure**

1. Copy, download, or locate a PolicyServer installation package on the endpoint you have installed PolicyServer on.

   To download the PolicyServer installation package or the Endpoint Encryption Suite, go to the Trend Micro Download Center:

   http://downloadcenter.trendmicro.com/

2. Go to `<PolicyServer Directory>\TMEE_PolicyServer\Tools\Diagnostics Monitor`.

3. Run the file `DiagnosticMonitor.exe` as an administrator.

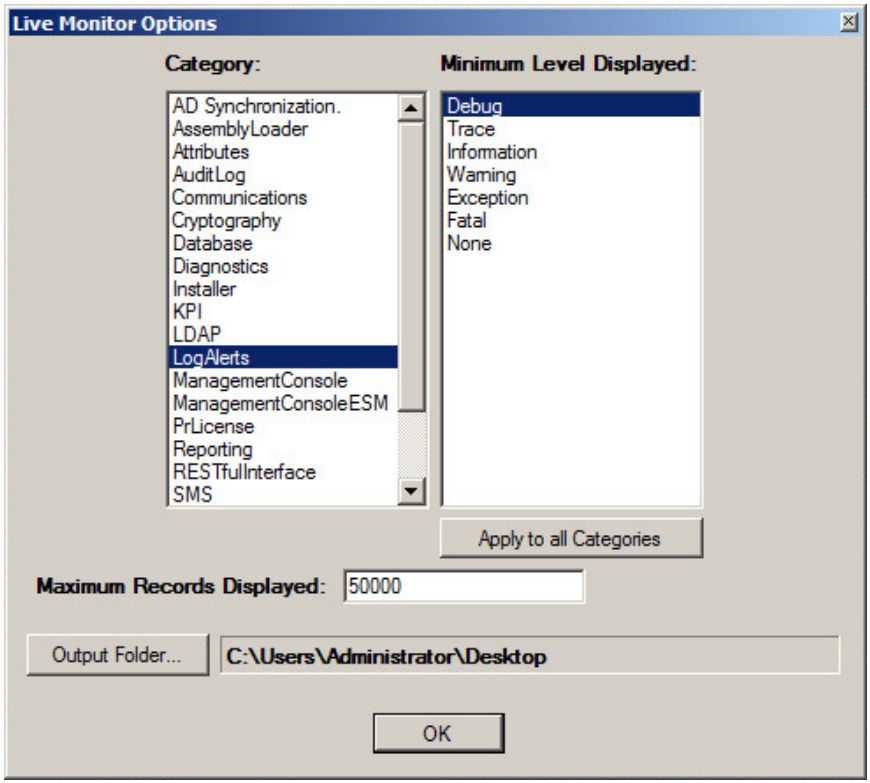
   The **License Renewal Tool** screen opens.

   **Important**

   Windows may encounter an error titled **Xenocode Postbuild 2010** at this point. The message text states that the application is unable to load a required virtual machine component. If this error occurs, open Windows Update, remove the update "KB3045999", and try to run Diagnostic Monitor again.

4. Go to **File** > **Options...**.

   The **Live Monitor Options** screen appears.




5. Go to **LogAlerts** and set the **Minimum Level Displayed** to **Debug**.

6. Set the **Maximum Records Displayed** field to a value between "3000" and "50000".

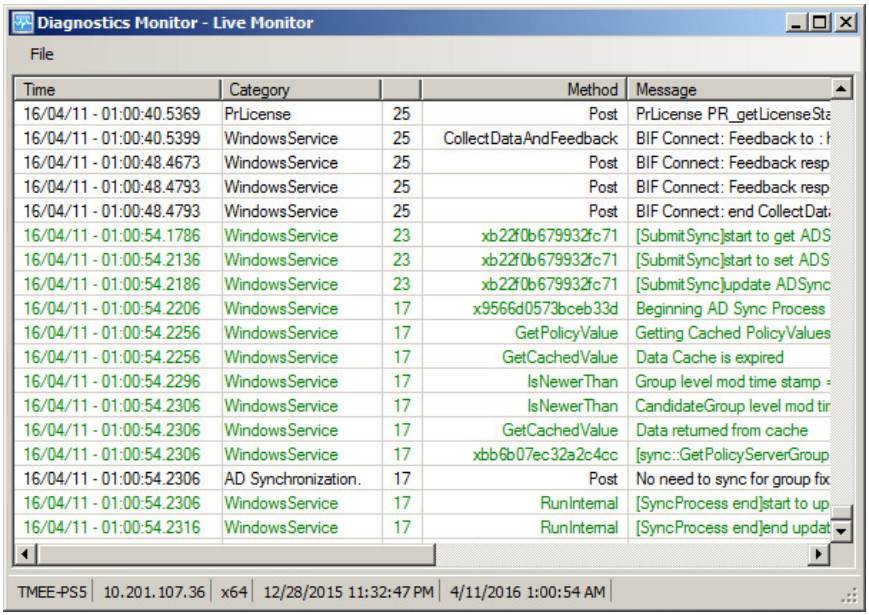
   After setting the **Maximum Records Displayed** value, an event may appear in Diagnostic Monitor stating that the system is out of memory. If this event appears, return to this window and set the **Maximum Records Displayed** to a lower value.

7. Click **Apply to all Categories** or select individual categories and apply specific settings to each of them.

8. Restart the service PolicyServerWindowsService from Windows Task Manager.

   When the PolicyServer service restarts, Active Directory synchronizes with PolicyServer. The Diagnostic Monitor will display events related to Active Directory synchronization.

9. View the logs in the Diagnostic Monitor window.




10. If you are using Diagnostic Monitor to troubleshoot a specific issue, perform all tasks necessary to replicate that issue while Diagnostic Monitor is open.

11. To generate a file of the diagnostic logs, go to **File** > **Save to File**.

    A log file appears at your selected output folder. The default output folder is the desktop. To change your selected output folder, go to **File** > **Option** > **Output Folder**.

    The name of the file is a timestamp of when you generated the file and the format is PSDM.

**Note**

If you contact Trend Micro Support regarding an issue, the support representative may request that you send a copy of the diagnostic logs for bug verification.

## Using the Log Server Tool

The Log Server Tool allows administrators to record all events related to Endpoint Encryption over a period of time to troubleshoot specific issues. The recorded logs are intended for use by Trend Micro Support, so Trend Micro does not recommend using the Log Server Tool on your own. If you have an issue, contact Trend Micro Support, and the support representative may request that you replicate your issue while using the Log Server Tool.

**Procedure**

1. Open the PolicyServer program folder.

   The default installation path is `C:\Program Files\Trend Micro \PolicyServer`.

2. Run the file `LogServer.exe` as an administrator.

   A command prompt titled **LogServer.exe** appears. The Log Server Tool is running at this time.

   The Log Server Tool generates PolicyServer diagnostic logs. The logs appear as a file named `psdedebug.log` in a folder named `log` in the PolicyServer program folder.

3. Perform all tasks necessary to replicate the issue that you contacted Trend Micro Support to address.

4. Close the command prompt titled **LogServer.exe**.

5. Send the file `psdedebug.log` to the support representative who requested that you use this tool.

## Using the PolicyServer Change Settings Tool

The main purpose of the PolicyServer Change Settings Tool is to allow administrators to change their SQL Server database credentials without requiring the user to reinstall PolicyServer. Additionally, this tool includes several related features, including testing the database connection and changing the PolicyServer Windows Service credentials.

---

**Procedure**

1. Copy, download, or locate a PolicyServer installation package on the endpoint you have installed PolicyServer on.

   To download the PolicyServer installation package or the Endpoint Encryption Suite, go to the Trend Micro Download Center:

   http://downloadcenter.trendmicro.com/

2. Go to `<PolicyServer Directory>\TMEE_PolicyServer\Tools \PolicyServer Change Settings`.

3. Run the file `PolicyServerChangeSettings.exe` as an administrator.

4. Accept the End User License Agreement (EULA) to continue.

   The EULA only appears the first time that you run this tool.

5. Change your settings as necessary using any of the following options:

| OPTION | DESCRIPTION |
|---|---|
| Primary Database | Specify your primary database SQL Server credentials in this section.<br><br>If you only have one database that serves as both your primary database and your log database, select **Use Primary Settings for Log Database**. |
| Log Database | If your primary database and log database are separate, specify your log dabase SQL Server credentials in this section.<br><br>This section is disabled if **Use Primary Settings for Log Database** is selected. |

| OPTION | DESCRIPTION |
|---|---|
| Load From Disk | Reset the credentials for the **Primary Database** and **Log Database** sections with the last saved configuration. |
| Test Connection | Check that PolicyServer can communicate with the databases shown in the **Primary Database** and **Log Database** sections. |
| Write To Disk | Overwrite the last saved configuration with the credentials in the **Primary Database** and **Log Database** sections. |
| Restart PS | Restart PolicyServer.<br><br>If you changed the credentials and clicked **Write To Disk**, PolicyServer will attempt to connect using the new SQL Server credentials. |
| Change Service Credentials... | Change the credentials for the PolicyServer Windows Service.<br><br>The **Change PS Credentials** window appears if you select this option. You may use either the local Windows system account or specify the credentials for a different account. |

## Using the License Renewal Tool

The License Renewal Tool allows administrators to update the Endpoint Encryption license in an environment managed entirely by PolicyServer MMC.

**Note**

If you manage Endpoint Encryption from Control Manager, use the license management options available in Control Manager. For more information, see the Control Manager documentation:

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

If your Activation Code is for a new license of Endpoint Encryption or a renewal of your license, the endpoint requires a connection to the Endpoint Encryption database, but does not require Internet access. If your Activation Code is for an extension of an existing license, the endpoint requires Internet access.

**Procedure**

1. Obtain your Activation Code from your Trend Micro service representative.

   If you have a Registration Key, go to Customer Licensing Portal to register your product. Trend Micro will email your Activation Code after product registration. Access the Customer Licensing Portal at:

   https://clp.trendmicro.com/

2. Copy, download, or locate a PolicyServer installation package on the endpoint you have installed PolicyServer on.

   To download the PolicyServer installation package or the Endpoint Encryption Suite, go to the Trend Micro Download Center:

   http://downloadcenter.trendmicro.com/

3. Go to `<PolicyServer Directory>\TMEE_PolicyServer\Tools\TMEE_LicenseRenewal`.

4. Run the file `TMEE_LicenseRenewal.exe` as an administrator.

   The **License Renewal Tool** screen opens.

5. Type your Activation Code in the **New Activation Code** field and click **Activate**.

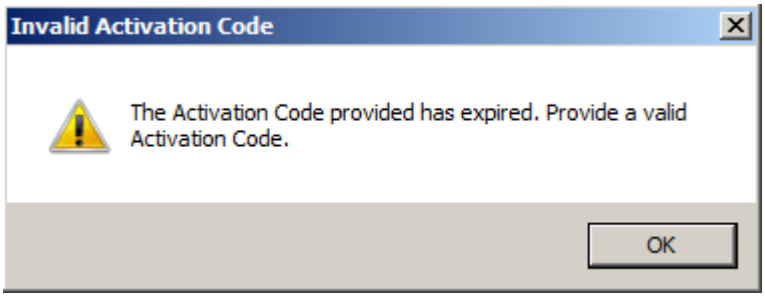
   Your license activates and all functions of Endpoint Encryption become available.

**Note**

After attempting to extend a license, you may encounter an error stating that your Activation Code has expired. To resolve this issue, see *Troubleshooting License Extension on page 8-28*.

## Troubleshooting License Extension

If you use the License Renewal Tool to extend an existing license, the following error may appear:




This error may occur due to a mismatch of your system registry with a proxy server in your network. Perform the following procedure to validate this potential cause and resolve this issue.

**Procedure**

1. Run Diagnostic Monitor on the same endpoint as the License Renewal Tool.

   For more information regarding the Diagnostic Monitor, see *Using the Diagnostics Monitor on page 8-21*.

2. View events near the time that you attempted to run the License Renewal Tool for the following events in the **Message** column:

   PrLicenlicensese PR_onlineUpdateLicensex64(): ret = E001005A, status = 60010123

   PrLicense [ActivationCodeValidator] onlineUpdatePrLicense Ret = E001005A, onlineUpdateState = 60010123, Status = 0

**Note**

If these messages appear, the issue is likely the aforementioned mismatch of your system registry with a proxy server. Continue this procedure to attempt to resolve the issue.

If these message do not appear, contact Trend Micro Support.

3. Open Windows Registry Editor.

   To access Registry Editor, type "regedit" into **Run** or the Windows search box.

4. Go to `HKEY_LOCAL_MACHINE\\SOFTWARE\\Trend Micro, Inc.`.

5. Right-click the folder `Trend Micro, Inc.` and go to **New** > **Key**.

6. Rename the new key folder **NetworkProxy**.

7. In the **NetworkProxy** folder, add the following values:

| NAME | TYPE | DATA | NOTES |
|---|---|---|---|
| ProxyServer | String value | The domain or IP address of the proxy server | This value is required. |
| ProxyPort | DWORD value | The proxy server port | If this value does not exist, the default port is "80". |
| ProxyType | DWORD value | Valid values:<br>• "0": HTTP proxy<br>• "1": SOCKS4 or SOCKS5 proxy | If this value does not exist, the default value is "0". |
| Account | String value | The account ID for proxy authentication | This value is only necessary for SOCKS proxies that require authentication. |

| NAME | TYPE | DATA | NOTES |
|---|---|---|---|
| Password | String value | The password for proxy authentication | This value is only necessary for SOCKS proxies that require authentication.<br><br>This value must be an encrypted value using Command Line Helper. See *Using the Command Line Helper on page 8-30*. |

8. Attempt to extend your license using the License Renewal Tool again.

## Using the Command Line Helper

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

**Procedure**

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

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

   http://downloadcenter.trendmicro.com/

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

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

2. Open a command prompt.

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

   Example:

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

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

   Example:

   ```
   CommandLineHelper.exe examplepassword
   ```

   **Tip**

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

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

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

   The Command Line Helper produces an encrypted string.

# Chapter 9

# Technical Support

Learn about the following topics:


- *Troubleshooting Resources on page 9-2*
- *Contacting Trend Micro on page 9-3*
- *Sending Suspicious Content to Trend Micro on page 9-4*
- *Other Resources on page 9-5*

# Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

## Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

**Procedure**

1. Go to http://esupport.trendmicro.com.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.

**Tip**

To submit a support case online, visit the following URL:

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

A Trend Micro support engineer investigates the case and responds in 24 hours or less.

## Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy. The Threat Encyclopedia

provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to http://about-threats.trendmicro.com/us/threatencyclopedia#malware to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

# Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone or email:

| | |
|---|---|
| Address | Trend Micro, Incorporated<br>225 E. John Carpenter Freeway, Suite 1500<br>Irving, Texas 75062 U.S.A. |
| Phone | Phone: +1 (817) 569-8900<br>Toll-free: (888) 762-8736 |
| Website | http://www.trendmicro.com |
| Email address | support@trendmicro.com |

- Worldwide support offices:

  http://www.trendmicro.com/us/about-us/contact/index.html

- Trend Micro product documentation:

  http://docs.trendmicro.com

## Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

# Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

## Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://ers.trendmicro.com/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

http://esupport.trendmicro.com/solution/en-US/1112106.aspx

## File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

Record the case number for tracking purposes.

## Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

http://global.sitesafety.trendmicro.com/

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

# Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

## Download Center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

http://www.trendmicro.com/download/

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

## Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

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

# Appendices

## Appendices

# Appendix A

## PolicyServer Message IDs

The following table explains PolicyServer error messages. Use it to find a Message ID, to understand the associated message meaning, the category of the message, and which agents/products the message affects.

**TABLE A-1. PolicyServer Message IDs**

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| Administrator Alerts | 100002 | Identifying Device | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Administrator Alerts | 100003 | Security Violation | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Administrator Alerts | 100007 | Critical Severity | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| Administrator Alerts | 100019 | Policy Change Unsuccessful | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Administrator Alerts | 100045 | Unsupported configuration | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Administrator Alerts | 100046 | Enterprise Pool created | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Administrator Alerts | 100047 | Enterprise Pool deleted | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Administrator Alerts | 100048 | Enterprise Pool modified | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Administrator Alerts | 100049 | Admin User locked due to too many failed logins. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Administrator Alerts | 100052 | Policy Value Integrity Check Failed | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |

| Category | Message ID | Description | Products |
|---|---|---|---|
| Administrator Alerts | 100053 | Policy request aborted due to failed policy integrity check. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Administrator Alerts | 100054 | File request aborted due to failed policy integrity check. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Administrator Alerts | 100055 | Admin Authentication Succeeded | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Administrator Alerts | 100056 | Admin Authentication Failed | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Administrator Alerts | 100062 | Admin Password Reset | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Administrator Alerts | 100463 | Unable to remove user. Try again. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Administrator Alerts | 100464 | Unable to unable user. Try again. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| Administrator Alerts | 100470 | Unable to change Self Help password. A response to one of the personal challenge questions was incorrect. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Administrator Alerts | 102000 | Enterprise Added | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Administrator Alerts | 102001 | Enterprise Deleted | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Administrator Alerts | 102002 | Enterprise Modified | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Administrator Alerts | 102003 | The number of users has exceeded the maximum allowed by this license. Reduce the number of existing users to restore this user account. | PolicyServer |
| Administrator Alerts | 200000 | Administrator updated policy | PolicyServer |
| Administrator Alerts | 200001 | Administrator added policy | PolicyServer |
| Administrator Alerts | 200002 | Administrator deleted policy | PolicyServer |

| Category | Message ID | Description | Products |
|---|---|---|---|
| Administrator Alerts | 200003 | Administrator enabled application | PolicyServer |
| Administrator Alerts | 200004 | Administrator disabled application | PolicyServer |
| Administrator Alerts | 200100 | Administrator added user | PolicyServer |
| Administrator Alerts | 200101 | Administrator deleted user | PolicyServer |
| Administrator Alerts | 200102 | Administrator updated user | PolicyServer |
| Administrator Alerts | 200103 | Administrator added user to group | PolicyServer |
| Administrator Alerts | 200104 | Administrator removed user from group | PolicyServer |
| Administrator Alerts | 200200 | User added | PolicyServer |
| Administrator Alerts | 200201 | User deleted | PolicyServer |
| Administrator Alerts | 200202 | User added to group | PolicyServer |
| Administrator Alerts | 200203 | User removed from group | PolicyServer |
| Administrator Alerts | 200204 | User updated | PolicyServer |
| Administrator Alerts | 200300 | Administrator deleted device | PolicyServer |
| Administrator Alerts | 200301 | Administrator added device to group | PolicyServer |
| Administrator Alerts | 200302 | Administrator removed device from group | PolicyServer |

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| Administrator Alerts | 200500 | Administrator added group | PolicyServer |
| Administrator Alerts | 200501 | Administrator deleted group | PolicyServer |
| Administrator Alerts | 200502 | Administrator updated group | PolicyServer |
| Administrator Alerts | 200503 | Administrator copy/ pasted group | PolicyServer |
| Administrator Alerts | 200600 | PolicyServer update applied. | PolicyServer |
| Administrator Alerts | 200602 | User added to device | PolicyServer |
| Administrator Alerts | 200603 | User removed from device | PolicyServer |
| Administrator Alerts | 200700 | Event executed successfully | PolicyServer |
| Administrator Alerts | 200701 | Failed event execution | PolicyServer |
| Administrator Alerts | 200800 | Event installed successfully | PolicyServer |
| Administrator Alerts | 200801 | Failed to install event | PolicyServer |
| Administrator Alerts | 700012 | Administrator Logged In Using One Time Password | File Encryption SP6 or Earlier |
| Administrator Alerts | 700013 | Administrator Logged In Using Fixed Password | File Encryption SP6 or Earlier |

| Category | Message ID | Description | Products |
|---|---|---|---|
| Administrator Alerts | 700014 | Administrator Logged In using Smart Card | File Encryption SP6 or Earlier |
| Administrator Alerts | 700017 | Administrator Logged In Using Remote Authentication | File Encryption SP6 or Earlier |
| Administrator Alerts | 700030 | Administrator Failed log In Using One Time Password | File Encryption SP6 or Earlier |
| Administrator Alerts | 700031 | Administrator Failed log In Using Fixed Password | File Encryption SP6 or Earlier |
| Administrator Alerts | 700032 | Administrator Failed log In using Smart Card | File Encryption SP6 or Earlier |
| Administrator Alerts | 700035 | Administrator Failed log In Using Remote Authentication | File Encryption SP6 or Earlier |
| Administrator Alerts | 900100 | Administrator logged in using one-time password. | KeyArmor |
| Administrator Alerts | 900101 | Administrator logged in using fixed password. | KeyArmor |
| Administrator Alerts | 900102 | Administrator logged in using Smart Card. | KeyArmor |
| Administrator Alerts | 900103 | Administrator logged in using domain authentication. | KeyArmor |

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| Administrator Alerts | 900104 | Administrator logged in using remote authentication. | KeyArmor |
| Administrator Alerts | 900105 | Administrator logged in using ColorCode authentication. | KeyArmor |
| Administrator Alerts | 900106 | Administrator logged in using PIN. | KeyArmor |
| Administrator Alerts | 900107 | Administrator logged in using OCSP. | KeyArmor |
| Administrator Alerts | 900250 | Administrator Failed To Login Using One Time Password | KeyArmor |
| Administrator Alerts | 900251 | Administrator Failed To Login Using Fixed Password | KeyArmor |
| Administrator Alerts | 900252 | Administrator Failed To Login Using Smart Card | KeyArmor |
| Administrator Alerts | 900253 | Administrator failed to login using domain authentication. | KeyArmor |
| Administrator Alerts | 900254 | Administrator Failed To Login Using Remote Authentication | KeyArmor |
| Administrator Alerts | 900255 | Administrator failed to login using ColorCode authentication. | KeyArmor |

| Category | Message ID | Description | Products |
|---|---|---|---|
| Administrator Alerts | 900256 | Administrator failed to login using PIN. | KeyArmor |
| Administrator Alerts | 900257 | Administrator Failed To Login Using OCSP | KeyArmor |
| Administrator Alerts | 900300 | Administrator Failed log In Using Remote Authentication | KeyArmor |
| Administrator Alerts | 901000 | Administrator Renamed A File | KeyArmor |
| Administrator Alerts | 901001 | Administrator Changed A File | KeyArmor |
| Administrator Alerts | 901002 | Administrator Deleted A File | KeyArmor |
| Administrator Alerts | 901003 | Administrator Created A File | KeyArmor |
| Audit Log Alerts | 100015 | Log Message | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Audit Log Alerts | 103000 | Audit Log Connection Opened | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Audit Log Alerts | 103001 | Audit Log Connection Closed | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| Audit Log Alerts | 103100 | Audit Log Record Missing | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Audit Log Alerts | 103101 | Audit Log Record Integrity Missing | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Audit Log Alerts | 103102 | Audit Log Record Integrity Compromised | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Audit Log Alerts | 103103 | Audit Log Record Integrity Validation Started | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Audit Log Alerts | 104003 | Authentication method set to SmartCard. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Audit Log Alerts | 904008 | Unable To Send Log Alert | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Authenticator Alerts | 700006 | Authenticator Logged In Using One Time Password | File Encryption SP6 or Earlier |

| Category | Message ID | Description | Products |
|---|---|---|---|
| Authenticator Alerts | 700007 | Authenticator Logged In Using Fixed Password | File Encryption SP6 or Earlier |
| Authenticator Alerts | 700008 | Authenticator Logged In using Smart Card | File Encryption SP6 or Earlier |
| Authenticator Alerts | 700009 | Authenticator Logged In using Windows Credentials | File Encryption SP6 or Earlier |
| Authenticator Alerts | 700011 | Authenticator Logged In Using Remote Authentication | File Encryption SP6 or Earlier |
| Authenticator Alerts | 700024 | Authenticator Failed log In Using One Time Password | File Encryption SP6 or Earlier |
| Authenticator Alerts | 700025 | Authenticator Failed log In Using Fixed Password | File Encryption SP6 or Earlier |
| Authenticator Alerts | 700026 | Authenticator Failed log In using Smart Card | File Encryption SP6 or Earlier |
| Authenticator Alerts | 700027 | Authenticator Failed log In using Windows Credentials | File Encryption SP6 or Earlier |
| Authenticator Alerts | 700029 | Authenticator Failed log In Using Remote Authentication | File Encryption SP6 or Earlier |
| Authenticator Alerts | 900050 | Authenticator logged in using one-time password. | KeyArmor |

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| Authenticator Alerts | 900051 | Authenticator logged in using fixed password. | KeyArmor |
| Authenticator Alerts | 900052 | Authenticator logged in using Smart Card. | KeyArmor |
| Authenticator Alerts | 900053 | Authenticator logged in using domain authentication. | KeyArmor |
| Authenticator Alerts | 900054 | Authenticator logged in using remote authentication. | KeyArmor |
| Authenticator Alerts | 900055 | Authenticator logged in using ColorCode authentication. | KeyArmor |
| Authenticator Alerts | 900056 | Authenticator logged in using PIN. | KeyArmor |
| Authenticator Alerts | 900057 | Authenticator logged in using OCSP. | KeyArmor |
| Authenticator Alerts | 900161 | User Failed To Login Using Self Help | KeyArmor |
| Authenticator Alerts | 900200 | Authenticator Failed To Login Using One Time Password | KeyArmor |
| Authenticator Alerts | 900201 | Authenticator Failed To Login Using Fixed Password | KeyArmor |

| Category | Message ID | Description | Products |
|---|---|---|---|
| Authenticator Alerts | 900202 | Authenticator Failed To Login Using Smart Card | KeyArmor |
| Authenticator Alerts | 900203 | Authenticator failed to login using domain authentication. | KeyArmor |
| Authenticator Alerts | 900204 | Authenticator Failed To Login Using Remote Authentication | KeyArmor |
| Authenticator Alerts | 900205 | Authenticator failed to login using ColorCode authentication. | KeyArmor |
| Authenticator Alerts | 900206 | Authenticator failed to login using PIN. | KeyArmor |
| Authenticator Alerts | 900207 | Authenticator Failed To Login Using OCSP | KeyArmor |
| Authenticator Alerts | 902000 | Authenticator Renamed A File | KeyArmor |
| Authenticator Alerts | 902001 | Authenticator Changed A File | KeyArmor |
| Authenticator Alerts | 902002 | Authenticator Deleted A File | KeyArmor |
| Authenticator Alerts | 902003 | Authenticator Created A File | KeyArmor |
| Certificate Alerts | 104008 | Certificate expired. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| Device Alerts | 100001 | PDA to Desktop Sync Authentication was unsuccessful. There was no device ID for this PDA found. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Device Alerts | 100012 | Device is not in its own Password Authentication File. PAF corrupted? | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Device Alerts | 100044 | Lock Device Action Received | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Device Alerts | 100071 | Device Kill Confirmed | KeyArmor |
| Device Alerts | 100072 | Device Lock Confirmed | KeyArmor |
| Device Alerts | 100100 | Install Started | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor |
| Device Alerts | 100101 | Install Completed | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor |
| Device Alerts | 100462 | Unable to connect to PolicyServer. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |

| Category | Message ID | Description | Products |
|---|---|---|---|
| Device Alerts | 101001 | The network connection is not working. Unable to get policy files from PolicyServer. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Device Alerts | 101002 | Corrupted PAF (DAFolder.xml) file | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Device Alerts | 105000 | Unable to synchronize policies with client. Verify that there is a network connection and try again. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Device Alerts | 200400 | Device added | PolicyServer |
| Device Alerts | 200401 | Device deleted | PolicyServer |
| Device Alerts | 200402 | Device added to group | PolicyServer |
| Device Alerts | 200403 | Device removed from group | PolicyServer |
| Device Alerts | 200404 | Device modified | PolicyServer |
| Device Alerts | 200405 | Device status updated | PolicyServer |
| Device Alerts | 200406 | Device status reset | PolicyServer |
| Device Alerts | 200407 | Device Kill Issued | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| Device Alerts | 200408 | Device Lock Issued | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Device Alerts | 200409 | Device Synchronized | PolicyServer |
| Device Alerts | 904012 | User Not Allowed To Register New Device | PolicyServer |
| Device Alerts | 1000052 | Uninstall of product | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor |
| Device Alerts | 1000053 | Product Uninstall Denied By Policy | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor |
| Error Alerts | 100005 | General Error | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Error Alerts | 100006 | Application Error | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| File Encryption Activity Alerts | 700000 | User Logged In Using One Time Password | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 700001 | User Logged In Using Fixed Password | File Encryption SP6 or Earlier |

| Category | Message ID | Description | Products |
|---|---|---|---|
| File Encryption Activity Alerts | 700002 | User Logged In using Smart Card | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 700003 | User Logged In using Windows Credentials | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 700005 | User Logged In Using Remote Authentication | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 700015 | Administrator Logged In using Windows Credentials | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 700018 | User Failed log In Using One Time Password | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 700019 | User Failed log In Using Fixed Password | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 700020 | User Failed log In using Smart Card | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 700021 | User Failed log In using Windows Credentials | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 700023 | User Could not log In Using Remote Authentication | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 700033 | Administrator Failed log In using Windows Credentials | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 700036 | Failed Login Attempts Exceeded | File Encryption SP6 or Earlier |

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| File Encryption Activity Alerts | 701000 | Encrypted File Using User Key | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 701001 | Encrypted File Using Group Key | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 701002 | Encrypted File Using Static Password | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 701003 | Self-extracting encrypted file created using a static password. | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 701004 | Encrypted File Using Cert | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 701005 | Self-extracting encrypted file created using certificate. | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 701006 | Encrypted File Using CD/DVD Burning | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 701007 | Encrypted Directory Using Group Key | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 701008 | Encrypted Directory Using Static Password | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 701009 | Self-extracting encrypted directory created using a static password. | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 701010 | Encrypted Directory Using Cert | File Encryption SP6 or Earlier |

| Category | Message ID | Description | Products |
|---|---|---|---|
| File Encryption Activity Alerts | 701011 | Self-extracting encrypted directory created using certificate. | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 701012 | Encrypted Directory Using CD/DVD Burning | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 701015 | Removable Media was fully encrypted | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 701016 | Removable Media Blocked | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 701017 | Removable Media Created and Covered Folders | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 701018 | File encrypted and moved to removable media. | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 701019 | File deleted from removable media. | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 703000 | File Armor Encrypted Folder Was Created | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 703001 | Folder Was Created and Covered | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 703002 | File Armor Encrypted Folder Was Deleted | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 703004 | Removable Media Folder was Created and Covered | File Encryption SP6 or Earlier |

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| File Encryption Activity Alerts | 703005 | Removable Media Device Was Fully Encrypted | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 703006 | File In Folder Was Created | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 703007 | File in Folder Was Deleted | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 703008 | File in Folder Was Changed | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 703009 | File in Folder Was Accessed | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 703010 | File in Folder Was Last Written | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 703011 | File Size Changed in Folder | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 703015 | Folder Encryption Started | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 703016 | Folder Decryption Started | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 703017 | Folder Encryption Complete | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 703018 | Folder Decryption Complete | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 703019 | Folder Decryption In progress | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 703020 | Folder Encryption In progress | File Encryption SP6 or Earlier |
| File Encryption Activity Alerts | 704000 | File Encryption Service Started | File Encryption SP6 or Earlier |

| Category | Message ID | Description | Products |
|---|---|---|---|
| File Encryption Activity Alerts | 704001 | File Encryption Service Shutdown | File Encryption SP6 or Earlier |
| Full Disk Encryption Activity Alerts | 300700 | Device log maximum size limit reached, event log truncated. | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 400001 | User has successfully logged in. | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 400002 | User login failed. | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 400003 | Device decryption started. | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 400004 | Device Encryption Started. | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 400005 | Mounted encrypted partition. | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 400006 | Restored native OS MBR. | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 400007 | Restored Application MBR. | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 400008 | Device encryption complete | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 400009 | Device Decryption Completed | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 400010 | Device Encryption In Progress | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 400011 | System MBR Corrupt | Full Disk Encryption or MobileSentinel |

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| Full Disk Encryption Activity Alerts | 400012 | System Pre-boot Kernel Deleted | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401000 | Recovery Console accessed | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401009 | Recovery Console error | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401010 | Decryption in place started | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401011 | Decryption in place stopped | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401012 | Decryption in place complete | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401013 | Decryption of removable device started | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401014 | Decryption to removable device stopped | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401015 | Decryption to removable device complete | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401018 | Decryption in place error | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401019 | Decryption to removable device error | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401020 | Encrypted files accessed | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401021 | Encrypted files modified | Full Disk Encryption or MobileSentinel |

| Category | Message ID | Description | Products |
|---|---|---|---|
| Full Disk Encryption Activity Alerts | 401022 | Encrypted files copied to removable device | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401029 | Encrypted files access error | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401030 | Network administration accessed | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401031 | PolicyServer address changed | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401032 | PolicyServer port number changed | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401033 | Switched to IPv6 | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401034 | Switched to IPv4 | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401035 | Switched to dynamic IP configuration | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401036 | Switched to static IP configuration | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401037 | DHCP port number changed | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401038 | IP address changed | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401039 | NetMask changed | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401040 | Broadcast address changed | Full Disk Encryption or MobileSentinel |

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| Full Disk Encryption Activity Alerts | 401041 | Gateway changed | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401042 | Domain name changed | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401043 | Domain name servers changed | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401049 | Network administration error | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401050 | User administration accessed | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401051 | User added | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401052 | User removed | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401053 | User modified | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401069 | User administration error | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401070 | Locally stored logs accessed | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401079 | Locally stored logs access error | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401080 | Original MBR restored | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401089 | Original MBR restoration error | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401090 | Default theme restored | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 401099 | Default theme restoration error | Full Disk Encryption or MobileSentinel |

| Category | Message ID | Description | Products |
|---|---|---|---|
| Full Disk Encryption Activity Alerts | 402000 | Application Startup | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 402001 | Application Shutdown | Full Disk Encryption or MobileSentinel |
| Full Disk Encryption Activity Alerts | 600001 | Update was successful in the Pre-boot. | Full Disk Encryption |
| Full Disk Encryption Activity Alerts | 600002 | Pre-boot Update failed | Full Disk Encryption |
| Installation Alerts | 100004 | Install Error | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Installation Alerts | 100020 | Successful Installation | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Installation Alerts | 700037 | Installation of File Encryption was successful | File Encryption SP6 or Earlier |
| Installation Alerts | 700038 | Installation of File Encryption was unsuccessful: Enterprise name is not valid. | File Encryption SP6 or Earlier |
| Installation Alerts | 700039 | Installation of File Encryption was unsuccessful: Username or password is incorrect. | File Encryption SP6 or Earlier |

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| KeyArmorActivity Alerts | 100034 | Invalid Registry Setting Detected | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| KeyArmorActivity Alerts | 500000 | VirusDefense | KeyArmor |
| KeyArmorActivity Alerts | 500001 | Object Cleaned | KeyArmor |
| KeyArmorActivity Alerts | 500002 | Object Disinfected | KeyArmor |
| KeyArmorActivity Alerts | 500003 | Object Quarantined | KeyArmor |
| KeyArmorActivity Alerts | 500004 | Object Deleted | KeyArmor |
| KeyArmorActivity Alerts | 500005 | Virus Detected | KeyArmor |
| KeyArmorActivity Alerts | 500006 | Full Scan Started | KeyArmor |
| KeyArmorActivity Alerts | 500007 | Full Scan Completed | KeyArmor |
| KeyArmorActivity Alerts | 500008 | Object Suspicious | KeyArmor |
| KeyArmorActivity Alerts | 500009 | Object Scan Completed | KeyArmor |
| KeyArmorActivity Alerts | 500010 | Removable Media Scan Requested | KeyArmor |
| KeyArmorActivity Alerts | 500011 | Removable Media Scan Completed | KeyArmor |
| KeyArmorActivity Alerts | 500012 | Folder Scan Requested | KeyArmor |
| KeyArmorActivity Alerts | 500013 | Folder Scan Completed | KeyArmor |
| KeyArmorActivity Alerts | 500014 | Access Denied To Object | KeyArmor |
| KeyArmorActivity Alerts | 500015 | Object Corrupt | KeyArmor |

| Category | Message ID | Description | Products |
|---|---|---|---|
| KeyArmorActivity Alerts | 500016 | Object Clean | KeyArmor |
| KeyArmorActivity Alerts | 500017 | Full Scan Cancelled | KeyArmor |
| KeyArmorActivity Alerts | 500018 | Object Scan Cancelled | KeyArmor |
| KeyArmorActivity Alerts | 500019 | Removable Media Scan Cancelled | KeyArmor |
| KeyArmorActivity Alerts | 500020 | Folder Scan Cancelled | KeyArmor |
| KeyArmorActivity Alerts | 500021 | Update Started | KeyArmor |
| KeyArmorActivity Alerts | 500022 | The update was unsuccessful. Try again. | KeyArmor |
| KeyArmorActivity Alerts | 500023 | Update Cancelled | KeyArmor |
| KeyArmorActivity Alerts | 500024 | Update Successful. | KeyArmor |
| KeyArmorActivity Alerts | 500025 | VirusDefense Up To Date | KeyArmor |
| KeyArmorActivity Alerts | 500026 | PalmVirusDefense | KeyArmor |
| KeyArmorActivity Alerts | 500027 | Object Scan Requested | KeyArmor |
| KeyArmorActivity Alerts | 500028 | PPCVirusDefense | KeyArmor |
| KeyArmorActivity Alerts | 900000 | User logged in using one-time password. | KeyArmor |
| KeyArmorActivity Alerts | 900001 | User logged in using fixed password. | KeyArmor |
| KeyArmorActivity Alerts | 900002 | User logged in using Smart Card. | KeyArmor |

| Category | Message ID | Description | Products |
|---|---|---|---|
| KeyArmorActivity Alerts | 900003 | User logged in using domain authentication. | KeyArmor |
| KeyArmorActivity Alerts | 900004 | User logged in using remote authentication. | KeyArmor |
| KeyArmorActivity Alerts | 900005 | User logged in using ColorCode authentication. | KeyArmor |
| KeyArmorActivity Alerts | 900006 | User logged in using PIN. | KeyArmor |
| KeyArmorActivity Alerts | 900007 | User logged in using OCSP | KeyArmor |
| KeyArmorActivity Alerts | 900008 | User logged in using Self Help. | KeyArmor |
| KeyArmorActivity Alerts | 900009 | User logged in using RSA | KeyArmor |
| KeyArmorActivity Alerts | 900150 | User Failed To Login Using One Time Password | KeyArmor |
| KeyArmorActivity Alerts | 900151 | User Failed To Login Using Fixed Password | KeyArmor |
| KeyArmorActivity Alerts | 900152 | User Failed To Login Using Smart Card | KeyArmor |
| KeyArmorActivity Alerts | 900153 | User failed to login using domain authentication. | KeyArmor |
| KeyArmorActivity Alerts | 900154 | User Failed To Login Using Remote Authentication | KeyArmor |

| Category | Message ID | Description | Products |
|---|---|---|---|
| KeyArmorActivity Alerts | 900155 | User failed to login using ColorCode authentication. | KeyArmor |
| KeyArmorActivity Alerts | 900156 | User failed to login using PIN. | KeyArmor |
| KeyArmorActivity Alerts | 900157 | User Failed To Login Using OCSP | KeyArmor |
| KeyArmorActivity Alerts | 900158 | User locked out after too many failed login attempts. | KeyArmor |
| KeyArmorActivity Alerts | 900301 | Failed Login Attempts Exceeded | KeyArmor |
| KeyArmorActivity Alerts | 900350 | Key Wiped | KeyArmor |
| KeyArmorActivity Alerts | 903000 | User Renamed A File | KeyArmor |
| KeyArmorActivity Alerts | 903001 | User Changed A File | KeyArmor |
| KeyArmorActivity Alerts | 903002 | User Deleted A File | KeyArmor |
| KeyArmorActivity Alerts | 903003 | User Created A File | KeyArmor |
| KeyArmorActivity Alerts | 903100 | Primary action enforced due to no PolicyServer connection. | KeyArmor |
| KeyArmorActivity Alerts | 903101 | Secondary action enforced due to no PolicyServer connection. | KeyArmor |
| KeyArmorActivity Alerts | 903102 | Policy updates applied | KeyArmor |

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| KeyArmorActivity Alerts | 904000 | Repaired infected file | KeyArmor |
| KeyArmorActivity Alerts | 904001 | Unable to repair infected file. | KeyArmor |
| KeyArmorActivity Alerts | 904002 | Skipping infected file, repair unsupported | KeyArmor |
| KeyArmorActivity Alerts | 904003 | Deleted infected file | KeyArmor |
| KeyArmorActivity Alerts | 904004 | Unable to delete infected file. | KeyArmor |
| KeyArmorActivity Alerts | 904005 | Killing device due to infected file | KeyArmor |
| KeyArmorActivity Alerts | 904006 | Error killing device due to infected file | KeyArmor |
| KeyArmorActivity Alerts | 904007 | Invoking infected file fall-back action | KeyArmor |
| KeyArmorActivity Alerts | 904010 | AntiVirus files updated | KeyArmor |
| KeyArmorActivity Alerts | 904011 | Unable to update antivirus files. | KeyArmor |
| Login / Logout Alerts | 100013 | Failed Login Attempt | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100014 | Successful Login | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |

| Category | Message ID | Description | Products |
|---|---|---|---|
| Login / Logout Alerts | 100016 | Unable to log in. Use Remote Authentication to provide the PolicyServer Administrator with a challenge code. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100021 | Unsuccessful ColorCode Login | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100022 | Unsuccessful Fixed Password Login | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100023 | Unsuccessful PIN Login | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100024 | Unsuccessful X99 Login | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100028 | Successful ColorCode Login | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| Login / Logout Alerts | 100031 | Successful X9.9 Login | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100032 | Successful Remote Login | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100035 | Successful WebToken Login | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100036 | Unsuccessful WebToken Login | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100050 | Fixed Password login blocked due to lockout. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100051 | User Login Successfully Unlocked | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100057 | LDAP User Authentication Succeeded | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |

| Category | Message ID | Description | Products |
|---|---|---|---|
| Login / Logout Alerts | 100058 | LDAP User Authentication Failed | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100059 | LDAP User Password Change Succeeded | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100060 | LDAP User Password Change Failed | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100061 | Access request aborted due to failed policy integrity check. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100070 | Successful Logout | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100433 | The ColorCode passwords do not match. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100434 | Unable to change ColorCode. The new ColorCode must be different than the current one. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| Login / Logout Alerts | 100435 | Unable to change ColorCode. The new ColorCode must meet the minimum length requirements defined by PolicyServer. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100436 | Unable to change ColorCode. The new ColorCode must be different than any previous ColorCode used. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100437 | ColorCode Change Failure - Internal Error | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100459 | X9.9 Password Change Failure - Can Not Connect toPolicyServer Host | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100460 | X9.9 Password Change Failure - Empty Serial Number | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 100461 | X9.9 Password Change Failure - Internal Error | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |

| Category | Message ID | Description | Products |
|---|---|---|---|
| Login / Logout Alerts | 101004 | Unable to reset locked device. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 104000 | Smart Card login successful. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Login / Logout Alerts | 104001 | Smart Card login unsuccessful. Check that the card is seated properly and that the Smart Card PIN is valid. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Mobile Device Alert | 100037 | Palm Policy Database is missing | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Mobile Device Alert | 100038 | Palm Encryption Error | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Mobile Device Alert | 100039 | PPC Device Encryption Changed | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Mobile Device Alert | 100040 | PPC Encryption Error | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| MobileFirewall Activity Alerts | 300000 | MobileFirewall | MobileFirewall |
| MobileFirewall Activity Alerts | 300001 | DenialOfServiceAttack | MobileFirewall |
| OCSP Alerts | 104005 | OCSP certificate status good. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| OCSP Alerts | 104006 | OCSP certificate status revoked. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| OCSP Alerts | 104007 | OCSP certificate status unknown. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| OTA Alerts | 100041 | OTA Object Missing or Corrupt. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| OTA Alerts | 100042 | OTA Sync Successful | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| OTA Alerts | 100043 | OTA Device Killed | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |

| Category | Message ID | Description | Products |
|---|---|---|---|
| Password Alerts | 100017 | Change Password Error | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Password Alerts | 100018 | Password Attempts Exceeded | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Password Alerts | 100025 | Password Reset to ColorCode | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Password Alerts | 100026 | Password Reset to Fixed | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Password Alerts | 100027 | Password Reset to PIN | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Password Alerts | 100029 | Successful Fixed Password Login | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Password Alerts | 100030 | Successful PIN Password Login | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| Password Alerts | 100033 | Unable to Reset Password | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Password Alerts | 100432 | Unable to change password. The new password must be different than the current password. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Password Alerts | 100439 | Unable to change password. The passwords do not match. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Password Alerts | 100441 | Unable to change password. The password field cannot be empty. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Password Alerts | 100442 | Unable to change password. The password does not meet the minimum length requirements defined by PolicyServer. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Password Alerts | 100443 | Unable to change password. Numbers are not permitted. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |

| Category | Message ID | Description | Products |
|---|---|---|---|
| Password Alerts | 100444 | Unable to change password. Letters are not permitted. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Password Alerts | 100445 | Unable to change password. Special characters are not permitted. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Password Alerts | 100446 | Unable to change password. The password cannot contain the user name. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Password Alerts | 100447 | Unable to change password. The password does not contain enough special characters. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Password Alerts | 100448 | Unable to change password. The password does not contain enough numbers. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Password Alerts | 100449 | Unable to change password. The password does not contain enough characters. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Password Alerts | 100450 | Unable to change password. The password contains too many consecutive characters. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| Password Alerts | 100451 | Unable to change password. The new password must be different than any previous password used. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Password Alerts | 100452 | Password Change Failure - Internal Error | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Password Alerts | 101003 | Successfully changed Fixed Password. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Password Alerts | 700100 | Password reset to Fixed Password. | File Encryption SP6 or Earlier |
| Password Alerts | 700101 | Password reset to Smart Card | File Encryption SP6 or Earlier |
| Password Alerts | 700102 | Password reset to Domain Authentication. | File Encryption SP6 or Earlier |
| Password Alerts | 900159 | Unable to change password. | KeyArmor |
| Password Alerts | 900160 | Password changed successfully. | KeyArmor |
| Password Alerts | 900302 | Password reset to fixed password. | KeyArmor |
| Password Alerts | 900303 | Password reset To Smart Card | KeyArmor |

| Category | Message ID | Description | Products |
|---|---|---|---|
| Password Alerts | 900304 | Password reset to domain authentication. | KeyArmor |
| PIN Change Alerts | 100438 | Unable to change PIN. The PINs do not match. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| PIN Change Alerts | 100440 | Unable to change PIN. One of the fields are empty. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| PIN Change Alerts | 100453 | Unable to change PIN. The PINs do not match. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| PIN Change Alerts | 100454 | able to change PIN. The new PIN cannot be the same as the old PIN. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| PIN Change Alerts | 100455 | Unable to change PIN. The new PIN does not meet the minimum length requirements defined by PolicyServer. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| PIN Change Alerts | 100456 | Unable to change PIN. The PIN cannot contain the user name. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |

| CATEGORY | MESSAGE ID | DESCRIPTION | PRODUCTS |
|---|---|---|---|
| PIN Change Alerts | 100457 | Unable to change PIN. The new PIN must be different than any previous PIN used. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| PIN Change Alerts | 100458 | PIN Change Failure - Internal Error | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Smart Card Alerts | 104002 | Registered SmartCard. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Smart Card Alerts | 104004 | Unable to register Smart Card. Check that the card is seated properly and that the Smart Card PIN is valid. | Full Disk Encryption, File Encryption, DriveArmor, KeyArmor, or PolicyServer |
| Windows Mobile Alerts | 800000 | OTA Install started | Full Disk Encryption for Windows Mobile |
| Windows Mobile Alerts | 800001 | OTA Install completed | Full Disk Encryption for Windows Mobile |
| Windows Mobile Alerts | 800100 | OTA SMS message sent | Full Disk Encryption for Windows Mobile |
| Windows Mobile Alerts | 800200 | OTA Directory Listing Received | Full Disk Encryption for Windows Mobile |
| Windows Mobile Alerts | 800300 | OTA Device Attributes Received | Full Disk Encryption for Windows Mobile |
| Windows Mobile Alerts | 800400 | OTA Device Backup | Full Disk Encryption for Windows Mobile |

| Category | Message ID | Description | Products |
|---|---|---|---|
| Windows Mobile Alerts | 800500 | OTA Device Restore | Full Disk Encryption for Windows Mobile |
| Installation Alert | 905001 | Install disks successful | Full Disk Encryption |
| Installation Alert | 905002 | Install disks failed | Full Disk Encryption |
| Full Disk Encryption Activity Alerts | 905003 | Move disk successful | Full Disk Encryption |
| Full Disk Encryption Activity Alerts | 905004 | Move disk failed | Full Disk Encryption |
| Device Alert | 907001 | Database corruption | Full Disk Encryption |
| Device Alert | 907002 | Database fixed successfully | Full Disk Encryption |
| Device Alert | 907003 | Unable to fix database | Full Disk Encryption |
| Device Alert | 907004 | Data disk database corruption | Full Disk Encryption |
| Device Alert | 907005 | Data disk database fixed successfully | Full Disk Encryption |
| Device Alert | 907006 | Unable to fix data disk database | Full Disk Encryption |

# Appendix B

## Endpoint Encryption Services

The following table describes all Endpoint Encryption services. Use it to understand which services control which Endpoint Encryption agent or feature and to troubleshoot a problem.

**TABLE B-1. Endpoint Encryption Services**

| PLATFORM | SERVICE OR DAEMON NAME | DISPLAY NAME | DESCRIPTION | FILE NAME |
|---|---|---|---|---|
| PolicyServer | PolicyServer Windows Service | PolicyServer Windows Service | Manages communication between Endpoint Encryption services and databases. | `PolicyServerWindowService.exe` |
| | TMEEService | Endpoint Encryption Service | Manages Endpoint Encryption agent 5.0 (and above) communication in an encrypted channel (RESTful). | `TMEEService.exe` |
| | IIS/ MAWebService2 | Legacy Web Service | Manages Endpoint Encryption agent 3.1.3 (and older) communication in an encrypted channel (SOAP). | N/A |
| | TMEEForward | TMEEForward | Forwards traffic from Endpoint Encryption 6.0 Patch 1 agents to PolicyServer. | TMEEForward.exe |
| | TMEEProxyWindowsService | PolicyServer LDAProxy Windows Service | Provides secure communications from Trend Micro PolicyServer to remote LDAP servers | `LDAProxyWindowsServices.exe` |

| Platform | Service or Daemon Name | Display Name | Description | File Name |
|---|---|---|---|---|
| Full Disk Encryption | DrAService | Trend Micro Full Disk Encryption | Provides Trend Micro endpoint security and full disk encryption. | `DrAService.exe` |
| Encryption Management for Microsoft BitLocker | FDE_MB | Trend Micro Full Disk Encryption, Encryption Management for Microsoft BitLocker | Provides data security for endpoints using Microsoft BitLocker. | `FDEforBitLocker.exe` |
| Encryption Management for Apple FileVault | Daemon: TMFDEMM<br>Agent: Trend Micro Full Disk Encryption | Trend Micro Full Disk Encryption, Encryption Management for Apple FileVault | Provides endpoint security for endpoints using Apple FileVault. | |
| File Encryption | FileEncryption Service | Trend Micro File Encryption | Provides Trend Micro endpoint security and data protection for files, folders, and removable media devices. | `FEService.exe` |

# Appendix C

## Policy Mapping Between Management Consoles

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

The following tables explain how policies are mapped between PolicyServer MMC and Control Manager. For environments using Control Manager to manage PolicyServer, use PolicyServer MMC to control any policy not listed in the table.

**TABLE C-1. Full Disk Encryption Policy Mapping**

| CONTROL MANAGER LABEL | POLICYSERVER MMC PATH |
|---|---|
| **Encryption** | |
| **Encrypt endpoint** | **Full Disk Encryption** > **Encryption** > **Encrypt Device** |
| **Client Settings** | |
| **Bypass Full Disk Encryption preboot** | **Full Disk Encryption** > **Login** > **Preboot Bypass** |
| **Users are allowed to access system recovery tools on the device** | **Full Disk Encryption** > **Agent** > **Allow User Recovery** |

| Control Manager Label | PolicyServer MMC Path |
|---|---|
| **Notifications** | |
| **If the endpoint is found, display the following message** | **Full Disk Encryption** > **Login** > **If Found** |
| **Display Technical Support contact information** | **Full Disk Encryption** > **Login** > **Support Info** |
| **Show legal notice** | **Full Disk Encryption** > **Login** > **Legal Notice** |
| • **Show legal notice** > **Installation**<br>• **Show legal notice** > **Startup** | **Full Disk Encryption** > **Login** > **Legal Notice** > **Legal Notice** > **Legal Notice Display Time** |
| **Show legal notice** | **Full Disk Encryption** > **Login** > **Legal Notice** > **Legal Notice** > **Legal Notice Text** |

**Table C-2. File Encryption Policy Mapping**

| Control Manager Label | PolicyServer MMC Path |
|---|---|
| **Folders to Encrypt** | |
| **Folders to Encrypt** text box | **File Encryption** > **Encryption** > **Specify Folders to Encrypt** |
| **Encryption Key Used** | |
| **Encryption Key Used** | **File Encryption** > **Encryption** > **Encryption Key Used** |
| **Storage Devices** | |
| **Disable optical drives** | **File Encryption** > **Encryption** > **Disable Optical Drive** |
| **Disable USB drives** | **File Encryption** > **Encryption** > **Removable Media** > **Disable USB Drive** |

| CONTROL MANAGER LABEL | POLICYSERVER MMC PATH |
|---|---|
| **Encrypt all files and folders on USB drives** | **File Encryption** > **Encryption** > **Removable Media** > **Fully Encrypt Device** |
| **Specify the file path to encrypt on USB devices** | **File Encryption** > **Encryption** > **Removable Media** > **Folders to Encrypt On Removable Media** |
| **Notifications** | |
| **Show legal notice** | **File Encryption** > **Login** > **Legal Notice** |
| • **Show legal notice** > **Installation**<br>• **Show legal notice** > **Startup** | **File Encryption** > **Login** > **Legal Notice** > **Legal Notice Display Time** |
| **Show legal notice** text box | **File Encryption** > **Login** > **Legal Notice** > **Legal Notice Text** |

**TABLE C-3. Common Policy Mapping**

| CONTROL MANAGER LABEL | POLICYSERVER MMC PATH |
|---|---|
| **Allow User to Uninstall** | |
| **Allow non-administrator accounts to uninstall agent software** | • **Full Disk Encryption** > **Agent** > **Allow User to Uninstall**<br>• **File Encryption** > **Agent** > **Allow User to Uninstall** |
| **Lockout and Lock Device Actions** | |
| **Lock account after** *<number>* **days** | **Full Disk Encryption** > **Login** > **Account Lockout Period** |
| **Account lockout action** | **Full Disk Encryption** > **Login** > **Account Lockout Action** |
| **Failed logon attempts allowed** | **Full Disk Encryption** > **Login** > **Failed Login Attempts Allowed** |

| CONTROL MANAGER LABEL | POLICYSERVER MMC PATH |
|---|---|
| Full Disk Encryption:<br>**Device locked action** | **Full Disk Encryption** > **Login** > **Device Locked Action** |
| Full Disk Encryption:<br>**Number of minutes to lock device** | **Full Disk Encryption** > **Login** > **Lock Device Time Delay** |
| File Encryption:<br>**Device locked action** | **File Encryption** > **Login** > **Device Locked Action** |
| File Encryption:<br>**Number of minutes to lock device** | **File Encryption** > **Login** > **Lock Device Time Delay** |
| **Password** | |
| **User must change password after <*number*> days** | **Common** > **Authentication** > **Local Login** > **User Password** > **Change Password Every** |
| **User cannot reuse the previous <*number*> passwords** | **Common** > **Authentication** > **Local Login** > **User Password** > **Password History Retention** |
| **Number of consecutive characters allowed in a password** | **Common** > **Authentication** > **Local Login** > **User Password** > **Consecutive Characters Allowed** |
| **Minimum length allowed for passwords** | **Common** > **Authentication** > **Local Login** > **User Password** > **Minimum Length** |
| **Password Character Requirements** | |
| **Letters** | **Common** > **Authentication** > **Local Login** > **User Password** > **Require How Many Characters** |
| **Lowercase characters** | **Common** > **Authentication** > **Local Login** > **User Password** > **Require How Many Lower Case Characters** |

| CONTROL MANAGER LABEL | POLICYSERVER MMC PATH |
|---|---|
| **Uppercase characters** | **Common** > **Authentication** > **Local Login** > **User Password** > **Require How Many Upper Case Characters** |
| **Numbers** | **Common** > **Authentication** > **Local Login** > **User Password** > **Require How Many Numbers** |
| **Symbols** | **Common** > **Authentication** > **Local Login** > **User Password** > **Require How Many Special Characters** |

**TABLE C-4. Remote Help Policy Locations**

| POLICY NAME | POLICYSERVER MMC MENU PATH | CONTROL MANAGER MENU PATH |
|---|---|---|
| **Account Lockout Action** | **Login** > **Account Lockout Action** | **Common** > **Lockout and Lock Device Actions** > **Account Lockout Action** |
| **Account Lockout Period** | **Login** > **Account Lockout Period** | **Common** > **Lockout and Lock Device Actions** > **Lock account after [ ] days** |
| **Device Locked Action** | For each agent:<br>**Login** > **Device Locked Action** | For each agent:<br>**Common** > **Lockout and Lock Device Actions** > **Device locked action** |
| **Failed Login Attempts Allowed** | For each agent:<br>**Login** > **Failed Login Attempts Allowed** | For each agent:<br>**Common** > **Lockout and Lock Device Actions** > **Failed logon attempts allowed** |

# Appendix D

# Glossary

The following table explains the terminology used throughout the Endpoint Encryption documentation.

**TABLE D-1. Endpoint Encryption Terminology**

| TERM | DESCRIPTION |
|---|---|
| Agent | Software installed on an endpoint that communicates with a management server. |
| Authentication | The process of identifying a user. |
| ColorCode™ | The authentication method requiring a color-sequence password. |
| Command Builder | A Trend Micro tool to generate scripts used to install PolicyServer and Endpoint Encryption agents for automatic or mass deployments. |
| Command Line Helper | A Trend Micro tool for creating encrypted values to secure credentials used by Endpoint Encryption agent installation scripts. |
| Control Manager | Trend Micro Control Manager is a central management console that manages Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. |

| TERM | DESCRIPTION |
|---|---|
| Device | Any computer, laptop, or removal media (external drive, USB drive) managed by Endpoint Encryption. |
| Domain authentication | The authentication method for single sign-on (SSO) using Active Directory. |
| DriveTrust™ | Hardware-based encryption technology by Seagate™. |
| Encryption Management for Microsoft BitLocker | The Endpoint Encryption Full Disk Encryption agent for Microsoft Windows environments that simply need to enable Microsoft BitLocker on the hosting endpoint.<br><br>Use the Encryption Management for Microsoft BitLocker agent to secure endpoints with Trend Micro full disk encryption protection in an existing Windows infrastructure. |
| Encryption Management for Apple FileVault | The Endpoint Encryption Full Disk Encryption agent for Mac OS environments that simply need to enable Apple FileVault on the hosting endpoint.<br><br>Use the Encryption Management for Apple FileVault agent to secure endpoints with Trend Micro full disk encryption protection in an existing Mac OS infrastructure. |
| Endpoint Encryption Service | The PolicyServer service that securely manages all Endpoint Encryption 6.0 Patch 1 agent communication.<br><br>For Endpoint Encryption 3.1.3 and below agent communication, see Legacy Web Service. |
| Enterprise | The Endpoint Encryption Enterprise is the unique identifier about the organization in the PolicyServer database configured during PolicyServer installation. One PolicyServer database may have multiple Enterprise configurations. However, Endpoint Encryption configurations using Control Manager may only have one Enterprise. |
| File Encryption | The Endpoint Encryption agent for file and folder encryption on local drives and removable media.<br><br>Use File Encryption to protect files and folders located on virtually any device that appears as a drive within the host operating system. |

| TERM | DESCRIPTION |
|---|---|
| Fixed password | The authentication method for using a standard user password consisting of letters and/or numbers and/or special characters. |
| Full Disk Encryption | The Endpoint Encryption agent for hardware and software encryption with preboot authentication. Full Disk Encryption secures data files, applications, registry settings, temporary files, swap files, print spoolers, and deleted files on any Windows endpoint. Strong preboot authentication restricts access vulnerabilities until the user is validated. |
| Legacy Web Service | The PolicyServer service that securely manages all Endpoint Encryption 3.1.3 and below agent communication. For details, see *About PolicyServer on page 2-8*.<br><br>For Endpoint Encryption 6.0 Patch 1 communication, see Endpoint Encryption Service. |
| OfficeScan | OfficeScan protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks. An integrated solution, OfficeScan consists of an agent that resides at the endpoint and a server program that manages all agents. |
| OPAL | Trusted Computing Group's Security Subsystem Class for client devices. |
| Password | Any type of authentication data used in combination with a user name, such as fixed, PIN, and ColorCode. |
| PIN | The authentication method for using a Personal Identification Number, commonly used for ATM transactions. |
| PolicyServer | The central management server that deploys encryption and authentication policies to the Endpoint Encryption agents. |
| Remote Help | The authentication method for helping Endpoint Encryption users who forget their credentials or Endpoint Encryption devices that have not synchronized policies within a pre-determined amount of time. |

| TERM | DESCRIPTION |
|---|---|
| Recovery Console | The Full Disk Encryption interface to recover Endpoint Encryption devices in the event of primary operating system failure, troubleshoot network issues, and manage users, policies, and logs. |
| Recovery Tool | A bootable disk used to repair a device if the device is unable to boot. The Recovery Tool is distributed as an ISO file in the Full Disk Encryption installation package. |
| SED | A self-encrypting drive. SEDs provide “hardware-based encryption”, as opposed to the type of encryption that Full Disk Encryption provides, which is referred to as “software-based encryption”. |
| Self Help | The authentication method for helping Endpoint Encryption users provide answers to security questions instead of contacting Technical Support for password assistance. |
| Smart card | The authentication method requiring a physical card in conjunction with a PIN or fixed password. |

# Index


**A**

about
- authentication, 4-2
- Endpoint Encryption Service, 2-8
- groups, 3-6
- Legacy Web Service, 2-8
- PolicyServer, 2-8, 3-1
- users, 3-6

Active Directory, 2-14, 3-20, 6-18
- configuration, 3-22
- import users, 6-5
- overview, 3-21
- resetting password, 6-21

agents, 2-11
alerts, 8-10
appendices, 1
authentication, 2-3, 2-13
- about, 4-2
- ColorCode, 2-13, 2-14
- domain, 2-14
- domain authentication, 2-13
- fixed password, 2-13, 2-15
- LDAP, 2-14
- PIN, 2-15
- prerequisites, 2-14
- remote help, 6-29
- Remote Help, 2-13, 2-15
- Self Help, 2-13, 2-16, 6-25
- setup requirements, 2-14
- smart card, 2-16, 6-22, 6-23

authentication methods, 2-13

**C**

central management, 2-3
ColorCode, 2-14
Command Line Helper, 8-30
Control Manager integration, 2-9, 3-1
CSV, 6-4

**D**

data protection, 2-1
device, 2-3
devices
- add to group, 5-11, 7-3
- directory listing, 7-11
- group membership, 7-11
- kill command, 7-12
- locking, 7-13
- PolicyServer MMC, 7-1
- reboot, 7-13
- recovery key, 7-7
- remove, 7-5
- remove Enterprise device, 7-5
- remove from group, 5-12, 7-4
- software token, 7-6
- view attributes, 7-8

Diagnostic Monitor, 8-21
documentation feedback, 9-6
domain authentication, 2-14

**E**

encryption, 4-33
- features, 2-3

Endpoint Encryption, 2-1
enhancements, 2-4

**F**

File Encryption
- Remote Help, 6-30

unlock device, 6-30
fixed password, 2-15
Full Disk Encryption
authentication, 2-16
Remote Help, 6-29

**G**

groups, 3-6, 5-1
creating offline groups, 5-13
install to group, 6-15
modifying, 5-5
offline groups, 5-12
remove device, 5-12, 7-4
removing, 5-5

**H**

help desk policies, 6-28

**I**

importing users, 6-4

**K**

key features, 2-3

**L**

LDAP, 2-14
LDAP Proxy, 6-2
License Renewal Tool, 8-26
extending license, 8-28
log events, 8-9, 8-14
logs, 8-1
alerts, 8-10
managing events, 8-10
setting alerts, 8-11

**M**

maintenance, 8-2
management consoles, 2-9, 3-1

**P**

passwords, 2-3, 6-18
Remote Help, 6-27
resetting, 6-20
Active Directory, 6-21
Enterprise Administrator, 6-19
Enterprise Authenticator, 6-19
Group Administrator, 6-20
Group Authenticator, 6-20
user, 6-20, 6-21
resetting to fixed password, 6-21
Self Help, 6-25
Personal Identification Number (PIN), 2-15
PIN, 2-13
policies, 2-3
common, 4-37
agent, 4-37
authentication, 4-38
File Encryption
agent, 4-33
encryption, 4-33
login, 4-35
password, 4-36
Full Disk Encryption, 4-23, 4-33
client, 4-24
encryption, 4-26
login, 4-26
password, 4-32
indicators, 3-15, 4-6
policy mapping, C-1
PolicyServer, 4-18
Administrator, 4-19
Authenticator, 4-20
console, 4-19
log alerts, 4-21
service pack download, 4-22

welcome message, 4-22
Support Info, 6-28
policy mapping
Control Manager, C-1
PolicyServer, C-1
PolicyServer
AD synchronization, 3-20
advanced premise, 8-13
enabling applications, 3-19
getting started, 3-1
interface, 3-4
log events, 8-9, 8-14
logs, 8-1
maintenance, 8-2
MMC hierarchy, 3-5
MMC window, 4-7
policies, 4-1, 4-5, 4-7
editing, 4-8
Support Info, 6-28
relay SMS/email delivery, 8-12
Remote Help, 6-27
reports, 8-1, 8-9, 8-14
setting log alerts, 8-11
smart card, 6-23
subgroups, 5-4
Support Info, 6-28
PolicyServer Change Settings Tool, 8-25
PolicyServer MMC, 2-11, 3-1
add enterprise user, 3-11, 6-2
add top group, 3-7, 5-2
authentication, 3-3
fields and buttons, 3-16, 4-7
first time use, 3-3
groups, 3-6
adding users, 3-8, 5-5, 6-10
modifying policies, 3-17
offline groups, 5-12
creating, 5-13
updating, 5-15
policies, 3-15
editing
multiple choice, 4-12
multiple option, 4-16
policies with ranges, 4-8
text string, 4-15
True/False, Yes/No, 4-10
users, 3-6
add enterprise user, 3-8, 5-5, 6-10
add to group, 3-8, 3-13, 5-5, 5-8, 6-10, 6-12
users and groups, 3-6
product definitions, D-1


## R


Remote Help, 2-15, 6-18, 6-27, 7-13
reporting, 2-1, 2-3
reports, 8-1, 8-9, 8-14
alert, 8-18
display errors, 8-20
displaying reports, 8-19
icons, 8-15
options, 8-14
scheduled reports, 8-19
standard, 8-16, 8-17
types of, 8-15


## S


security
account lock, 2-15
account lockout action, 2-15
account lockout period, 2-15
device lock, 2-15
failed login attempts allowed, 2-15

Self Help, 2-16, 6-18
    password support, 6-25
smart card, 2-16, 6-22
    authentication, 6-23
smart cards, 2-16, 6-22
SSO, 2-14
support
    resolve issues faster, 9-4

## T

terminology, D-1
tokens, 6-23, 6-25
top group, 3-7, 5-2

## U

users, 3-6, 4-3, 6-1
    Active Directory passwords, 6-21
    adding, 6-2
    adding existing user to group, 3-13, 5-8, 6-12
    adding new user to group, 3-8, 5-5, 6-10
    add new enterprise user, 3-11, 6-2
    change default group, 6-14
    finding, 6-8
    group membership, 6-9
    group vs enterprise changes, 6-9
    import from AD, 6-5
    importing with CSV, 6-4
    install to group, 6-15
    managing, 6-7
    modifying, 6-9
    passwords, 6-18
    remove from group, 5-10, 6-17
    restore deleted, 6-17, 8-8
users and groups, 3-6

## W

what's new, 2-4

**TREND MICRO INCORPORATED**

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

www.trendmicro.com

Item Code: APEM68337/180626