

Symantec Endpoint Encryption Full Disk

Installation Guide

Version 8.2.1

Copyright © 2012 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. GuardianEdge, Encryption Anywhere, and Authenti-Check are either trademarks or registered trademarks of GuardianEdge Technologies Inc. (now part of Symantec). Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 “Commercial Computer Software - Restricted Rights” and DFARS 227.7202, et seq. “Commercial Computer Software and Commercial Computer Software Documentation”, as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
<http://www.symantec.com>

Contents

Chapter 1	Introduction	
	Overview	1
	Architecture	2
	Basics	2
	Installation Sequence	2
	Protocols and Ports	3
	System Requirements	3
	Basics	3
	Directory Service Integration	3
	Symantec Endpoint Encryption Management Server	4
	SQL Server Instance	4
	Manager Computer(s)	5
	Mac Client Computers	5
	Basics	5
	Hardware Requirements	6
	Software Requirements	6
	Windows Client Computers	6
	BIOS	6
	File System	6
	Compatibility Notes	6
	Section 508	7
	Hardware Requirements	7
	Software Requirements	7
	Token Support	8
	Account Provisioning	11
	Basics	11
	Required Accounts	11
	Synchronization Accounts	12
	Optional Group	12
	Symantec Endpoint Encryption Roles	13
	Policy Administrator	13
	Client Administrator	13
	Basics	13
	Windows Client	13
	Mac Client	14
	User	14
	Basics	14
	Mac Client	14
	Windows Client	14
Chapter 2	Installing the Symantec Endpoint Encryption Management Server	
	Management Server Installation Overview	17
	Management Server Installation Prerequisites	18
	Configuring Encrypted Client Computer/Management Server Communications	18
	Server-Side TLS/SSL Certificate Requirements	18
	Client-Side TLS/SSL Certificate Requirements	18
	Configuring Encrypted Database Communications	18

Configuring Encrypted Active Directory Synchronization Communications	19
Required Additional Software/Required Features	19
Basics	19
Windows Server 2003	19
.NET Framework	19
Internet Information Server (IIS)	20
Windows Server 2008	20
Management Server InstallShield Wizard	21
Basics	21
Initial Steps	22
Database Location and Credentials	22
Database: New or Existing	23
Management Server Account Type	23
Management Server Account with SQL Authentication	24
Management Server Account with Windows Authentication	25
Concluding Steps	25
Management Server Configuration Wizard	27
Basics	27
Directory Service Synchronization Options	27
Basics	27
Directory Service Synchronization Configuration	29
Active Directory Configuration Area	29
Novell Configuration Area	30
Page Completed	31
Web Service Configuration	31
Verification	32
Symantec Endpoint Encryption Management Server	32
Symantec Endpoint Encryption Database	33
Back Up Symantec Endpoint Encryption Database	34

Chapter 3 Installing the Symantec Endpoint Encryption Manager Console

Installation Overview	35
Before You Begin	35
Prepare for Encrypted Client Computer Communications	35
Additional Software/Required Features	36
Before You Begin	36
Windows XP	36
Group Policy Management Console	36
.NET Framework	36
Microsoft Management Console 3.0	36
Windows Server 2003 Administration Tools Pack	37
Windows Vista	37
Remote Server Administration Tools for Windows Vista	37
Windows 7	37
Windows Server 2003	38
Group Policy Management Console	38
.NET Framework	38
Microsoft Management Console 3.0	38
Windows Server 2008 and Windows Server 2008 R2	38
Manager Console Installation	39
Framework InstallShield Wizard	39
Initial Steps	39
Concluding Steps	42
Full Disk InstallShield Wizard	43
Help Desk Program	43

Basics	43
Installation	43
Add Forest	45
Back Up Symantec Endpoint Encryption Database	46
Manager Console Snap-In Access Control	46
Basics	46
Controlling Access to the Symantec Endpoint Encryption Snap-ins	47
Basics	47
Creating a Policy that Restricts Access to Snap-ins	47
Restricting Access to Snap-in Extensions	48
Creating a Policy that Permits Access to Snap-ins	49
Segmenting Support Duties	50

Chapter 4 Client Installation Package Creation

Overview	51
Framework Installation Settings Wizard	52
Basics	52
Client Administrators	52
Registered Users	54
Basics	54
Authentication Method	55
Registration	56
Unregistration	56
Next Button	56
Single Sign-On	56
Password Authentication	57
Basics	57
Password Attempts	58
Password Complexity	59
Maximum Password Age	59
Password History	59
Minimum Password Age	60
Token Authentication	60
Authentication Message	60
Authenti-Check	61
One-Time Password	62
Communication	63
Encryption	65
Saving the Framework Client Installer MSI	65
Full Disk Installation Settings Wizard	66
Basics	66
Startup	66
Basics	66
Guidelines for Creating a Custom Startup Image	67
Logon History	68
Encryption	69
Installer Customization	70
Hardware Configuration	71
Client Monitor	71
Mac Client Package	72
Saving the Full Disk Client Installer MSI	73

Chapter 5 Client Installations

Overview	75
----------------	----

Basics	75
Windows Clients	75
Mac Clients	76
Manual Mac Client Installations	76
Deploying Client Installer Packages	76
Third-Party Tool Deployment	76
Basics	76
Syntax	76
Group Policy Deployment	77
Manual Client Installations	79
Basics	79
Framework Install	80
Full Disk Install	81

Chapter 6 Upgrades

Overview	83
Symantec Endpoint Encryption Management Server	83
Basics	83
From Versions that Utilize an SQL Database	84
Basics	84
Preliminary Steps For Multiple Management Servers	84
Single Management Server	84
Concluding Steps for Multiple Management Servers	86
From Versions that Utilize an ADAM Database	86
Basics	86
Prerequisites	87
Running the Key Exporter Script	87
Examples	88
Success	89
Verification	89
Symantec Endpoint Encryption Manager	89
Basics	89
Version Number Determination	90
Framework Upgrade	90
Full Disk Upgrade	90
One-Time Password Program Upgrade	91
From Symantec Endpoint Encryption Full Disk 8.0.0	91
From Symantec Endpoint Encryption Full Disk 7.0.8	91
From Symantec Endpoint Encryption Full Disk 7.0.7 and Earlier or any Version of GuardianEdge Hard Disk	91
Upgrading Windows Clients	92
About Upgrading Windows Clients	92
Upgrading Windows Clients Using a Third Party Tool	93
Basics	93
Syntax	93
Upgrading Windows Clients Using a GPO	94
Performing a Manual Upgrade of a Windows Client	96
Upgrading Mac Clients	96

Chapter 7 Encryption Plus Hard Disk Migration

Overview	99
Client Migration Package Preparation	99
Client Migration Package Deployment	100
Utility Analogs	100

Chapter 8	Uninstallation	
	Overview	101
	Symantec Endpoint Encryption Management Server	101
	Symantec Endpoint Encryption Manager Console	102
	Mac Client Computer	103
	Windows Client Computer	103
	Basics	103
	Third Party Tool	103
	Client Packages Deployed Using a GPO	103
	Manual	104
	Basics	104
	Encrypted Secondary Disk, Connected	104
	Encrypted Secondary Disk, Not Connected	105
	Recovery of Secondary Disk Post-Uninstallation	105
Appendix A	Management Server Configuration	
	Overview	107
	Configuration Manager	107
	Basics	107
	Database Configuration Tab	107
	Directory Sync Service Status	109
	Directory Sync Services Configuration	110
	Basics	110
	Active Directory Configuration Area	111
	Novell Configuration Area	112
	Policy Priority Settings Area	112
	Web Server Configuration	113
	Symantec Endpoint Encryption Management Server Clusters	114
	Basics	114
	Creating the Cluster	114
	Verifying Successful Cluster Failover	114
Appendix B	Extending Domain User Rights with DSACLS	
	Overview	117
	Prerequisites	117
	Summary of Steps	118
	Install ADAM Administrator Tools	118
	Grant List Children & Read Property Access Permissions	118
	Testing AD Synchronization	119
Appendix C	Certificates & Token Software Settings	
	Overview	121
	Symantec Endpoint Encryption Authentication Certificates	121
	Issuance from Windows Server 2003	121
	Single Certificate on Token	121
	Required Key Usage	122
	Required Extended Key Usage	122
	Required Token Software Configuration	122
	Recommended Token Software Configuration	123
	Basics	123
	ActivClient	123
	eToken PKI Client	123

Appendix D

Mapped Windows Domain Account Privileges

Overview 125

Prerequisites 125

Summary of Steps 125

Add Metabase Permissions 125

Add Other Permissions 126

Appendix E

Installation Settings Honored by Mac Clients

Appendix F

Taking Additional Drives Under Full Disk Management

About Taking Additional Drives Under Full Disk Management 129

Adding the Physical Disk Drive 130

Configuring the Logical Drives 130

Creating the Framework Client Upgrade Package 130

Creating the Full Disk Client Upgrade Package 130

Creating the Removable Storage Client Upgrade Package 131

Deploying the Client Upgrade Packages 131

Verifying That the Additional Drives Have Been Taken Under Management 131

Glossary 133

Index 137

Introduction

This chapter includes the following topics:

- [Overview](#)
- [Architecture](#)
- [System Requirements](#)
- [Symantec Endpoint Encryption Roles](#)

Overview

Symantec Endpoint Encryption Full Disk ensures that only authorized users can access data stored on hard disks. This safeguards enterprises from the accidental loss or theft of a laptop or computer and eliminates the legal need for public disclosure. Full Disk protects the following.

Table 1-1 Hard Disks and Other Storage That Full Disk Can Protect

Operating System	Primary Hard Drive	Secondary Hard Drive(s)	External Hard Drive(s)	eSATA Drive	Opal-Compliant Drive	Removable Storage	Solid State Drive(s)
Mac OS X	Y	Y	Y	N	N	Y	Y
Windows	Y	Y	N	N	Y*	N	Y

** Only a single Opal-compliant drive per computer. It must be configured as the primary, boot drive.*

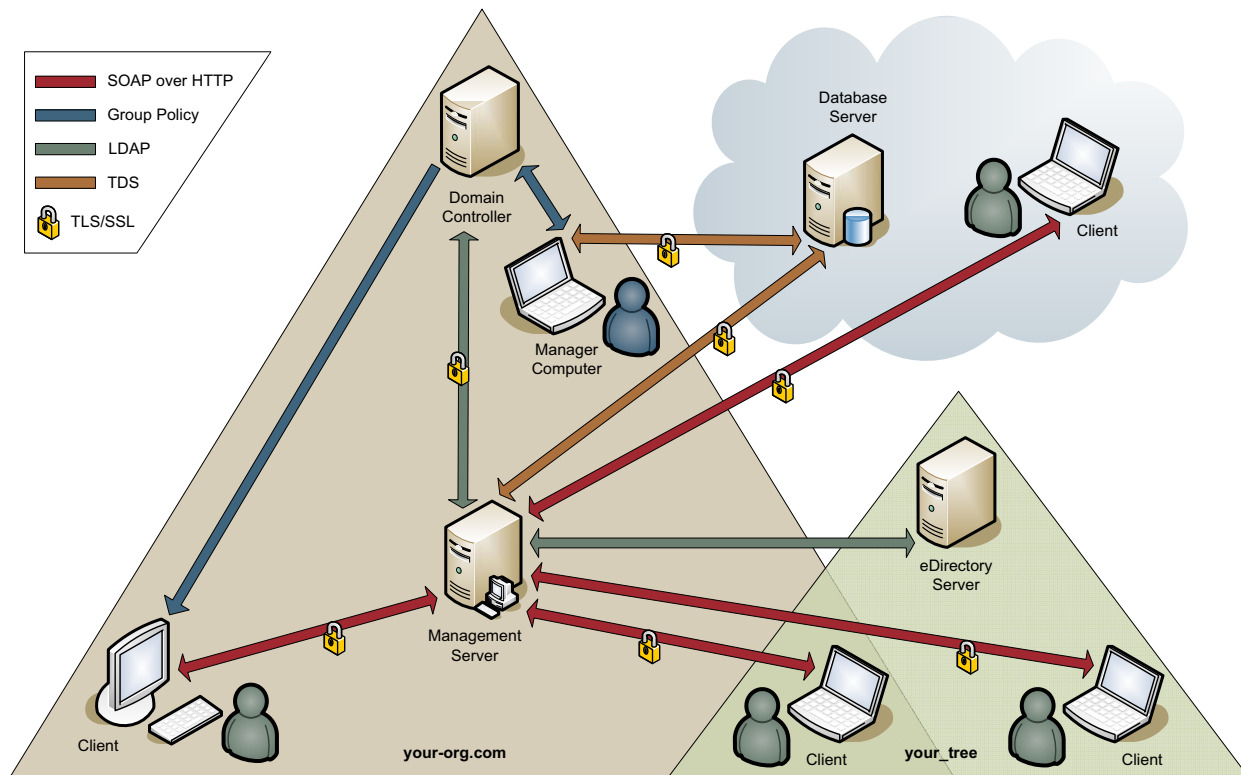
As part of Symantec Endpoint Encryption, Full Disk leverages existing IT infrastructures for seamless deployment and operation. This Guide is intended for use by the team of administrators responsible for provisioning and deploying the system.

Architecture

Basics

The following diagram illustrates a sample configuration of Symantec Endpoint Encryption.

Figure 1-1 Sample Network Configuration



The Active Directory domain controller and Management Server are required.

Multiple domains, forests, trees, and Management Servers are supported.

A database server is recommended, but the Symantec Endpoint Encryption database can also reside on a Microsoft SQL Server instance located on the Management Server. If a database server is chosen to host the Symantec Endpoint Encryption database, the database server can be located inside or outside of Active Directory.

The Manager Console can be installed on multiple Manager Computers. It can also be installed on the Management Server. It must reside on a computer that is a member of Active Directory.

The Novell eDirectory tree, Active Directory group policy communications, and TLS/SSL encryption are optional.

Installation Sequence

Symantec Endpoint Encryption must be installed in the following sequence:

- 1 Required account provisioning,
- 2 SQL Server instance,
- 3 Symantec Endpoint Encryption Management Server,
- 4 Symantec Endpoint Encryption Manager, and
- 5 Symantec Endpoint Encryption client.

Protocols and Ports

The following table identifies each protocol and port used.

Table 1-2 Protocols and Ports

Application Layer Protocol	Communication Protocol	Purpose(s)	Used by	Port
Group Policy Core Protocols	TCP/IP	Group Policy Object (GPOs)	Client Computers Manager Computers	445, 389
SOAP over Hypertext Transport Protocol (HTTP)	TCP/IP	Client-server communication	Client Computers Symantec Endpoint Encryption Management Server	configurable
Lightweight Directory Access Protocol (LDAP)	TCP/IP	Query Active Directory and eDirectory directories.	Symantec Endpoint Encryption Management Server	389, 3268, or configurable
Tabular Data Stream (TDS)	TCP/IP	Communications with the Symantec Endpoint Encryption database	Symantec Endpoint Encryption Management Server Symantec Endpoint Encryption database Manager Computers	1443, dynamically allocated, or configurable
Transport Layer Security (TLS) and/or Secure Sockets Layer (SSL)	TCP/IP	Optionally layered on top of TDS, LDAP, and/or HTTP to achieve encrypted communications	Symantec Endpoint Encryption Management Server Symantec Endpoint Encryption database Manager Computers Client Computers	636, 3269, or configurable

System Requirements

Basics

One or more Active Directory domains are required for hosting the Symantec Endpoint Encryption Management Server and Manager Computer(s).

Directory Service Integration

Symantec Endpoint Encryption supports synchronization with an Active Directory that has a domain functional level of Windows 2000 native or higher and a forest functional level of Windows 2000 or higher.

Symantec Endpoint Encryption supports synchronization with Novell eDirectory versions 8.7.3.7 and 8.7.3.9.

The Novell Single Sign-On and Novell directory service synchronization features will only be available for Windows clients installed with Novell Client 4.91 Service Pack 3 (SP3), Service Pack 4 (SP4), and/or Service Pack 5 (SP5).

Symantec Endpoint Encryption Management Server

The Symantec Endpoint Encryption Management Server can be installed on either a physical machine or a VMware ESXi 3.5 virtual machine.

Table 1-3 Symantec Endpoint Encryption Management Server Hardware Requirements

Component Type	Requirement
Processor	1.4 GHz Intel Pentium 4 or higher processor (or equivalent)
RAM	1 GB
Free disk space	80 MB

Table 1-4 Symantec Endpoint Encryption Management Server Software Requirements

Operating System	Edition(s)	Service Pack(s)	Additional Software
Windows Server 2003	Standard or Enterprise (32-bit x86 only)*	SP1 or SP2	Microsoft .NET Framework 2.0*, 3.0, or 3.5 Internet Information Services (IIS) 6.0
Windows Server 2003 R2	Standard or Enterprise (32-bit x86 only)*	SP2	
Windows Server 2008	Standard, Standard x64, Enterprise, or Enterprise x64	SP1 or SP2	—
Windows Server 2008 R2	Standard or Enterprise	SP1	—

* 64-bit Editions are not supported.

* .NET 2.0 is included with .NET 3.0 and 3.5

SQL Server Instance

The SQL Server instance hosting the Symantec Endpoint Encryption database can reside on a database server or on the Symantec Endpoint Encryption Management Server. If located on a database server, the database server does not need to belong to an Active Directory domain. For optimal performance, Symantec recommends storing the data file and log files on separate physical disks. The disk storing the log files must be formatted with the NTFS file system.

The Symantec Endpoint Encryption database can reside on either a physical machine or a VMware ESXi 3.5 virtual machine.

Table 1-5 SQL Server Instance Software Requirements

Product Version	Edition	Connection Type
Microsoft SQL Server 2005	Express with Advanced Services, Standard, or Enterprise (32-bit x86 only)*	Local and remote connections using either TCP/IP or TCP/IP and named pipes
Microsoft SQL Server 2008	Express with Advanced Services, Express with Advanced Services x64, Standard, Standard x64, Enterprise, or Enterprise x64	

* 64-bit Editions are not supported.

Manager Computer(s)

Each Manager Computer must be a member of an Active Directory forest/domain.

Table 1-6 Manager Computer Hardware Requirements

Component Type	Requirement
Processor	223 MHz or faster
RAM	512 MB or more recommended
Free disk space	80 MB

Table 1-7 Manager Computer Software Requirements

Operating System	Edition(s)	Service Pack(s)	Additional Software
Windows XP	Professional	SP2 or SP3	Group Policy Management Console with SP1 (GPMC.msi) Microsoft .NET Framework 2.0* Microsoft Management Console 3.0 Server 2003 Administration Tools Pack (adminpak.msi)
Windows Vista	Business, Business 64-Bit, Ultimate, Ultimate 64-Bit, Enterprise, or Enterprise 64-Bit	SP1 or SP2	Remote Server Administration Tools for Windows Vista
Windows 7	Professional, Professional x64, Ultimate, Ultimate x64, Enterprise, Enterprise x64	—	Remote Server Administration Tools for Windows 7
Windows Server 2003	Standard, Enterprise	SP1 or SP2	Group Policy Management Console with SP1 (GPMC.msi) Microsoft .NET Framework 2.0* Microsoft Management Console 3.0
Windows Server 2003 R2	Standard, Enterprise	SP2	Group Policy Management Console with SP1 (GPMC.msi) Microsoft .NET Framework 2.0* Microsoft Management Console 3.0
Windows Server 2008	Standard, Standard x64, Enterprise, or Enterprise x64	SP2	—
Windows Server 2008 R2	Standard or Enterprise	—	—

* .NET 2.0 is included with .NET 3.0 and 3.5

Mac Client Computers

Basics

Disks formatted using Apple Partition Map (APM) or the Unix File System (UFS) are not supported. Mac OS Extended (not journaled) file systems are not supported. RAID configurations are not supported. Dual-boot and multi-boot systems are not supported. BootCamp is not supported. Fast user switching is not supported. Safe Mode boots are not supported. Opal-compliant drives are not supported.

You must decrypt the disk before repartitioning, reformatting, or resizing any partitions.

Decrypt the disk before running any disk recovery applications, such as DiskWarrior from Alsoft.

Full Disk must be uninstalled before an upgrade to the operating system occurs.

Hardware Requirements

Table 1-8 Mac Client Computer Hardware Requirements

Component Type	Requirement	
RAM	512 MB or more recommended	
Free disk space	360 MB	
Keyboard*	English (US - International)	French (France)
	Japanese (Japan)	Spanish (Latin America)
	German (Germany)	Spanish (Spain; ISO)
* Users and Client Administrators will be unable to enter their credentials during pre-boot authentication with the thin aluminum Apple keyboards on a Mac mini.		

Software Requirements

Table 1-9 Mac Client Computer Software Requirements

Operating System
Apple Mac OS X 10.6.5 or later (Intel)

Windows Client Computers

BIOS

The system BIOS must support extended INT 13h. SCSI devices that do not use INT 13h to access the hard disk are not supported.

Changes to the NUMLOCK BIOS settings are not supported.

File System

The NTFS and FAT32 formats are supported.

Compatibility Notes

Note: Contact Symantec technical support before running CHKDSK on your Client Computers.

Note: Full Disk relies on its client database files and cannot protect them before Windows has loaded. Boot-time defragmentation programs will scramble the client database files and prevent the computer from booting.

Note: Full Disk relies on the Master Boot Record (MBR). System restore tools that replace the MBR, such as IBM Rescue and Recover, are not compatible with Full Disk and can cause serious problems if used.

Ensure that the hard drives of the Client Computers are not encrypted with any other full disk encryption software before deploying Full Disk.

DisplayPort connections are not supported.

Self-encrypting drives that don't conform to the Opal 1.0 standard are not supported. Samsung Opal-compliant drives are not supported. Opal-compliant drives will only be taken under management if they are configured as the primary boot drive. Secondary Opal-compliant drives won't be taken under management.

Note: Disable sleep mode on computers with Opal-compliant drives. Symantec does not support sleep mode with Opal-compliant drives.

Fast user switching is not supported. Roaming user profiles are not supported.

Section 508

Full Disk provides Section 508-compliant text-to-speech capability for its Windows user interface components when used with JAWS version 9.0.2152 or later.

Hardware Requirements

Table 1-10 Client Computer Hardware Requirements

Component Type	Requirement	
Processor	223 MHz or faster	
RAM	512 MB or more recommended	
Free disk space	360 MB	
Fixed disk(s)	2 TB or less	
Keyboard	Belgian (Period)	Japanese*
	Canadian French	Korean*
	Chinese (Simplified) - US Keyboard*	Latin American
	Chinese (Traditional) - US Keyboard*	Norwegian
		Portuguese (Brazil)
	Danish	Portuguese
	Dutch	Spanish
	Finnish	Swedish
	French	Swiss German
	German	Turkish Q*
	Hungarian*	United Kingdom
	Irish	US English
	Italian	

* Users will only be able to enter those characters that can also be typed from the US English keyboard.

* Only Latin-1 characters are supported.

Software Requirements

Once Full Disk has been installed, no changes to the partition table are supported. Before repartitioning, reformatting, or resizing any partitions on the Client Computer, you must first uninstall Full Disk.

Changes to the drive letters of encrypted disks and partitions are not supported.

Disks encrypted by Full Disk must be decrypted before they can be removed from one machine and inserted into another machine. Swapping of encrypted disks is not supported.

RAID configurations are not supported. Dual-boot and multi-boot systems are not supported.

Full Disk must be uninstalled before an upgrade to the operating system occurs. Moving from one Edition to another is considered an upgrade of the operating system. The application of a service pack is not considered an upgrade of the operating system.

Table 1-11 Windows Client Computer Software Requirements

Operating System	Edition(s)	Service Pack(s)	Additional Software
Windows 2000	Professional	SP4	Microsoft .NET Framework 2.0 Microsoft Internet Explorer 6.0 with SP2, 7, 8, or 9
Windows XP	Professional, Professional x64, or Tablet	SP1, SP2, or SP3	Microsoft .NET Framework 2.0 Microsoft Internet Explorer 6.0 with SP2, 7, 8, or 9
Windows Vista [†] *	Business, Business x64, Ultimate, Ultimate x64, Enterprise, or Enterprise x64 [*]	None, SP1, or SP2	Microsoft Internet Explorer 7, 8, or 9
Windows 7	Professional, Professional x64, Ultimate, Ultimate x64, Enterprise, or Enterprise x64	SP1	Microsoft Internet Explorer 8 or 9

** A keyboard is required for tablet PCs.*

[†] Windows Vista is only supported when run on Vista Capable hardware.

** SSO synchronization with the Novell Client is not supported on Windows Vista or Windows 7.*

Token Support

Table 1-12 Windows Client Computer Token Support

Data Model	Client Software for 32-bit Operating System [*]	Client Software for 64-bit Operating System [*]	Supported Tokens	Tested Tokens
Aladdin eToken	eToken PKI Client 5.1 SP1	eToken PKI Client 5.1 SP1	All with Aladdin eToken data model	Aladdin eToken NG-OTP 32K
				Aladdin eToken NG-OTP 64K
				Aladdin eToken PRO 32K
				Aladdin eToken PRO 64K
				Aladdin eToken PRO 72K (Java Card)
GSC-IS 2.1	Axalto Access Client 5.3***	Gemalto Access Client (x64) 5.5***	Axalto Cyberflex 64K v1	Axalto Cyberflex 64K v1
	Gemalto Access Client 5.5***		Axalto Cyberflex 64K v2c	Axalto Cyberflex 64K v2c
	Gemalto Access Client 5.6***		Cyberflex Access 64K v1 SM4.1	Cyberflex Access 64K v1 SM4.1

Table 1-12 Windows Client Computer Token Support (Continued)

Data Model	Client Software for 32-bit Operating System*	Client Software for 64-bit Operating System*	Supported Tokens	Tested Tokens
CACv2	ActivClient 6.1** ActivClient CAC 6.1 ActivClient 6.2 ActivClient CAC 6.2	ActivClient 6.2 ActivClient CAC 6.2	All with CACv2 data model†	Axalto Access 64K v2
				Axalto Access Cyberflex 64K v1 SM4.1
				Gemalto Cyberflex Access 64K v2c
				Gemplus GemXpresso 64K R3 FIPS V2#2
				Oberthur CosmopolIC 32K V4
				Oberthur CosmopolIC 64K v5.2 Fast ATR
				Oberthur CosmopolIC 64K v5.2 Fast ATR (dual)
				Schlumberger Access Cyberflex Access32K V2 SM7.2
CAC Next Generation (NG)	ActivClient 6.1** ActivClient 6.2	ActivClient 6.2	All with CAC NG data model (aka Transitional PIV)†	Oberthur CosmopolIC 64K v5.2 Fast ATR (dual)
				Oberthur CosmopolIC 72K v5.2 Fast ATR (dual)
				Gemalto TOPDLGX4 144K
				ID-One Cosmo 64 v5.2D Fast ATR with PIV application SDK
PIV I/ PIV II	ActivClient 6.1** ActivClient 6.2 VeriSign PKI Client v1.5.1***	ActivClient 6.2 VeriSign PKI Client v1.5.1***	All with PIV I/PIV II data model***	Athena IDProtect Duo PIV
				Gemalto SafesITe PIV TPC DM
				Oberthur ID-One Cosmo 64 v5.2D Fast ATR with PIV application SDK
				Oberthur ID-One 128K v5.5 (dual)
				Oberthur PIV End Point Dual Interface Smart Card
RSA	RSA Authentication Client 3.5**	RSA Authentication Client 3.5**	All with RSA data model	RSA SID800
				RSA Smart Card 5200**
SafeSign v2.1	SafeSign Identity Client v3.0.40	SafeSign Identity Client v3.0.40	HID Crescendo C700	HID Crescendo C700

* Single Sign-On is not supported with Windows 2000.

† Contactless authentication is not currently supported. Dual-interface cards must be inserted into a reader.

* Required for Windows activities such as registration, but not for pre-boot authentication.

** Apply FIXS0709005.

** If the token has been used with older versions of the token software, it may require conversion. Refer to RSA documentation for details.

** Must be installed before Framework is installed.

*** Refer to Appendix C "Required Token Software Configuration" on page 122 for mandatory components.

*** Only supported when used with USB CCID-compliant readers.

*** 128K cards are not supported with VeriSign PKI Client.

Table 1-13 Client Computer Token Reader Support

Type	Supported Readers	Tested Readers
Embedded	Argus 3015 USB 2.0 Dual Card Reader (Smart Card Reader slot)	Argus 3015 USB 2.0 Dual Card Reader (Smart Card Reader slot)
	Dell D410 (TI PCI 6515)	Dell D410 (TI PCI 6515)
	Dell D420 / D430 (O2Micro OZ776 USB CCID Smartcard Reader)	Dell D420 / D430 (O2Micro OZ776 USB CCID Smartcard Reader)
	Dell D600 (O2Micro OZ711EC1 PCMCIA/Smart Card Controller)	Dell D600 (O2Micro OZ711EC1 PCMCIA/Smart Card Controller)
	Dell D610 (TI PCI 6515)	Dell D610 (TI PCI 6515)
	Dell D620 (OZ6912 /601/711E0 CardBus/ SmartCardBus Controller)	Dell D620 (OZ6912 /601/711E0 CardBus/ SmartCardBus Controller)
	Dell D630 (O2Micro OZ711MP1/MS1 MemoryCardBus Controller)	Dell D630 (O2Micro OZ711MP1/MS1 MemoryCardBus Controller)
	Dell D820 (O2Micro OZ711EZ1 MemoryCardBus Controller)	Dell D820 (O2Micro OZ711EZ1 MemoryCardBus Controller)
	Dell E4200 (Broadcom Corp. 5880)	Dell E4200 (Broadcom Corp. 5880)
	Dell E4300 (Broadcom Corp. 5880)	Dell E4300 (Broadcom Corp. 5880)
	Dell E6400 (Broadcom Corp. 5880)	Dell E6400 (Broadcom Corp. 5880)
	Dell E6500 (Broadcom Corp. 5880)	Dell E6500 (Broadcom Corp. 5880)
	Dell M6400 (Broadcom Corp. 5880)	Dell M6400 (Broadcom Corp. 5880)
	Fujitsu 4210 (O2Micro OZ711MP1/MS1 MemoryCardBus Controller)	Fujitsu 4210 (O2Micro OZ711MP1/MS1 MemoryCardBus Controller)
	Fujitsu 4215 (O2Micro OZ711MP1/MS1 MemoryCardBus Controller)	Fujitsu 4215 (O2Micro OZ711MP1/MS1 MemoryCardBus Controller)
	RICOH SmartCard Reader	HP Compaq 6910p (RICOH SmartCard Reader)
ExpressCard	All CCID-compliant ExpressCard smart card readers	HP Compaq 8510p (RICOH SmartCard Reader)
		HP EliteBook 6930p (RICOH SmartCard Reader)
PCMCIA	Axalto Reflex 20 PCMCIA v2 & v3 ActivIdentity PCMCIA HP SCM SCR 243 PCMCIA SCM SCR 201 PCMCIA rev 1.3 SCM SCR 241 PCMCIA SCM SCR 243 PCMCIA	HP EliteBook 8730w (RICOH SmartCard Reader)
		SCM SCR3340 - ExpressCard54 Smart Card Reader
		Gemplus GemPC USB-SW
		Axalto Reflex 20 PCMCIA v2 & v3
		ActivIdentity PCMCIA
		HP SCM SCR 243 PCMCIA
		SCM SCR 201 PCMCIA rev 1.3
		SCM SCR 241 PCMCIA
		SCM SCR 243 PCMCIA

Table 1-13 Client Computer Token Reader Support (Continued)

Type	Supported Readers	Tested Readers
USB	All CCID-compliant USB smart card readers	ActivIdentity USB Reader 3.0
		Axalto Reflex USB v2
		Axalto Reflex USB v3
		Dell SK 3106 keyboard w/ SmartCard reader
		GemPC Express
		GemPC Pinpad*
		GemPC Twin
		OmniKey 3021
		OmniKey 3121
		SCM SCR3311 USB Reader
* Entering PIN with PIN pad is not supported; computer keyboard must be used.		

Refer to Appendix C “[Certificates & Token Software Settings](#)” on page 121 for required key usage settings for token certificates, as well as for required and recommended settings for the client token software.

Account Provisioning

Basics

The following tables list the accounts that must be provisioned prior to installation of the Symantec Endpoint Encryption Management Server, as well as accounts and groups that are optional to deployment.

Required Accounts

The following accounts are required.

Table 1-14 Required Accounts

Account	Description
Management Server account	If you plan to use SQL authentication with your SQL Server instance, no provisioning is required. The Management Server installer will create a SQL account for you with execute permissions to the Symantec Endpoint Encryption database catalog and assign it with the following database roles: db_datareader, db_datawriter, and public. The SQL account will be used by the Management Server for authentication to the database. The Management Server will use built-in accounts for the Symantec Endpoint Encryption Services website and synchronization service communications with the database.
	If you plan to use Windows authentication with your SQL Server instance, you must provision a Windows domain account prior to Management Server installation and perform the procedure outlined in Appendix D “ Mapped Windows Domain Account Privileges ” on page 125. The Management Server installer will map the Windows domain account to a SQL account that has execute permissions to the Symantec Endpoint Encryption database catalog and the following database roles: db_datareader, db_datawriter, and public. This account is used for configuring the Management Server. This account will also be used as a service account for the Symantec Endpoint Encryption Services website and as a log on account for the synchronization service communications with the database.

Table 1-14 Required Accounts (Continued)

Account	Description
Database creation account	Installing and configuring the Symantec Endpoint Encryption Management Server requires an account with Microsoft SQL Server dbcreator and securityadmin server roles. You can use either a Windows domain account or a SQL account. If you use a Windows account, it must have local administrator rights on the server hosting the Management Server. The credentials of this account are only used to authenticate to Microsoft SQL Server for the purposes of achieving the installation and configuration and are not stored or used again.
Database upgrade account	Upgrading the Symantec Endpoint Encryption Management Server requires an account with Microsoft SQL Server dbcreator and securityadmin server roles. This account must also have db_owner database role membership for the Symantec Endpoint Encryption database. The credentials of this account are only used to authenticate to Microsoft SQL Server for the purposes of achieving the upgrade and are not stored or used again.
IIS client account	Each Client Computer shares a single domain user account to authenticate to IIS on the Symantec Endpoint Encryption Management Server. No specific privileges are required for this account.
Policy Administrator account	Policy Administrators must be provisioned with read-write access to the Symantec Endpoint Encryption database. Either a Windows or an SQL account can be used. This account will allow the Policy Administrator to use the snap-ins of the Symantec Endpoint Encryption Manager. If you choose to use a Windows account for database access, a Policy Administrators group may ease administration. See “Optional Group” on page 12.

Synchronization Accounts

The following accounts are required to enable the optional synchronization feature.

Table 1-15 Synchronization Accounts

Account	Description
Active Directory synchronization account	To enable synchronization with Active Directory, a domain user account is required. The Active Directory synchronization service uses this account to bind to Active Directory. If the account does not have domain administrator privileges, you must extend the account privileges so that they include read permissions to the deleted objects container in Active Directory. One method of doing so is described in Appendix B “Extending Domain User Rights with DSACLs” on page 117.
eDirectory synchronization account	To enable synchronization with Novell eDirectory, an eDirectory account with read-only permissions to the eDirectory tree is required.

Optional Group

The following group may be used to ease the administration of Policy Administrator database accounts, if Windows authentication is chosen for this purpose. In order to create a domain groups, you will need an

account with create child permissions in Active Directory. Domain local groups can be assigned member permissions only within the same domain, but can contain accounts or groups from any domain.

Table 1-16 Optional Group

Account	Description
Policy Administrators group	An optional domain local group with read-write permissions to the Symantec Endpoint Encryption database. It is used for managing Policy Administrator accounts when Windows authentication to the database is used.

Symantec Endpoint Encryption Roles

Policy Administrator

Policy Administrators perform centralized administration of Symantec Endpoint Encryption. Using the Manager Console and the Manager Computer, the Policy Administrator:

- Updates and sets client policies.
- Issues commands to encrypt or decrypt endpoint drives and/or partitions.
- Runs reports.
- Changes the Management Password.
- Runs the Help Desk Program.
- Creates the computer-specific Recover DAT file necessary for Recover /B, Recover /O, and Recover /S.

Policy Administrators log on to their workstation using a Windows account. Access to the individual snapshots of the Symantec Endpoint Encryption Manager can be restricted by Windows privilege. The Policy Administrator will require access privileges to the Symantec Endpoint Encryption database (see [“Required Accounts”](#) on page 11). The Policy Administrator’s account privileges are maintained by Windows and Microsoft SQL Server; Symantec Endpoint Encryption does not manage these accounts.

Policy Administrators should be trusted in accordance with their assigned level of privilege.

Client Administrator

Basics

Client Administrators provide local support to Symantec Endpoint Encryption users.

Client Administrator accounts are created and maintained from the Symantec Endpoint Encryption Manager. Client Administrator accounts are managed entirely by Symantec Endpoint Encryption, independent of operating system or directory service, allowing Client Administrators to support a wide range of users.

Client Administrator passwords are managed from the Manager Console and cannot be changed at the Client Computer. This single-source password management allows Client Administrators to remember only one password as they move among many Client Computers.

Windows Client

Client Administrators may be configured to authenticate with either a password or a token.

Each Client Administrator account can be assigned any of the following individual administrative privileges:

- *Unregister users*—allows Client Administrators to unregister registered users from the Administrator Client Console;
- *Decrypt drives*—provides Client Administrators with the right to decrypt encrypted disks and partitions from the Administrator Client Console or through the use of Recover /D;
- *Extend lockout*—permits Client Administrators to extend the Client Computer's next communication date using the Administrator Client Console; and
- *Unlock*—enables Client Administrators to unlock Client Computers that have been locked for failure to communicate with the Symantec Endpoint Encryption Management Server.

Client Administrators are always able to authenticate to Client Computers and can always initiate encryption.

Client Administrators should be trusted in accordance with their assigned level of privilege.

Each Client Computer must have one default Client Administrator account. The default Client Administrator account has all administrative privileges and authenticates using a password. Only Client Administrators that authenticate with a password and have all administrative privileges can perform hard disk recovery. Up to 1024 total Client Administrator accounts can exist on each Client Computer.

Client Administrator accounts have the following restrictions:

- Client Administrators do not have either of the authentication assistance methods (Authenti-Check and One-Time Password) available.
- Client Administrators cannot use Single Sign-On.

Mac Client

Each Mac client has one Client Administrator account. The Client Administrator account will be created as specified within the client installation package or policy at the time that the encryption of the boot disk is manually initiated on the Mac endpoint. The Client Administrator account cannot be deleted by the user, ensuring administrative access to the Client Computer. The Client Administrator authenticates with a password. Privilege level will not affect the Client Administrator on the Mac client. The Client Administrator account cannot be used to initiate encryption.

User

Basics

Full Disk protects the data stored on the Client Computer by requiring valid credentials before allowing the operating system to load. Users set their Symantec Endpoint Encryption credentials, which allow them to power the machine on from an off state and gain access to the operating system. Only the credentials of registered users and Client Administrators will be accepted by Full Disk.

Mac Client

Upon manual initiation of encryption, a user account must be created. Up to 119 users can be added.

Windows Client

At least one user is required to register with Symantec Endpoint Encryption on each Client Computer. A wizard guides the user through the registration process, which involves a maximum of five screens. The registration process can also be configured to occur without user intervention.

Authentication to Full Disk can be configured to occur in one of three ways:

- *Single Sign-On enabled*—The user will be prompted to authenticate once each time they restart their computer.

- *Single Sign-On not enabled*—The user must log on twice: once to Full Disk and then separately to Windows.
- *Automatic authentication enabled*—The user is not prompted to provide credentials to Full Disk; the authentication process is transparent. This option relies on Windows to validate the user's credentials.

A maximum of 1024 users can be allowed during the creation of the installation package and can be changed by policy.

To ensure the success of this product in securing your encrypted assets, do not define users as local administrators or give users local administrative privileges.

Installing the Symantec Endpoint Encryption Management Server

This chapter includes the following topics:

- [Management Server Installation Overview](#)
- [Management Server Installation Prerequisites](#)
- [Required Additional Software/Required Features](#)
- [Management Server InstallShield Wizard](#)
- [Management Server Configuration Wizard](#)
- [Verification](#)
- [Back Up Symantec Endpoint Encryption Database](#)

Management Server Installation Overview

This chapter provides instructions for installing the Symantec Endpoint Encryption Management Server.

To install the Management Server

- 1 Comply with the following pre-requisites:
 - If you plan to encrypt client-server communications, you must install a server-side TLS/SSL certificate on the Management Server, and provide a client-side TLS/SSL certificate when prompted during installation of the Management Server ([“Management Server Installation Prerequisites”](#) on page 18).
 - If you plan to encrypt database-server communications, you must install a server-side TLS/SSL certificate on the server hosting the Symantec Endpoint Encryption database ([“Configuring Encrypted Database Communications”](#) on page 18).
 - If you plan to encrypt directory synchronization traffic, you must install a server-side TLS/SSL certificate on the domain controller ([“Configuring Encrypted Active Directory Synchronization Communications”](#) on page 19).
 - Install any additional software required by the Management Server, and enable required Windows features ([“Required Additional Software/Required Features”](#) on page 19).
- 2 Run the Management Server InstallShield Wizard ([“Management Server InstallShield Wizard”](#) on page 21).
- 3 Complete the Management Server Configuration Wizard ([“Management Server Configuration Wizard”](#) on page 27).
- 4 Reboot the Management Server.
- 5 Verify the success of the operation ([“Verification”](#) on page 32).

- 6 Back up the Symantec Endpoint Encryption database (“[Back Up Symantec Endpoint Encryption Database](#)” on page 34).

Management Server Installation Prerequisites

Configuring Encrypted Client Computer/Management Server Communications

To secure your communications between Client Computers and the Management Server using HTTPS (optional), you must install a server-side TLS/SSL certificate on the Management Server, and provide a client-side TLS/SSL certificate when prompted during installation of the Management Server.

Server-Side TLS/SSL Certificate Requirements

The server-side TLS/SSL certificate must be valid for IIS and must have the following characteristics:

- Valid during the period in which it will be used
- Enabled for server authentication
- Contains the private key
- Has a common name (CN) that matches the name of the Management Server exactly, as set in the **Web Server Name** box of the Configuration Wizard (“[Web Service Configuration](#)” on page 31) or the Configuration Manager (“[Web Server Configuration](#)” on page 113)
- Issued by the same certificate authority that issued the client-side TLS/SSL certificate
- Installed in the local computer personal certificate store of the Management Server

Note: If you plan to use HTTPS communication between Client Computers and one or more Management Servers configured in an NLB cluster, each cluster member must be installed with a server-side TLS/SSL certificate issued to the FQDN of the cluster. For information on how to configure and verify the correct operation of an NLB cluster of Management Servers, see Appendix A “[Symantec Endpoint Encryption Management Server Clusters](#)” on page 114.

Client-Side TLS/SSL Certificate Requirements

The client-side TLS/SSL certificate must have the following characteristics:

- Is in the .CER format
- Valid during the period in which it will be used
- Is the root certificate of the same certificate authority that issued the server-side TLS/SSL certificate

Configuring Encrypted Database Communications

To secure the database traffic between the SQL Server instance hosting the Symantec Endpoint Encryption database and the Management Server using TLS/SSL (optional), you must install a server-side TLS/SSL certificate on the server hosting the Symantec Endpoint Encryption database. This server-side TLS/SSL certificate must have the following characteristics:

- Valid during the period in which it will be used
- Enabled for server authentication
- Contains the private key
- Issued to the FQDN of the server hosting the Symantec Endpoint Encryption database if the server is a member of the domain.

Note: If the server hosting the Symantec Endpoint Encryption database is not a domain member, the TLS/SSL certificate must be issued to the NetBIOS name.

- Installed in the **Personal** certificate store of the computer hosting the Symantec Endpoint Encryption database

Note: You must enable SSL encryption and assign the TLS/SSL certificate on the server using the SQL Server Configuration Manager snap-in. Refer to the help system for Microsoft SQL Server, and/or the Microsoft knowledgebase article at the following URL: <http://support.microsoft.com/kb/316898>

Configuring Encrypted Active Directory Synchronization Communications

To secure the directory synchronization traffic between Active Directory and the Management Server using TLS/SSL (optional), you must install a server-side TLS/SSL certificate on the domain controller. This certificate must have the following characteristics:

- Valid during the period in which it will be used
- Enabled for server authentication
- Contains the private key
- Issued to the FQDN of the domain controller
- Installed in the **Personal** certificate store of the computer hosting the domain controller

Required Additional Software/Required Features

Basics

Before you begin, review the system requirements and ensure that the computer you are installing on is in compliance (see “[Symantec Endpoint Encryption Management Server](#)” on page 4). This section describes how to install the additional software and how to enable required operating system features. See the section that corresponds to the operating system of the Management Server.

- Windows Server 2003 (“[Windows Server 2003](#)” on page 19)
- Windows Server 2008 (“[Windows Server 2008](#)” on page 20)

Windows Server 2003

.NET Framework

.NET Framework 2.0 must be installed. It is included as part of .NET Framework 3.5.

If you do not already have .NET Framework installed:

- 1 Download version 3.5 from the Microsoft website at the following URL:
<http://www.microsoft.com/downloads/details.aspx?FamilyId=333325FD-AE52-4E35-B531-508D977D32A6&displaylang=en>
- 2 Double-click the dotNetFx35setup.exe file and follow the on screen instructions. On the final installation screen, click **Finish**.

Internet Information Server (IIS)

Internet Information Services (IIS) is a required component of the Management Server. It comes with Windows Server 2003, but the operating system can be installed without this component. This section describes how to add IIS to the Management Server, if the operating system was installed without it.

Note: If IIS is already installed, ensure that ASP.NET is enabled.

Installing IIS requires the Windows Server 2003 setup CD.

To install IIS:

- 1 Click **Start** to > **Programs > Administrative Tools**, then click **Configure Your Server Wizard**.
- 2 On the Welcome page of the wizard, click **Next**, then click **Next** again.
- 3 On the **Server Role** page, select **Application server (IIS, ASP.NET)**, and then click **Next**.
- 4 On the **Application Server Options** page, select **Enable ASP.NET**, and then click **Next**.
- 5 On the **Summary of Selections** page, click **Next**.
- 6 Insert the Windows Server 2003 setup CD when prompted, and then click **OK**.
- 7 On the **This Server is Now an Application server** page, click **Finish**.

Windows Server 2008

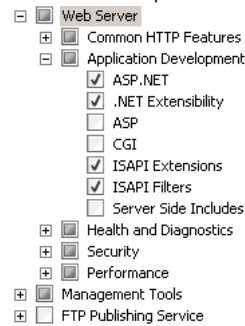
The Web Server (IIS) server role and required role services are included as part of Windows Server 2008.

To enable the server role and role services

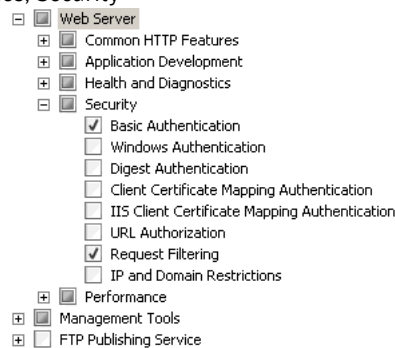
- 1 Click **Start**, then click **Server Manager**.
- 2 In the left pane of the Server Manager snap-in, right-click **Roles** and click **Add roles**.
- 3 On the welcome page of the **Add Roles Wizard**, click **Next**.
- 4 On the **Select Server Roles** page, select **Web Server (IIS)**.
- 5 On the **Add features required for Web Server (IIS)** dialog box, click **Add Required Features**, then click **Next**. Click **Next** again.

Note: Selecting the IIS role automatically selects additional role services required by IIS. In the following steps, ensure that you do not deselect any of these pre-selected check boxes.

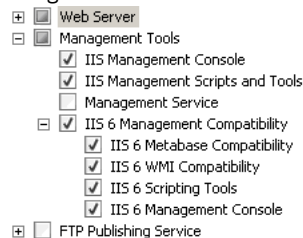
- 6 On the **Select Role Services** page, expand **Web Server > Application Development**, and select **ASP.NET**.
- 7 On the **Add role services and features required for ASP.NET** dialog box, click **Add Required Role Services**. Note that selecting this option causes **.NET Extensibility**, **ISAPI Extensions**, and **ISAPI Filters** also to be selected.

Figure 2-1 Select Role Services, Application Development

8 Expand **Security** and select **Basic Authentication**.

Figure 2-2 Select Role Services, Security

9 Expand **Management Tools**, then select **IIS Management Scripts and Tools** and **IIS 6 Management Compatibility**.

Figure 2-3 Select Role Services, Management Tools

10 Click **Next**, then click **Install**. When the Add Roles Wizard indicates that installation was successful, click **Close**. Choose **File**, and then click **Exit** to close the Server Manager snap-in.

Management Server InstallShield Wizard

Basics

Use the Management Server InstallShield Wizard to specify the initial settings of your Symantec Endpoint Encryption database and its communications. You can change these settings later using the Configuration Manager.

Initial Steps

To perform this procedure

- 1 Ensure that the server hosting the Symantec Endpoint Encryption database meets the minimum system requirements (Chapter 1 “[Software Requirements](#)” on page 6).
- 2 If your database creation account (Chapter 1 “[Required Accounts](#)” on page 11) is a Windows account, log on to the server hosting the Management Server using the database creation account.
If your database creation account is a SQL account, log on using a Windows domain account having local administrator rights on the Management Server.
- 3 Copy the Management Server installer (Symantec Endpoint Encryption Management Server.msi) to the local hard disk of the system on which you plan to install the Symantec Endpoint Encryption Management Server. Launch the installer using the method appropriate for the Management Server's operating system.
 - Windows Server 2008 or later—Click the **Start** button. Expand **Accessories**. Right-click **Command-prompt**. Select **Run as administrator**. Provide the credentials of a domain administrator account with sufficient rights for installing software at the prompt.
 - Windows Server 2003—Launch Symantec Endpoint Encryption Management Server.msi from the GUI or command line. To run the installer from the command line, click **Start > Run**, type **cmd**, then click **OK** to open a new command prompt window.
- 4 In the command prompt window, invoke the Windows Installer (msiexec.exe) by typing the following command-line parameters:
MSIEXEC /i "[path]\Symantec Endpoint Encryption Management Server.msi"

Note: Running the installer from the command line allows you to specify a output log file, which can be helpful for troubleshooting installation problems. To specify an output log file, add /lvx [logpath]\logfile to the end of the command line, where [logpath]\logfile is the path and name of the output log file that will be created.

- 5 On the **Welcome** page of the Management Server InstallShield Wizard, click **Next**.
- 6 Invoke the installer using one of the methods shown in “[Initial Steps](#)” on page 22.
- 7 The **License Agreement** page appears. Select the option **I accept the terms in the license agreement**, then click **Next**.

Database Location and Credentials

To specify the database location and credentials:

- 1 On the **Database Location and Credentials** page, specify the location of the Microsoft SQL Server instance that will host the Symantec Endpoint Encryption database and the database creation account credentials using one of the following methods: In the **Database Instance** box, do one of the following:
 - Click the arrow to open the list and select an instance that is local to your current computer.
 - Click **Browse** to select from a list of instances on the network.
 - Type the NetBIOS name of the instance, e.g., **SEEDB-01**. If it is a named instance, you must also include the name of the instance, e.g., **SEEDB-01\NAMEDINSTANCE**.

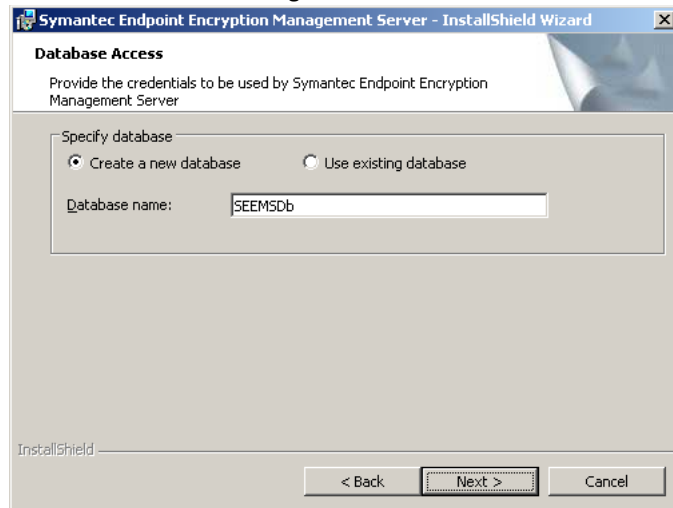
Note: Symantec Corporation recommends that you use a database server, but you can also install the Symantec Endpoint Encryption database locally on the Management Server, if a supported version of Microsoft SQL Server has been installed.

- 2 Click **Enable TLS/SSL** to encrypt all communications between the Management Server and the Symantec Endpoint Encryption database. Ensure that you are in compliance with the prerequisites (See [“Configuring Encrypted Database Communications”](#) on page 18).
- 3 Select **My database server operates on custom port number** if your database server has been configured to use a custom port. Selecting this option displays a port field. Type the custom port number.
- 4 Select **Windows authentication** option to use the Windows account you are currently logged on with as your database creation account (Chapter 1 [“Required Accounts”](#) on page 11), or select **SQL authentication** to manually specify the credentials of a SQL Server account that will serve as your database creation account. Click **Next**.

Database: New or Existing

After the installer succeeds in connecting to the instance, the **Database Access** page will appear.

Figure 2-4 Database Access, New or Existing Database



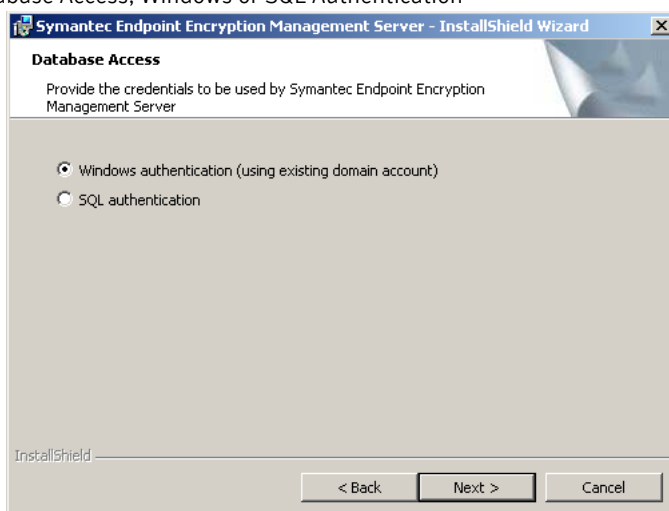
This page allows you to create a new database or use an existing one. If you are installing the Symantec Endpoint Encryption Management Server for the first time, use the default choice, **Create a new database**. Accept the default database name of SEEMSDb or type a unique custom name.

If you are reinstalling the Management Server and want to use an existing Symantec Endpoint Encryption database, choose **Use existing database**.

Management Server Account Type

Click **Next**. The **Database Access** page will appear.

Figure 2-5 Database Access, Windows or SQL Authentication

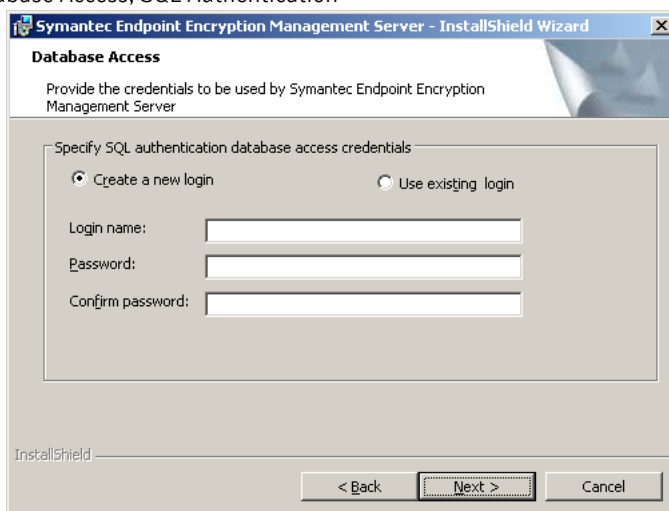


This page allows you to choose whether the Management Server account authenticates to the database using a SQL Server account or a mapped Windows domain account. Select **SQL authentication** to use SQL authentication. Click **Next** and continue to the next section. Select **Windows authentication (using existing domain account)** to use Windows authentication and skip to [“Management Server Account with Windows Authentication”](#) on page 25. Click **Next**.

Management Server Account with SQL Authentication

If you chose to use SQL authentication for the Management Server account, the following page will appear.

Figure 2-6 Database Access, SQL Authentication



If you are creating a new database, you can specify a new SQL account or use an existing SQL account.

If you are using an existing database, you must use an existing SQL account.

To specify a new SQL account, select **Create a new login** and type the user name, password, and password confirmation of the new account in the **Login name**, **Password**, and **Confirm password** boxes. This SQL Server account is used solely for communication between the Management Server and the Symantec Endpoint Encryption database. The SQL Management Server account has execute permissions to the Symantec Endpoint Encryption database catalog and has the following database roles: db_datareader, db_datawriter, and public.

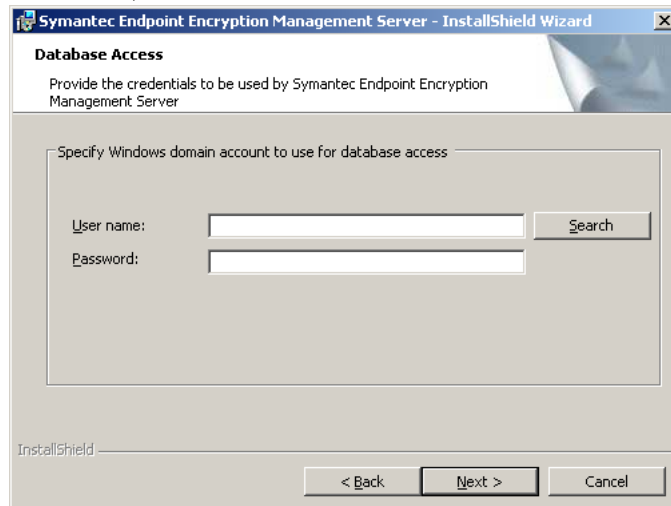
To use an existing SQL account, select **use existing login**. The **Confirm Password** box will be removed. In the **Login name** and **Password** boxes, type the credentials of the database communications account you created during a previous installation.

Click **Next**, then skip to [“Concluding Steps”](#) on page 25.

Management Server Account with Windows Authentication

If you chose to use Windows authentication with the Management Server account, the following page will appear.

Figure 2-7 Database Access, Windows Authentication



To specify the Management Server account on Windows Server 2003 or Windows Server 2008, type the account name in NetBIOS format in the **User name** box. Type the password for the selected account in the **Password** box.

If you are installing on Windows Server 2003, you can alternately select the domain and account from a list. Click **Search**. The **Browse for a user account** window opens. Click **Browse** next to the **Domain or server** box. The **Select a Domain or Server** window opens. Select a domain from the list and click **OK**. Click **Browse** next to the **User name** box. The **Select a User Name** window opens. Select a user account from the list and click **OK**.

The Management Server account is used for communication between the Management Server and the Symantec Endpoint Encryption database, as a service account for the Symantec Endpoint Encryption Services web site, and as a log on account for the synchronization services. The Windows Management Server account has membership in the IIS_WPG group, "log on as a batch job" permission, and permissions to the IIS metabase and file system. The installer will apply the required database permissions and roles to the mapped Windows domain account during installation.

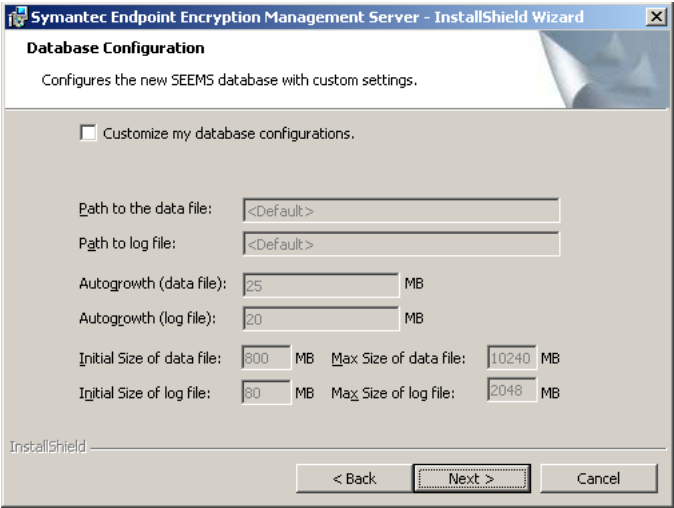
Click **Next**.

The installer will validate the selected account. An alert will be displayed if the selected account exists. Click **Yes** to use the selected account.

Concluding Steps

If you chose to use an existing database, skip to [“Database: New or Existing”](#) on page 23. If you chose to create a new database, the **Database Configuration** page will appear.

Figure 2-8 Database Configuration



Leave the **Customize my database configurations** check box deselected to accept the database configuration default values (recommended).

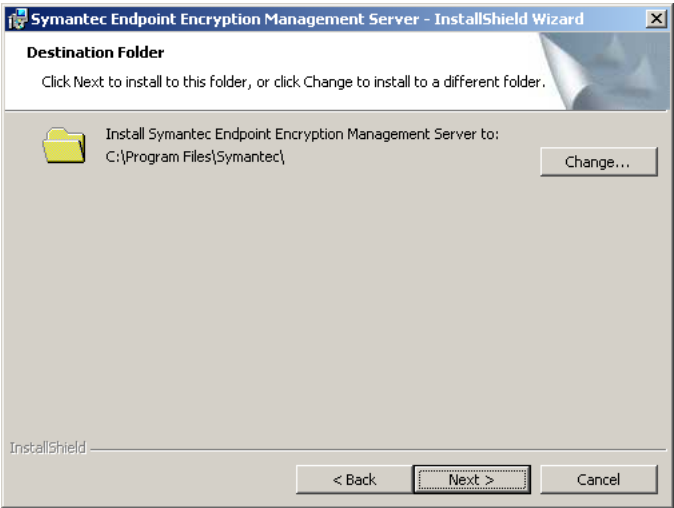
To specify your own configuration settings, select the **Customize my database configurations** check box. Type the paths to the data file and the log file. Note that the directories in this path must already exist on the server hosting the Symantec Endpoint Encryption database and will not be created by the installer. Type file size values in megabytes for the data and log files (autogrowth size, initial size, and maximum size).

Note: The database configuration settings can be changed later using the Microsoft SQL Server tool of your choice. The Symantec Endpoint Encryption Configuration Manager is not used for this purpose. However, the size settings can only be increased, not decreased. In addition, changing the paths will require detaching and reattaching the Symantec Endpoint Encryption database.

Note: Ensure that the server hosting the Symantec Endpoint Encryption database has sufficient space for the data and log files.

Click **Next**. The **Destination Folder** page will appear.

Figure 2-9 Destination Folder

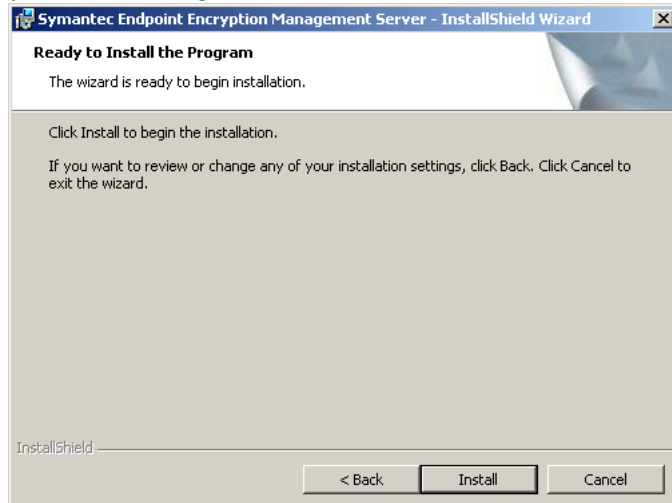


This page allows you to change the destination of the Management Server files.

Click **Change** to choose a different location to install the Management Server files, or click **Next** to accept the default installation location.

The **Ready to Install the Program** page appears.

Figure 2-10 Ready to Install the Program



Click **Install**.

After the **Symantec Endpoint Encryption Management Server InstallShield Wizard Completed** page appears, click **Finish**. The Management Server Configuration Wizard will launch.

Management Server Configuration Wizard

Basics

The Management Server Configuration Wizard will launch automatically once the InstallShield Wizard has completed its execution. You can dismiss the wizard by clicking **Cancel**. You can resume the wizard by launching `Symantec.Endpoint.Encryption.ConfigManager.exe`, located in `C:\Program Files\Symantec\Symantec Endpoint Encryption Management Server\Services`.

Note: Until you complete the Symantec Endpoint Encryption Management Server Configuration Manager, you won't be able to synchronize with your directory service(s) or create client installation packages.

All of the settings in the wizard can be changed later using the Configuration Manager (Chapter A [“Management Server Configuration”](#) on page 107).

Directory Service Synchronization Options

Basics

The Management Server Configuration Wizard will launch with its first page displayed, **Directory Service Synchronization Options**.

Figure 2-11 Configuration Wizard, Directory Service Synchronization Options

The screenshot shows the 'SEEMS Configuration Wizard' window with the title 'Directory Service Synchronization Options'. Below the title is the instruction 'Choose directory service synchronization options.' The dialog contains two sections for selecting directory services. The first section, 'Microsoft Active Directory', has a checked checkbox, a 'Startup Mode' dropdown set to 'Automatic', and a 'Sync Mode' dropdown set to 'Primary'. The second section, 'Novell eDirectory', also has a checked checkbox, a 'Startup Mode' dropdown set to 'Automatic', and a 'Sync Mode' dropdown set to 'Primary'. At the bottom, there is a note: 'If an endpoint is managed by both Active Directory and eDirectory, specify which has precedence in policy definitions.' Below this note are two radio buttons: 'Microsoft Active Directory' (which is selected) and 'Novell eDirectory'. At the very bottom are three buttons: 'Prev', 'Next' (which is highlighted with a dashed border), and 'Cancel'.

This page allows you to select the directory services with which the Symantec Endpoint Encryption database will be synchronized. The Management Server ensures that the Symantec Endpoint Encryption database remains up to date with information from these directory services. For example, when computer or container objects are added to or deleted from Active Directory and/or eDirectory, directory service synchronization propagates those changes to the Symantec Endpoint Encryption database. This allows you to use the Symantec Endpoint Encryption Manager to view and apply Symantec Endpoint Encryption native policies to the computers in your organization according to the directory OUs or containers in which they reside.

Select the **Microsoft Active Directory** and/or **Novell eDirectory** check boxes to allow synchronization with the respective directory service.

The **Startup Mode** list boxes, along with the **Sync Mode** list boxes, establish synchronization priority among multiple Management Servers. If you are planning to deploy an NLB cluster of multiple Management Servers to provide hot failover capability (see Appendix A “[Symantec Endpoint Encryption Management Server Clusters](#)” on page 114), you will need to designate one Management Server as the primary synchronizer, and all other Management Servers as secondary synchronizers. If you only have one Management Server and you select the **Microsoft Active Directory** and/or **Novell eDirectory** check boxes, it will automatically synchronize with the respective directory service(s) regardless of whether you’ve configured it to act as a primary or secondary synchronizer.

To configure this Management Server to act as a primary synchronizer for Active Directory, select the **Microsoft Active Directory** check box, and choose **Automatic** from the **Startup Mode** list box.

To configure this Management Server to act as a secondary synchronizer for Active Directory, select the **Microsoft Active Directory** check box, and choose **Automatic** from the **Startup Mode** list to run the service automatically at boot time. Choose **Manual** if you don’t want the service to automatically run and begin synchronization at boot time.

To configure this Management Server to act as a primary synchronizer for eDirectory, select the **Novell eDirectory** check box, and choose **Automatic** from the **Startup Mode** list box.

To configure this Management Server to act as a secondary synchronizer for eDirectory, select the **Novell eDirectory** check box, and choose **Automatic** from the **Startup Mode** list to run the service automatically at boot time. Choose **Manual** if you don't want the service to automatically run and begin synchronization at boot time.

When you select both the **Microsoft Active Directory** and the **Novell eDirectory** check boxes, the policy precedence option will be displayed. When Active Directory and eDirectory are both present, a Client Computer can potentially be a member of both, thus receiving two sets of potentially conflicting Symantec Endpoint Encryption policies. To mitigate potential policy conflicts, you must choose the directory service whose policies will have priority. Select either Microsoft Active Directory or Novell eDirectory. Click **Next**.

Directory Service Synchronization Configuration

If you selected either the **Microsoft Active Directory** check box and/or the **Novell eDirectory** check box in the Directory Service Synchronization Options page, the **Directory Service Synchronization Configuration** page will appear. Otherwise, skip to [“Web Service Configuration”](#) on page 31.

Figure 2-12 Configuration Wizard, Directory Service Synchronization Configuration

SEEMS Configuration Wizard

Directory Service Synchronization Configuration

Provide the directory configuration details.

Active Directory Configuration 1/1 AD Forest

Active Directory Forest Name: your-org.com

Preferred Global Catalog Server: cadc-01.your-org.com

Active Directory User Name: adsyncuser

Password: [masked] Confirm Password: [masked]

User Domain: your-org.com

☐ Enable TLS/SSL

Configure Domain Filter Delete Prev Add

Novell Configuration

Novell Tree Name: [text box]

LDAP Host Server IP: [text box] LDAP Port: [text box]

User Distinguished Name: [text box]

Password: [text box] Confirm Password: [text box]

Delete Prev Add

Prev Next Cancel

Active Directory Configuration Area

If you selected the **Microsoft Active Directory** check box on the Directory Service Synchronization Options page, the **Active Directory Configuration** area will be available.

In the **Active Directory Forest Name** box, type the name of the specified forest.

In the **Preferred Global Catalog Server** box, type the FQDN of a global catalog server of the specified forest.

In the **Active Directory User Name**, **Password**, and **Confirm Password** boxes, type the credentials of the Active Directory synchronization account ([“Synchronization Accounts”](#) on page 12).

In the **User Domain** box, type the NetBIOS name of the Active Directory synchronization account.

To synchronize with additional Active Directory forests, click **Add**. The status text above the right side of the **Active Directory Forest Name** field will update to display **2/2 AD Forest**, indicating that the

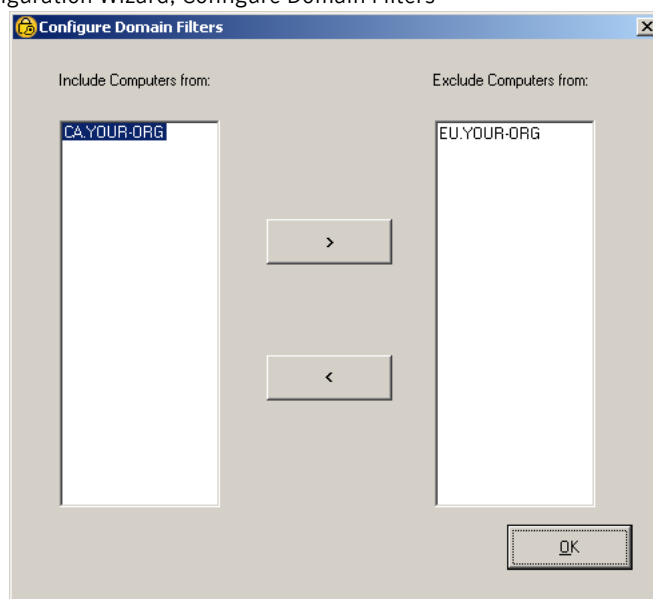
configuration settings for the second of a total of two forests are currently displayed. Type the configuration information for the new forest.

Click **Delete** to remove the configuration information for the currently displayed forest, or click **Prev** to view the configuration information for the previous forest.

Domain filtering allows you to exclude specific Active Directory domains from synchronization while including others. For example, there may be domains within your forest(s) that do not contain Symantec Endpoint Encryption Client Computers. To improve performance and usability, you can exclude these domains from being synchronized.

To use the domain filter, click **Configure Domain Filter**.

Figure 2-13 Configuration Wizard, Configure Domain Filters



In the **Include Computers from** column on the left, select a domain you wish to exclude, then click > to move the domain into the **Exclude Computers from** column on the right. Moving a parent domain from the **Include Computers from** column to the **Exclude Computers from** column will also move all child domains of that parent domain. In a typical deployment, you would exclude the top level of a domain, then include only those child domains containing Symantec Endpoint Encryption Client Computers. Click **OK** when finished.

Select the **Enable TLS/SSL** check box to encrypt all synchronization traffic between Active Directory and the Symantec Endpoint Encryption Management Server. Ensure that you are in compliance with the prerequisites ("[Configuring Encrypted Active Directory Synchronization Communications](#)" on page 19).

Novell Configuration Area

If you selected the **Novell eDirectory** check box on the Directory Service Synchronization Options page, the **Novell Configuration** area will be available.

In the **Novell Tree Name** box, type the name of the specified tree.

In the **LDAP Host Server IP** and **LDAP Port** boxes, type the IP and port of the eDirectory host for the specified tree.

Optionally, you can provide the distinguished name (DN) and password of the Novell synchronization account in the **User Distinguished Name**, **Password**, and **Confirm Password** boxes.

To synchronize with additional eDirectory trees, click **Add**. The status text above the right side of the **Novell Tree Name** field will update to display **2/2 Novell Tree**, indicating that the configuration settings for

the second of a total of two trees are currently displayed. Type the configuration information for the new tree.

Click **Delete** to remove the configuration information for the currently displayed tree, or click **Prev** to view the configuration information for the previous tree.

Page Completed

Click **Next**. After the information you entered has been successfully validated, the **Web Service Configuration** page appears.

Web Service Configuration

The **Web Service Configuration** page is used to set the protocol and/or port used for communications between the Client Computers and the Management Server.

Figure 2-14 Configuration Wizard, Web Service Configuration

The screenshot shows the 'Web Service Configuration' window of the SEEMS Configuration Wizard. The window title is 'SEEMS Configuration Wizard'. The main heading is 'Web Service Configuration' with the subtitle 'Set the configuration data to be used for client-server communications.' The form contains several sections: 'Web Server Name' with a text box containing 'seems-01'; 'IIS Client Account Credentials' with fields for 'Account Name' (administrator), 'Password' (empty), and 'Domain' (your-org.com); 'Protocol' with radio buttons for 'HTTP' and 'HTTPS' (selected), and corresponding 'HTTP Port' (1001) and 'HTTPS Port' (1002) text boxes; and 'Client Computer Communications' with 'Client-Side TLS/SSL Certificate' and 'Server-Side TLS/SSL Certificate' sections, each featuring a 'Browse' button and a 'Certificate Hash' label followed by a long alphanumeric string. At the bottom are 'Prev', 'Finish' (highlighted), and 'Cancel' buttons.

The **Web Server Name** box will be prefilled with the NetBIOS name of the computer hosting the Management Server. You should modify the entry to FQDN if:

- DNS configuration issues prevent the NetBIOS name from resolving and an FQDN is more appropriate to your network environment.
- You will use an NLB cluster of Management Servers. You must edit this value on each cluster member so that it contains the FQDN of the cluster. See [“Symantec Endpoint Encryption Management Server Clusters”](#) on page 114.

Note: If you intend to use HTTPS communication between Client Computers and the Management Server, this name must match the common name (CN) specified in the server-side TLS/SSL certificate exactly. Refer to [“Server-Side TLS/SSL Certificate Requirements”](#) on page 18.

In the **Account Name**, **Password**, and **Domain** boxes, type the credentials and domain of the IIS client account (“[Required Accounts](#)” on page 11). Leave the **HTTP** option selected if you do not wish to encrypt client communications with the Management Server.

Select the **HTTPS** option to encrypt these communications. An **HTTPS Port** field will be displayed, along with the **Client Computer Communications** area.

Type the number of the TCP port on the Management Server that should be used for the unencrypted client communications in the **HTTP Port** box. A TCP port for unencrypted communications will be required even if the HTTPS option is selected. IIS requires this information, but Symantec Endpoint Encryption will not use this port. If you selected the HTTPS option, type the TCP port on the Management Server that should be used for the encrypted client communications in the **HTTPS Port** box.

To select the client-side TLS/SSL certificate Symantec Endpoint Encryption client computers use for encrypted communication with the Management Server, click the **Browse** button adjacent to **Client-Side TLS/SSL Certificate**. A **Choose SSL certificate file** dialog will be displayed, listing the certificates available in the personal certificate store of the local computer (i.e., the Management Server). Navigate to the location of a CER file suitable for use as a client-side TLS/SSL certificate, then click **Open**. The certificate hash string will be displayed below the **Browse** button.

To select or change the server-side TLS/SSL certificate the web service of the Symantec Endpoint Encryption Management Server uses for encrypted communication with Symantec Endpoint Encryption client computers, click the **Browse** button adjacent to the text **Server-Side TLS/SSL Certificate**. The **Certificate selection** dialog will display a list of certificates found in the local certificate store. Select a certificate suitable for use as a server-side TLS/SSL certificate, then click **OK**. The certificate hash string will be displayed below the **Browse** button.

Note: Selecting the server-side TLS/SSL certificate in the Configuration Manager is equivalent to assigning the server-side TLS/SSL certificate to the Symantec Endpoint Encryption Services website using the IIS Manager snap-in.

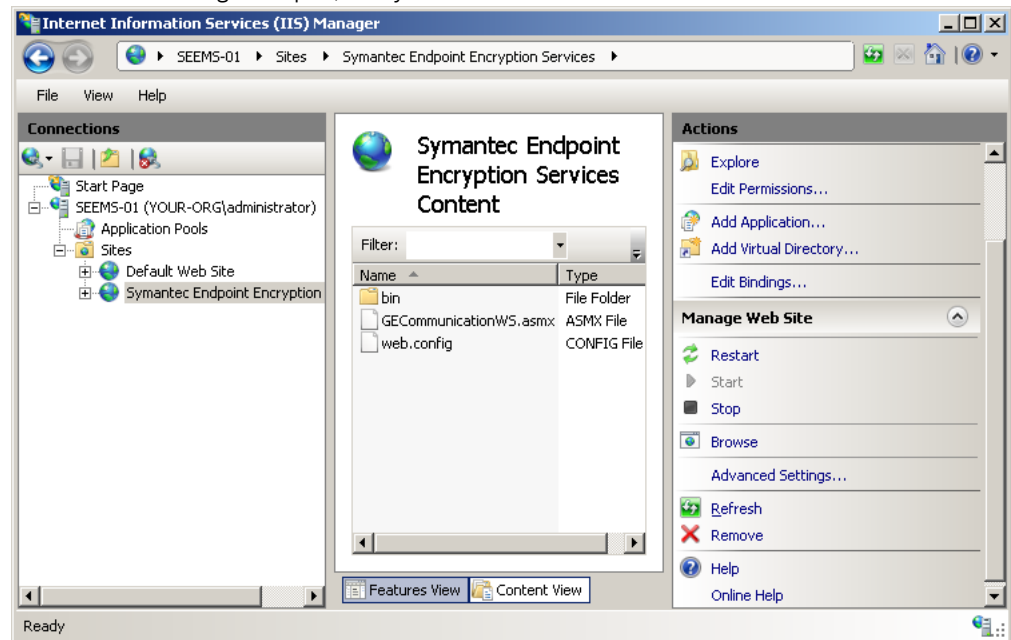
Click **Finish**. You will be prompted to restart the Management Server. A restart is required to complete the installation. Click **Restart** when prompted.

Verification

Symantec Endpoint Encryption Management Server

To verify correct installation of the Management Server, perform the following steps:

- 1 Open the **Internet Information Service (IIS) Manager** snap-in. Expand the Symantec Endpoint Encryption Management Server computer. For Windows Server 2003, expand and select **Web Sites**. For Windows Server 2008, expand **Sites**, then right-click **Symantec Endpoint Encryption Services** and choose **Switch to Content View**.

Figure 2-15 IIS Manager Snap-in, Verify Installation on Windows Server 2008

- 2 Verify that the **Symantec Endpoint Encryption Services** website is listed and that it is started. If the website is stopped, it indicates that a port number that you specified for communications with the Client Computers is already in use. See Appendix A “[Web Server Configuration](#)” on page 113 for instructions on using the Configuration Manager to change the port number(s).
- 3 Click on **Symantec Endpoint Encryption Services**, and verify that the right-hand pane contains the following three items:
 - The bin subfolder,
 - The GECCommunicationWS.asmx file, and
 - The web.config file.
- 4 For Windows Server 2003, highlight **Web Service Extensions**. Check to make sure that ASP.NET v2.0.50727 is listed in the right-hand panel with a status of **Allowed**.
- 5 Open the Event Viewer snap-in and examine the Application event log to verify that there are no errors generated by the event sources ADSyncService or NovellSyncService.

If you ran the MSI from the command line and enabled logging, each step of the installation process will be logged in the file and at the location specified from the command line prompt. If no path was specified, then the files will be stored in the working directory that was current at the time that the command was issued from the command line prompt.

Symantec Endpoint Encryption Database

Access the Symantec Endpoint Encryption database using the Microsoft SQL Server Management Studio (part of an optional install of tools for SQL Server 2005) using administrator-level privileges, and verify the following:

- A new database has been created using either the name you specified or the default name, SEEMSDb.
- The Management Server account you specified in the Management Server InstallShield wizard has been added as a user of the new database.
- The new database has been populated with Symantec Endpoint Encryption–specific tables, for example, dbo.GEMSEventLog.
- If you selected eDirectory synchronization, the contents of the dbo.NovellContainers database table reflect the container structure of your eDirectory.

- Check the Windows System Event Viewer on the computer hosting the Symantec Endpoint Encryption database. Events related to the creation of the Symantec Endpoint Encryption database will be logged in the Application category with the source MSSQLSERVER. Ensure that no error messages were generated.

Back Up Symantec Endpoint Encryption Database

Once the Management Server has been installed and its operation verified, it is critical to now perform a complete backup of the Symantec Endpoint Encryption database you just created.

Furthermore, consult with personnel from your enterprise backup group to arrange for regular backups of the Symantec Endpoint Encryption database.

Installing the Symantec Endpoint Encryption Manager Console

This chapter includes the following topics:

- [Installation Overview](#)
- [Prepare for Encrypted Client Computer Communications](#)
- [Additional Software/Required Features](#)
- [Manager Console Installation](#)
- [Manager Console Snap-In Access Control](#)

Installation Overview

You can install the Symantec Endpoint Encryption Manager Console on one or more computers, which are then known as Manager Computers.

Before You Begin

- If you plan to encrypt the communication between the Client Computer and the Management Server, ensure that each Manager Computer meets the prerequisites (see [“Prepare for Encrypted Client Computer Communications”](#) on page 35).
- Ensure that each Manager Computer meets the minimum system requirements.
- Install additional software as per system requirements and enable required features (see [“Additional Software/Required Features”](#) on page 36).
- Determine whether the Manager Computer is running a 32-bit edition of Windows or a 64-bit edition of Windows, then run the compatible Manager Console setup packages (see [“Manager Console Installation”](#) on page 39).

Prepare for Encrypted Client Computer Communications

If you plan to use HTTPS communication between Client Computers and the Management Server, you must install, on each Manager Computer, the same client-side TLS/SSL certificate that you specified during installation of the Management Server (see Chapter 2 [“Configuring Encrypted Client Computer/Management Server Communications”](#) on page 18). This client-side TLS/SSL certificate must be installed in the local computer Trusted Root Certification Authorities certificate store on each Manager Computer.

Additional Software/Required Features

Before You Begin

Review the system requirements and ensure that the computer you are installing on is in compliance (see Chapter 1 “Symantec Endpoint Encryption Management Server” on page 4).

This section describes how to install the additional software and how to enable required operating system features. Refer to the section that corresponds to the operating system of the Manager Computer.

- Windows XP (“Windows XP” on page 36);
- Windows Vista (“Windows Vista” on page 37);
- Windows 7 (“Windows 7” on page 37).
- Windows Server 2003 (“Windows Server 2003” on page 38); or
- Windows Server 2008 and Windows Server 2008 R2 (“Windows Server 2008 and Windows Server 2008 R2” on page 38).

Windows XP

Group Policy Management Console

If the target computer is missing the Group Policy Management Console, this section provides instructions to obtain and install this software. The Microsoft Group Policy Management Console with Service Pack 1 (Gpmc.msi) may be downloaded from the Microsoft website at the following URL if it is not already installed:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=0a6d4c24-8cbd-4b35-9272-dd3cbfc81887&DisplayLang=en>

To install the Group Policy Management Console snap-in, double-click the gpmc.msi file and follow the on screen instructions. On the final installation screen, click **Finish**.

.NET Framework

.NET Framework 2.0 is required. It is included as part of .NET Framework 3.5. If you do not already have .NET Framework installed, version 3.5 may be downloaded from the Microsoft website at the following URL:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=333325FD-AE52-4E35-B531-508D977D32A6&displaylang=en>

To install .NET Framework 3.5, double-click the dotNetFx35setup.exe file and follow the on screen instructions. On the final installation screen, click **Finish**.

Microsoft Management Console 3.0

The Microsoft Management Console 3.0 may be downloaded from the Microsoft website at the following URL if it is not already installed:

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=61fc1c66-06f2-463c-82a2-cf20902ffae0>

To install Microsoft Management Console 3.0, double-click the WindowsXP-KB907265-x86-ENU.exe file and follow the on screen instructions. On the final installation screen, click **Finish**.

Windows Server 2003 Administration Tools Pack

The Windows Server 2003 Administration Tools Pack may be downloaded from the Microsoft website at the following URL if it not already installed:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=c16ae515-c8f4-47ef-a1e4-a8dcbaeff8e3&DisplayLang=en>

To install the Windows Server 2003 Administration Tools Pack, double-click the adminpak.msi file and follow the on-screen instructions. On the final installation screen, click **Finish**.

Windows Vista

Remote Server Administration Tools for Windows Vista

You will need to download either the 32-bit or 64-bit version of the Microsoft Remote Server Administration Tools appropriate to the edition of Windows Vista you are running.

The 32-bit version of Microsoft Remote Server Administration Tools for Windows Vista may be downloaded from the Microsoft website at the following URL:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=9FF6E897-23CE-4A36-B7FC-D52065DE9960&displaylang=en>

The 64-bit version of Microsoft Remote Server Administration Tools for Windows Vista may be downloaded from the Microsoft website at the following URL:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=D647A60B-63FD-4AC5-9243-BD3C497D2BC5&displaylang=en>

If the operating system is 32 bits, launch the Windows6.0-KB941314-x86_en-US.msu file. If the operating system is 64 bits, launch the Windows6.0-KB941314-x64_en-US.msu file. On the final installation screen, click **Close**.

You must now enable specific components to make the Active Directory Users and Computers and Group Policy Management snap-ins available to the Manager Console.

To perform this procedure

- 1 Click **Start**, point to **Control Panel**, and click **Programs**.
- 2 Under **Programs and Features**, click **Turn Windows Features on or off**. The Windows Features window appears.
- 3 Expand **Remote Server Administration Tools**, expand **Feature Administration Tools**, and select the **Group Policy Management Tools** check box.
- 4 Under **Remote Server Administration Tools**, expand **Role Administration Tools**, expand **Active Directory Domain Services Tools**, and select the **Active Directory Domain Controller Tools** check box.
- 5 Click **OK**.

Windows 7

You will need to download either the 32-bit or 64-bit version of the Microsoft Remote Server Administration Tools appropriate to the edition of Windows 7 you are running. Both the 32- and 64-bit versions of the Microsoft Remote Server Administration Tools for Windows 7 may be downloaded from the Microsoft website at the following URL:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=7D2F6AD7-656B-4313-A005-4E344E43997D&displaylang=en>

If the operating system is 32 bits, launch the x86fre_GRMRSAT_MSU.msu file. If the operating system is 64 bits, launch the amd64fre_GRMRSATX_MSU.msu file. On the final installation screen, click **Close**.

Windows Server 2003

Group Policy Management Console

If the target computer is missing the Group Policy Management Console, this section provides instructions to obtain and install this software. The Microsoft Group Policy Management Console with Service Pack 1 (Gpmc.msi) may be downloaded from the Microsoft website at the following URL if it is not already installed:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=0a6d4c24-8cbd-4b35-9272-dd3cbfc81887&DisplayLang=en>

To install the Group Policy Management Console snap-in, double-click the gpmc.msi file and follow the on screen instructions. On the final installation screen, click **Finish**.

.NET Framework

.NET Framework 2.0 is required. It is included as part of .NET Framework 3.5. If you do not already have .NET Framework installed, version 3.5 may be downloaded from the Microsoft website at the following URL:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=333325FD-AE52-4E35-B531-508D977D32A6&displaylang=en>

To install .NET Framework 3.5, double-click the dotNetFx35setup.exe file and follow the on screen instructions. On the final installation screen, click **Finish**.

Microsoft Management Console 3.0

The Microsoft Management Console 3.0 may be downloaded from the Microsoft website at the following URL if it is not already installed:

<http://www.microsoft.com/downloads/details.aspx?familyid=4C84F80B-908D-4B5D-8AA8-27B962566D9F&displaylang=en>

To install Microsoft Management Console 3.0, double-click the WindowsServer2003-KB907265-x86-ENU.exe file and follow the on screen instructions. On the final installation screen, click **Finish**.

Windows Server 2008 and Windows Server 2008 R2

The Microsoft Remote Server Administration Tools are included as part of Windows Server 2008. Complete the following steps to enable the features that the Manager Console requires:

- 1 Click **Start**, point to **Administrative Tools**, and click **Server Manager**. The Server Manager snap-in appears.
- 2 In the left-hand pane, click **Features**. In the Features pane on the right, click **Add Features**. The **Add Feature Wizard** appears.
- 3 Select the **Group Policy Management** check box.
- 4 Expand **Remote Server Administration Tools**, expand **Role Administration Tools**, expand **Active Directory Domain Services Tools**, and select the **Active Directory Domain Controller Tools** check box.
- 5 Click **Next**, then click **Install**. After the Add Features Wizard indicates that installation was successful, click **Close**. Choose **File**, then click **Exit** to close the Server Manager snap-in.

Manager Console Installation

Framework InstallShield Wizard

Initial Steps

If you are using Windows authentication for the Policy Administrator account (see Chapter 1 “[Required Accounts](#)” on page 11), log on to the target computer using this account.

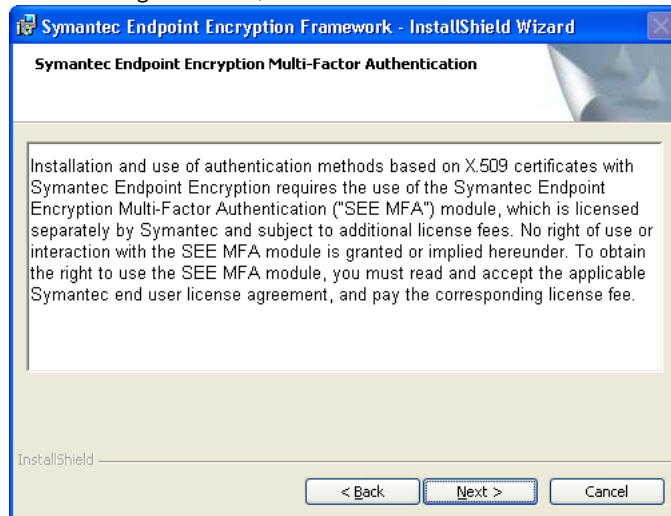
Determine whether the Manager Computer is running a 32-bit edition of Windows or a 64-bit edition of Windows.

If the operating system is 32 bits, launch the Symantec Endpoint Encryption Framework.msi file. If the operating system is 64 bits, launch the Symantec Endpoint Encryption Framework x64.msi file.

The **Welcome** page of the Framework InstallShield Wizard appears. Click **Next**.

The **Symantec Endpoint Encryption Multi-Factor Authentication** page of the Framework InstallShield appears.

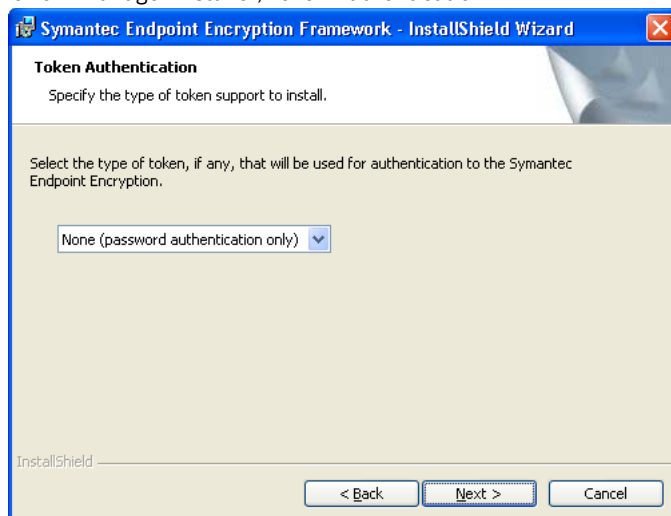
Figure 3-1 Framework Manager Installer, Multi-Factor Authentication



Click **Next**. The **License Agreement** page appears. Select the option **I accept the terms in the license agreement**, then click **Next**.

The **Token Authentication** page appears.

Figure 3-2 Framework Manager Installer, Token Authentication



This page allows you to choose the type of token, if any, that will be used to authenticate to Symantec Endpoint Encryption.

Select **None** to use password authentication only.

Select **RSA USB tokens and cards** to use devices that support the RSA data model.

Select **Common Access Card** to use devices that support the CACv2 data model.

Select **Smart card** to use devices that support the GSC-IS 2.1 data model.

Select **Aladdin eToken** to use devices that support the Aladdin eToken data model.

Select **Personal Identity Verification** to use devices that support the PIV-I/PIV-II or CAC NG (Transitional PIV) data model.

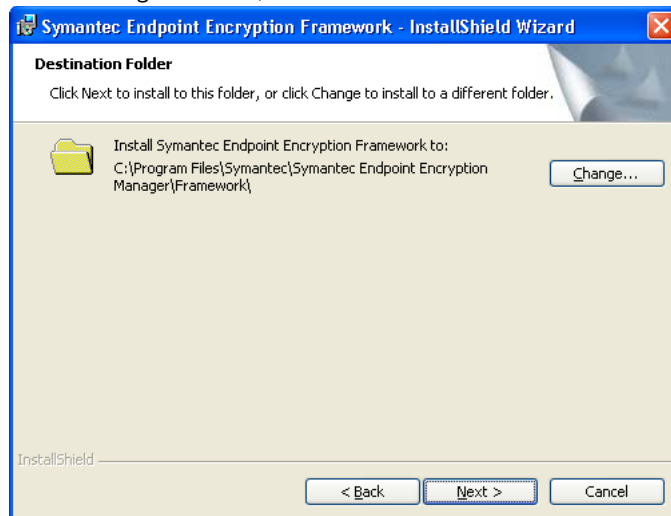
Select **SafeSign v2.1** to use devices that support the SafeSign v2.1 data model.

For more information about supported tokens, refer to [Table 1-13](#).

Note: Ensure the accuracy of your selection, as it will affect all client installation packages created from this machine.

Choose a token type, or accept the default value of **None**, then click **Next**.

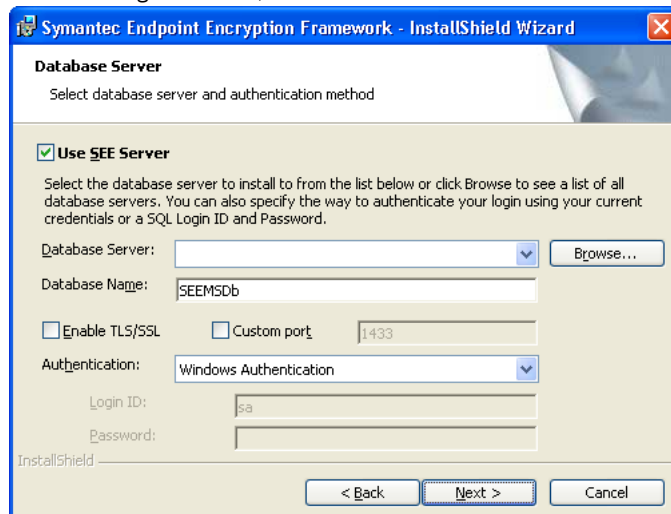
The **Destination Folder** page appears.

Figure 3-3 Framework Manager Installer, Destination Folder

This page allows you to change where the Manager Console program files will be installed.

Click **Change** to choose a different location to install the Manager Console, or click **Next** to accept the default installation location.

The **Database Server** page appears.

Figure 3-4 Framework Manager Installer, Database Server

Leave the **Use SEE Server** check box selected to install this Manager Console in default mode. If you do not want to make use of the Symantec Endpoint Encryption database, deselect the **Use SEE Server** check box and request the *Serverless Mode Supplement* from Symantec technical support.

Select the Microsoft SQL Server instance hosting the Symantec Endpoint Encryption database. Click **Browse** to select from a list of instances, or type the NetBIOS name of the instance in the **Database Server** box. If the database was created using the default name of SEEMSDb, accept this name. Otherwise, type the unique custom name that the database was created with in the **Database Name** box. If the SQL Server instance was configured to use TLS/SSL encryption, select the **Enable TLS/SSL** check box. Select the **Custom port** check box if your database server has been configured to use a custom port. Selecting the **Custom port** check box will cause a port field to become available and allow you to type the custom port number.

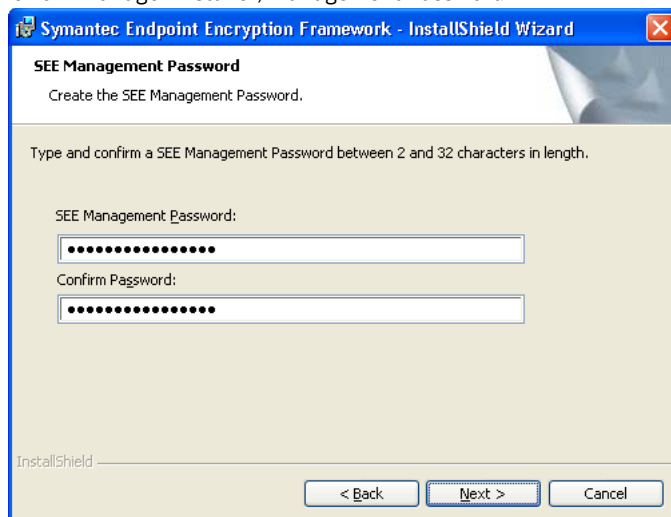
Provide the credentials of the Policy Administrator account (Chapter 1 [“Required Accounts”](#) on page 11). Select **Windows Authentication** from the Authentication list box to use the credentials of the currently logged on Windows user to authenticate to the Symantec Endpoint Encryption database. Alternatively, you

can authenticate using a SQL account. Select **SQL Account** from the **Authentication** list box and type the SQL credentials of the Policy Administrator account (see Chapter 1 “[Required Accounts](#)” on page 11).

Click **Next**. The InstallShield Wizard authenticates to the database server you specified and verifies that the account credentials you entered are correct before allowing you to continue.

If this is the first installation of a Manager Console following a fresh Management Server installation, or if OTP keys are not found in the Symantec Endpoint Encryption database, the **Symantec Endpoint Encryption Management Password** page appears. If this page does not appear, skip to “[Concluding Steps](#)” on page 42.

Figure 3-5 Framework Manager Installer, Management Password



The Management Password only needs to be set once. It will be encrypted and stored in the Symantec Endpoint Encryption database. During subsequent installations of the Framework Manager Console on additional Manager Computers, the installer will detect that the Management Password has already been set, and this screen will not be shown. Instead, the **Ready to Install the Program** page (“[Concluding Steps](#)” on page 42) will appear.

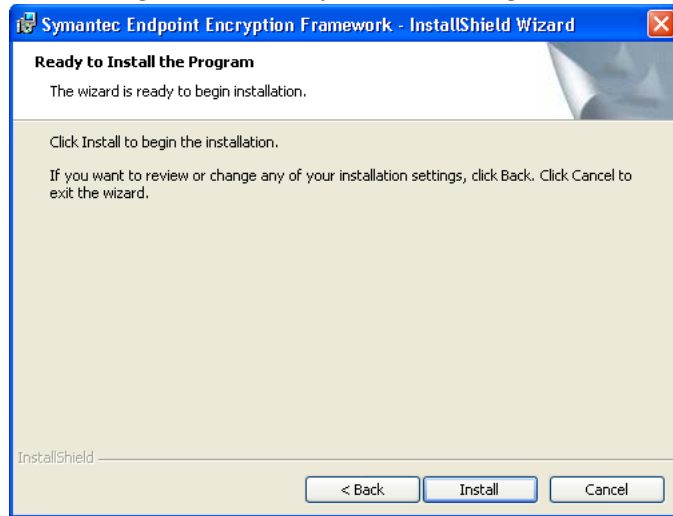
The Management Password must be between 2 and 32 characters in length. The Management Password can be changed at a later time using the Management Password snap-in from the Symantec Endpoint Encryption Manager.

Once you have established a Management Password, click **Next**.

Concluding Steps

The **Ready to Install the Program** page appears.

Figure 3-6 Framework Manager Installer, Ready to Install the Program



Click **Install**.

After the Framework **InstallShield Wizard Completed** page appears, click **Finish**. Continue to [“Full Disk InstallShield Wizard”](#) on page 43 and run the Full Disk InstallShield Wizard.

Full Disk InstallShield Wizard

Once the Framework InstallShield Wizard completes, launch the package compatible with your installed version of Windows.

If the operating system is 32 bits, launch the Symantec Endpoint Encryption Full Disk Edition.msi file. If the operating system is 64 bits, launch the Symantec Endpoint Encryption Full Disk Edition x64.msi file.

The **Welcome** page of the Full Disk InstallShield Wizard appears. Click **Next**.

The **License Agreement** page of the Full Disk InstallShield Wizard appears. Select the option **I accept the terms in the license agreement**, then click **Next**.

The **Ready to Install the Program** page appears. Click **Install**.

After the Full Disk **InstallShield Wizard Completed** page appears, click **Finish**.

Help Desk Program

Basics

The Help Desk Program allows administrators to assist users who have forgotten their credentials. Using the Help Desk Program, the administrator provides the user with a one-time response key that allows the user to gain access to their computer. For more details on running the Help Desk Program, refer to the *Policy Administrator Guide*.

Installation

Once you have completed the installation of the Manager (see [“Manager Console Installation”](#) on page 39), proceed to install the One-Time Password Program (optional).

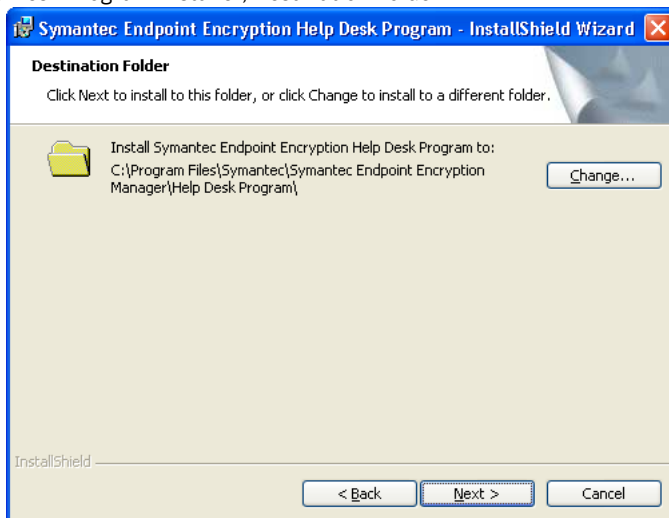
If the operating system is 32 bits, launch the Symantec Endpoint Encryption Help Desk.msi file. If the operating system is 64 bits, launch the Symantec Endpoint Encryption Help Desk x64.msi file.

The **Welcome** page of the Symantec Endpoint Encryption Help Desk Program InstallShield Wizard appears. Click **Next**.

The **License Agreement** page of the Symantec Endpoint Encryption Help Desk Program InstallShield Wizard appears.

Select the option **I accept the terms in the license agreement**, then click **Next**. The **Destination Folder** page appears.

Figure 3-7 Help Desk Program Installer, Destination Folder



Click **Change** to choose a different location to install the Help Desk Program files, or click **Next** to accept the default installation location. The **Ready to Install the Program** page appears.

Click **Install**.

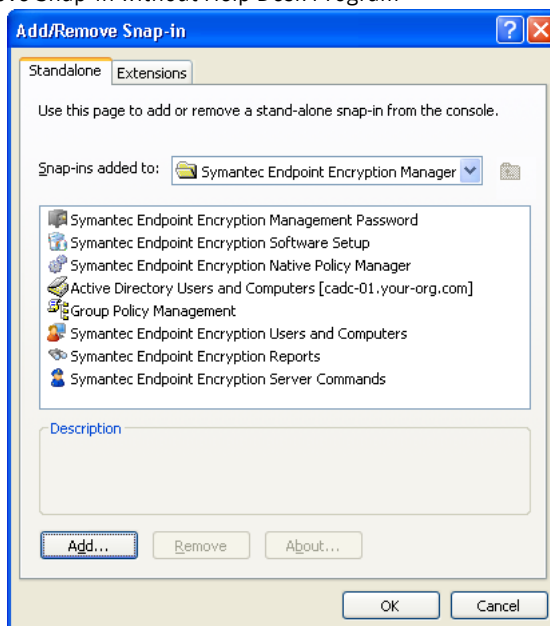
After the **Symantec Endpoint Encryption Help Desk Program InstallShield Wizard Completed** page appears, click **Finish**.

Launch the Symantec Endpoint Encryption Manager from the **Start** menu.

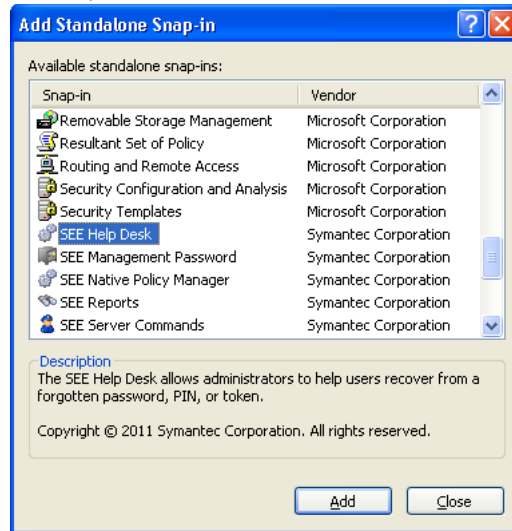
Select **Add/Remove Snap-In** from the **File** menu.

The **Add/Remove Snap-in** dialog will be displayed.

Figure 3-8 Add/Remove Snap-In without Help Desk Program

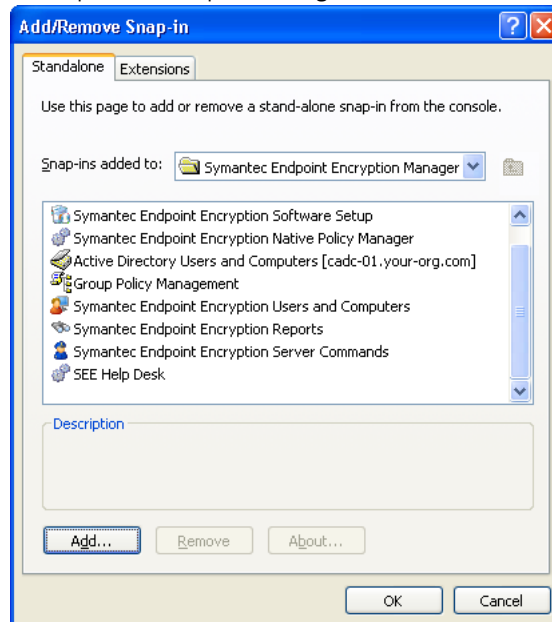


Click **Add**.

Figure 3-9 Add Standalone Snap-In

Scroll until you locate the Help Desk Program. Highlight **Symantec Endpoint Encryption Help Desk** and click **Add**.

Then click **Close**.

Figure 3-10 Add/Remove Snap-In with Help Desk Program

The Help Desk Program should now appear in the list of snap-ins included in the Symantec Endpoint Encryption Manager. Click **OK**.

The Help Desk Program should now be shown in the console tree of the Symantec Endpoint Encryption Manager. To optionally restrict access to the other snap-ins of the Manager Console, see [“Restricting Access to Snap-in Extensions”](#) on page 48.

Add Forest

To complete the installation, follow these steps:

- 1 Open the Symantec Endpoint Encryption Manager. Click **Start**, point to **All Programs**, then click **Symantec Endpoint Encryption Manager Console**.

- 2 In the navigation pane on the left, select the Group Policy Management snap-in, right-click, and choose **Add Forest**.

Figure 3-11 Group Policy Management Console, Add Forest



- 3 In the **Add Forest** dialog box, type the fully-qualified domain name.
- 4 Click **OK**.

With the Manager Console now installed on the Manager Computer, you are now ready to create client installer packages.

Back Up Symantec Endpoint Encryption Database

Perform an immediate backup of the Symantec Endpoint Encryption database.

Manager Console Snap-In Access Control

Basics

The Manager Console is comprised of both Microsoft and Symantec Endpoint Encryption snap-ins. To ensure that Symantec Endpoint Encryption management facilities are limited only to authorized personnel, Symantec recommends that you create a default policy that restricts Symantec Endpoint Encryption snap-in access. Once this default policy is in place, Policy Administrators should be assigned access on a per snap-in basis.

Controlling Access to the Symantec Endpoint Encryption Snap-ins

Basics

Controlling access to the Symantec Endpoint Encryption snap-ins can be done in two steps:

- 1 Create a policy which restricts users from running the Symantec Endpoint Encryption snap-ins (see [“Creating a Policy that Restricts Access to Snap-ins”](#) on page 47) and/or snap-in extensions (see [“Restricting Access to Snap-in Extensions”](#) on page 48).
- 2 Create a second policy with a higher precedence which permits selected users or groups to run the Symantec Endpoint Encryption snap-ins and/or snap-in extensions (see [“Creating a Policy that Permits Access to Snap-ins”](#) on page 49).

Note: The “Permitted” policy must be applied at a lower level (i.e., higher precedence) in the Active Directory container hierarchy than the “Restricted” policy. If both policies are applied to the same OU, make sure that the “Permitted” policy has a lower link order number (higher precedence) than the “Restricted” policy.

Creating a Policy that Restricts Access to Snap-ins

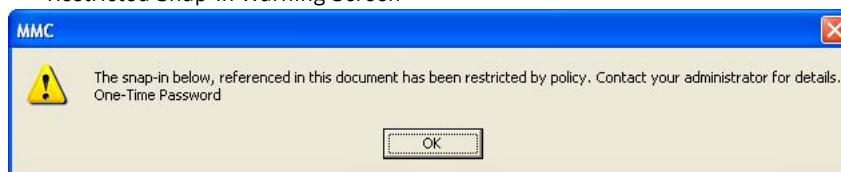
In the first step, you will create and edit a new GPO, disable the Restricted/Permitted snap-ins settings for all currently installed Symantec Endpoint Encryption snap-ins, and link this GPO at the domain level to prevent all domain users from running the Symantec Endpoint Encryption snap-ins.

To perform this procedure

- 1 Open the Manager Console, click the Group Policy Management container and expand the entire container hierarchy to reveal the Group Policy Objects container. Right-click **Group Policy Objects** and select **New**. A **New GPO** window displays.
- 2 Type the name for the GPO and click **OK**. Right-click the GPO and choose **Edit**. The GPOE (Group Policy Object Editor) will open.
- 3 In the navigation pane on the left side of the GPOE window, expand **User Configuration**, then **Administrative Templates**.
If the Symantec Endpoint Encryption subfolder is already present within the Administrative Templates folder, skip ahead to step 7. If you have previously accessed a Symantec Endpoint Encryption settings panel within this GPO, the Symantec Endpoint Encryption templates were loaded automatically.
- 4 Select the Administrative Templates folder. From the **Action** menu, choose **Add/Remove Templates**, and the **Add/Remove Templates** window opens.
- 5 In the **Add/Remove Templates** window, click **Add**, and navigate to the local path where the Framework administrative template is stored:
C:\Program Files\Symantec\Symantec Endpoint Encryption Manager\Framework\ADM
- 6 Select the template file EA Framework.adm, click **Open**, then click **Close**.
- 7 With the Framework template now loaded in the GPOE, expand Symantec Endpoint Encryption, expand **Framework**, then select **Restricted/Permitted Snap-ins**. This folder will contain the Extension Snap-ins folder and several settings panels, one for each Framework snap-in or snap-in extension.
- 8 In the pane on the right, double-click the item named *SEE Software Setup*, and the panel properties for that item opens with the *Setting* tab shown. Change the option from **Not Configured** to **Disabled**, click **Apply**, then **Next Setting**. The next panel in the sequence will appear.
- 9 Using the **Next Setting** and **Apply** buttons, change the options for all six remaining panels to **Disabled**. Click **OK** when finished, and close the GPOE window.
- 10 Select and drag the GPO onto the OU named *Human Resources* to link it.

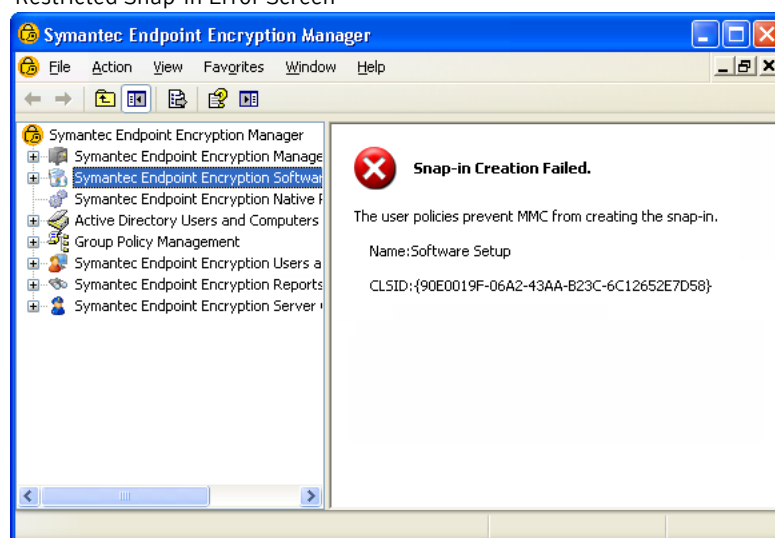
When this policy has been processed on the Client Computers, users that are members of the *Human Resources* OU who log on and launch the Manager Console, or launch a custom MMC console containing a Symantec Endpoint Encryption snap-in, will see a warning screen similar to the following:

Figure 3-12 Restricted Snap-in Warning Screen



After the Manager Console or other MMC console containing the Symantec Endpoint Encryption snap-ins has fully launched, clicking on an individual Symantec Endpoint Encryption snap-in produces an error screen similar to the one shown in the following figure:

Figure 3-13 Restricted Snap-in Error Screen



The error message shown in the figure reflects the fact that this user has been prohibited by policy from accessing the selected snap-in, the Symantec Endpoint Encryption Software Setup snap-in. Notice also that the Framework and Full Disk submodules normally located beneath the parent node of the Symantec Endpoint Encryption Software Setup snap-in are not present in the navigation pane. These submodules extend the functionality of their parent snap-in, and are called snap-in extensions. If desired, you can restrict access to individual snap-in extensions.

Restricting Access to Snap-in Extensions

The Manager Console is comprised of Symantec Endpoint Encryption snap-ins and extensions, as well as Symantec Endpoint Encryption extensions to Microsoft snap-ins. The Symantec Endpoint Encryption extensions to the Microsoft Group Policy Management Console snap-in are what enable the Symantec Endpoint Encryption policy settings panels to appear in the Group Policy Object Editor.

By disabling two of the settings mentioned previously (Symantec Endpoint Encryption Software Setup and Symantec Endpoint Encryption Group Policy), you can restrict access to both the Framework and Full Disk settings used for creating Symantec Endpoint Encryption installation settings or policy settings. If for some reason you wish to only restrict access to a specific snap-in extension, such as the Symantec Endpoint Encryption Software Setup Framework, create a policy to do so.

To create a policy that restricts access to snap-in extensions

- 1 Open the Manager Console, expand the Group Policy Management Console (GPMC) snap-in, select Group Policy Objects, right-click, and choose **New** to create a new GPO.

- 2 Type the name for the new GPO, select it, right-click, and choose **Edit**. The Group Policy Object Editor (GPOE) will open.
- 3 In the navigation pane on the left side of the GPOE window, expand **User Configuration**, expand **Administrative Templates**, expand Symantec Endpoint Encryption, expand **Framework**, expand **Restricted/Permitted Snap-ins**, then select **Extension Snap-ins**. This folder will contain one settings panel for each of the Framework snap-in extensions.
- 4 Double-click the item named *Framework Software Setup*, and the panel properties for that item opens with the *Setting* tab shown.
- 5 Change the option from **Not Configured** to **Disabled**, click **Apply**, then **Next Setting**. Click **OK** when finished, and close the GPOE window.
- 6 Finally, select and drag the GPO onto the OU named *Human Resources* to link it.

When this policy has been processed on the Client Computers, domain users who launch the Symantec Endpoint Encryption Manager, or who launch a custom MMC console containing the Symantec Endpoint Encryption Software Setup snap-in, will see the warning and error screens shown earlier.

After the Manager Console or other MMC console containing the Symantec Endpoint Encryption Software Setup snap-in has fully launched, the Symantec Endpoint Encryption Software Setup snap-in will be available, but the Framework extension to this snap-in will not be loaded.

When this policy is in effect, domain users will be unable to add any restricted Symantec Endpoint Encryption snap-ins when creating a custom MMC. Also, domain users will receive the warning and error messages shown earlier if they attempt to run a Symantec Endpoint Encryption snap-in on a computer where the Manager Console has already been installed, or on a computer where a custom Microsoft Management Console (MMC) has been created and one or more Symantec Endpoint Encryption snap-ins have been added.

Creating a Policy that Permits Access to Snap-ins

With a policy in place which prevents all domain users from running Symantec Endpoint Encryption snap-ins, the second and final step of limiting comprehensive access to the Symantec Endpoint Encryption snap-ins requires that you create a matching policy which is linked at a higher level in the Active Directory object hierarchy. This second policy overrides the first policy, permitting selected users (Policy Administrators) who are members of that OU to run Symantec Endpoint Encryption snap-ins.

Open the Symantec Endpoint Encryption Manager, expand the Group Policy Management Console (GPMC) snap-in, select Group Policy Objects, right-click, and choose **New** to create a new GPO. Type the name for the new GPO, select it, right-click, and choose **Edit**. The Group Policy Object Editor (GPOE) will open. In the navigation pane on the left side of the GPOE window, expand **User Configuration**, expand **Administrative Templates**, expand Symantec Endpoint Encryption, expand **Framework**, and select **Restricted/Permitted Snap-ins**. This folder will contain the Extension Snap-ins folder and several settings panels, one for each Framework snap-in or snap-in extension.

To perform this procedure

- 1 Double-click the item named *Symantec Endpoint Encryption Software Setup*, and the panel properties for that item opens with the *Setting* tab displayed. Change the option from **Not Configured** to **Enabled**, click **Apply**, then **Next Setting**.
- 2 The next panel in the sequence will appear. Using the **Next Setting** and **Apply** buttons, change the options for all three remaining panels to **Disabled**. Click **OK** when finished, and close the GPOE window.
- 3 Next, change the security filtering for this policy so that only Policy Administrators for this OU, HR Admins, will receive the policy. With the policy still selected, click **Remove** in the Security Filtering section to remove the default group, Authenticated Users. Click **Add**, and in the input field of the window that opens, type "HR", click **Check Names**, and the input field will fill with the HR Admins group name. Click **OK**.

- 4 Finally, link this second policy to the same OU as you did the first policy, making sure that the second policy has a higher order of precedence in the Active Directory object hierarchy. With the policy selected, drag it on top of the OU named *Human Resources*, and click **OK** to confirm policy linking.
- 5 Select the Human Resources OU, and in the **Linked Group Policy Objects** tab in the right pane, make sure that the **Link Order** of the “Permitted” policy you just created is at a higher precedence (i.e., the link order number is lower) than the “restricted” policy. If necessary, you can adjust the link order using the up or down arrow buttons in the area to the left of the **Link Order** column.

When both the “Restricted” and “Permitted” policies have been successfully processed on the clients, all Policy Administrator accounts in the Human Resources OU will have full access to the Symantec Endpoint Encryption snap-ins, and all domain user accounts in the Human Resources OU will be unable to access the Symantec Endpoint Encryption snap-ins.

Segmenting Support Duties

The ability to restrict access to individual Symantec Endpoint Encryption snap-ins allows you to assign the duties of Symantec Endpoint Encryption support staff in a granular fashion. For example, you could create a custom MMC file containing only the Symantec Endpoint Encryption Reports snap-in, and distribute this file to select Policy Administrator accounts which you had restricted from accessing the other Symantec Endpoint Encryption snap-ins. This would allow those Policy Administrator accounts the ability to create Symantec Endpoint Encryption recovery media (provided they had also been given the Management Password) and view the last check-in time of Symantec Endpoint Encryption Client Computers, while at the same time preventing them from accessing the Symantec Endpoint Encryption policy settings panels or allowing them to create Symantec Endpoint Encryption installation packages.

Client Installation Package Creation

This chapter includes the following topics:

- [Overview](#)
- [Framework Installation Settings Wizard](#)
- [Full Disk Installation Settings Wizard](#)

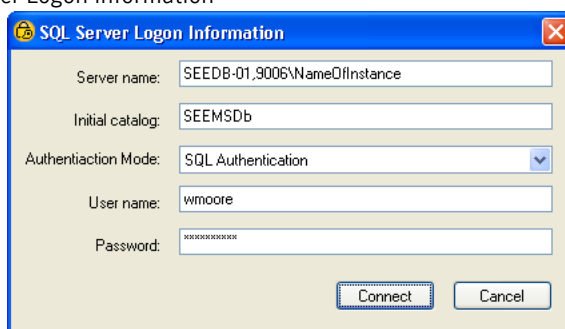
Overview

The Symantec Endpoint Encryption client installation packages deliver the client software, software upgrades, and initial settings to Client Computers. The client installation packages consist of four MSIs, one ZIP file (optional), and two log files. The log files document the contents of the associated MSI and include the date and time that they were created in their file names.

- Symantec Endpoint Encryption Framework Client.msi
- Symantec Endpoint Encryption Framework Client_x64.msi
- FrameworkSettings month_day_year-hour.minute.sec.log
- Symantec Endpoint Encryption Full Disk Edition Client.msi
- Symantec Endpoint Encryption Full Disk Edition Client_x64.msi
- Symantec Endpoint Encryption Full Disk Edition Client_MAC.zip (optional)
- FullDiskSettings month_day_year-hour.minute.sec.log

If you are using Windows authentication, ensure that you are logged on using the Policy Administrator account (see [“Required Accounts”](#) on page 11). Open the Manager Console.

If the credentials of the user account you are logged on to Windows with are not validated for database access, you will be prompted to provide the SQL or Windows credentials of the Policy Administrator account (Chapter 1 [“Required Accounts”](#) on page 11).

Figure 4-1 SQL Server Logon Information

The **Server name** and **Initial catalog** fields will contain the information that was provided when this Manager Console was installed. In general, you should not modify the default contents of these fields. Circumstances that require you to edit these entries would be unusual, such as the loss of your primary Symantec Endpoint Encryption database. In such a situation, you could edit the **Server name** and **Initial catalog** fields to connect to a disaster recovery site. The syntax used in the **Server name** field is as follows:

computer name,port number\instance name

While the NetBIOS name of the server hosting the Symantec Endpoint Encryption database will always be required, the TCP port number will only be necessary if you are using a custom port, and the instance name will only be needed if you are using a named instance. The custom port number would need to be preceded by a comma and the instance name by a backslash.

To use a SQL account, select **SQL Authentication** and type the SQL user name in the **User name** field. Otherwise, select **Windows Authentication** and type the Windows account name in NetBIOS format in the **User name** field. Type the account password in the **Password** field. Click **Connect** to authenticate.

Framework Installation Settings Wizard

Basics

Prior to deploying Framework to your clients, you need to run a wizard that lets you select installation settings specific to Framework. The panels shown by the wizard will differ depending on the authentication method you choose. When you reach the final panel of the wizard, you will be prompted for a location to save the Framework client installation settings MSI package.

Client Administrators

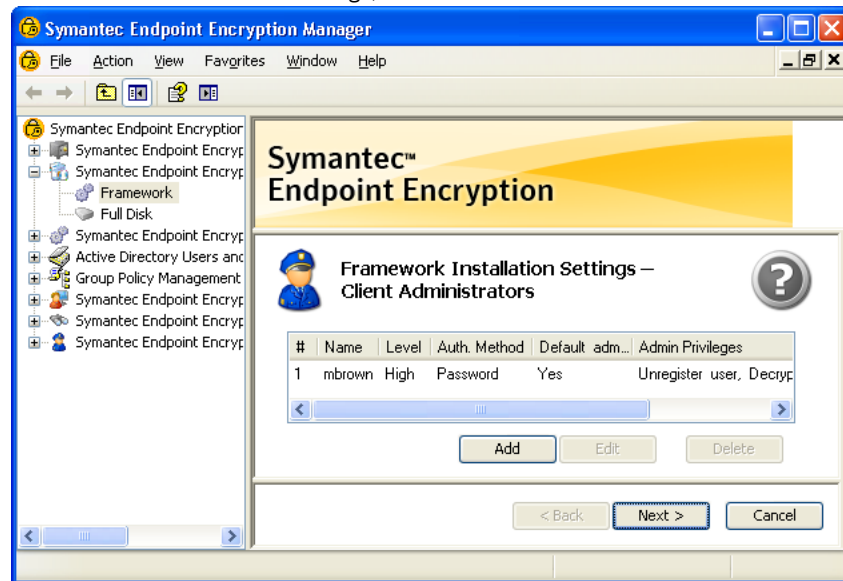
In the left pane, expand the **Symantec Endpoint Encryption Software Setup** container, and click on **Framework**. The first wizard screen appears in the right pane of the Manager window.

Use the Client Administrators panel to specify Client Administrator accounts for the computers on which this software setup package will be installed. When you define a Client Administrator account, you must choose whether the account uses password or token authentication, and select the privilege of the account. Note that you must specify at least one password-based Client Administrator account with full privileges, known as the default Client Administrator account.

Only the default Client Administrator account will be included in your Mac client installation package.

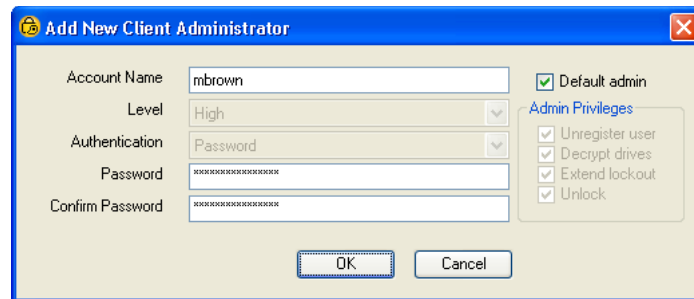
For more information on adding or removing Client Administrators following the deployment of the initial installation package, refer to the *Policy Administrator Guide*.

Figure 4-2 Framework Installation Settings, Client Administrators



To specify a Client Administrator account, click **Add**. The **Add New Client Administrator** dialog is displayed.

Figure 4-3 Add New Client Administrator



To perform this procedure

- 1 In the **Account Name** box, type the account name for this Client Administrator. The account name can be between 1 and 32 characters in length.
- 2 If the **Default admin** check box is available, leave it selected to designate this Client Administrator as the default Client Administrator account. Otherwise, deselect the check box. If you deselect the **Default admin** check box, the **Level**, **Authentication**, and **Admin Privileges** controls become available. The **Default admin** check box will be unavailable if you already added a default Client Administrator.
- 3 The **Admin Privileges** area is only available if the **Default admin** check box is deselected. Select the **Unregister users** check box to allow the Client Administrator to unregister users. Select the **Decrypt drives** check box to allow the Client Administrator to decrypt encrypted disks and partitions, and to use the Recover /D option. Select the **Extend lockout** check box to allow the Client Administrator to extend the Client Computer's next communication date. Select the **Unlock** check box to allow the Client Administrator to unlock Client Computers. Deselect all the check boxes to only allow the Client Administrator to authenticate to Client Computers.
- 4 The **Level** list box is only available if the **Default admin** check box is deselected. Note that the privileges you set in the **Level** list box will be ignored.
- 5 The **Authentication** list box is only available if the **Default admin** check box is deselected. Click **Authentication** to set the Client Administrator's authentication method. If you selected **None (password authentication only)** when installing the Framework Manager (discussed in this chapter "Framework Installation Settings Wizard" on page 52), the list box will display **Password** and be

unavailable. If you selected one of the token types when installing the Framework Manager, the list box will have both **Password** and **Token** options available.

- 6 Provide the password or certificate to be used by this Client Administrator to authenticate.
 - If you select **Password** authentication, type the desired password for this Client Administrator account in the **Password** box. The password must be a minimum of two characters and no longer than 32. Type the password a second time in the **Confirm password** box.
 - If you select **Token** authentication, you will be prompted for the location of the PKCS#7 format certificate file (P7B) corresponding to this Client Administrator account.
- 7 Click **OK** to add this Client Administrator account.
- 8 Click **Add** to add more Client Administrator accounts. If you decide not to include a Client Administrator you have already added, select the account, and click the **Delete** button.
- 9 Click **Next** to advance to the next panel. If you did not designate one Client Administrator account as the default Client Administrator account, you will be unable to advance to the next panel.

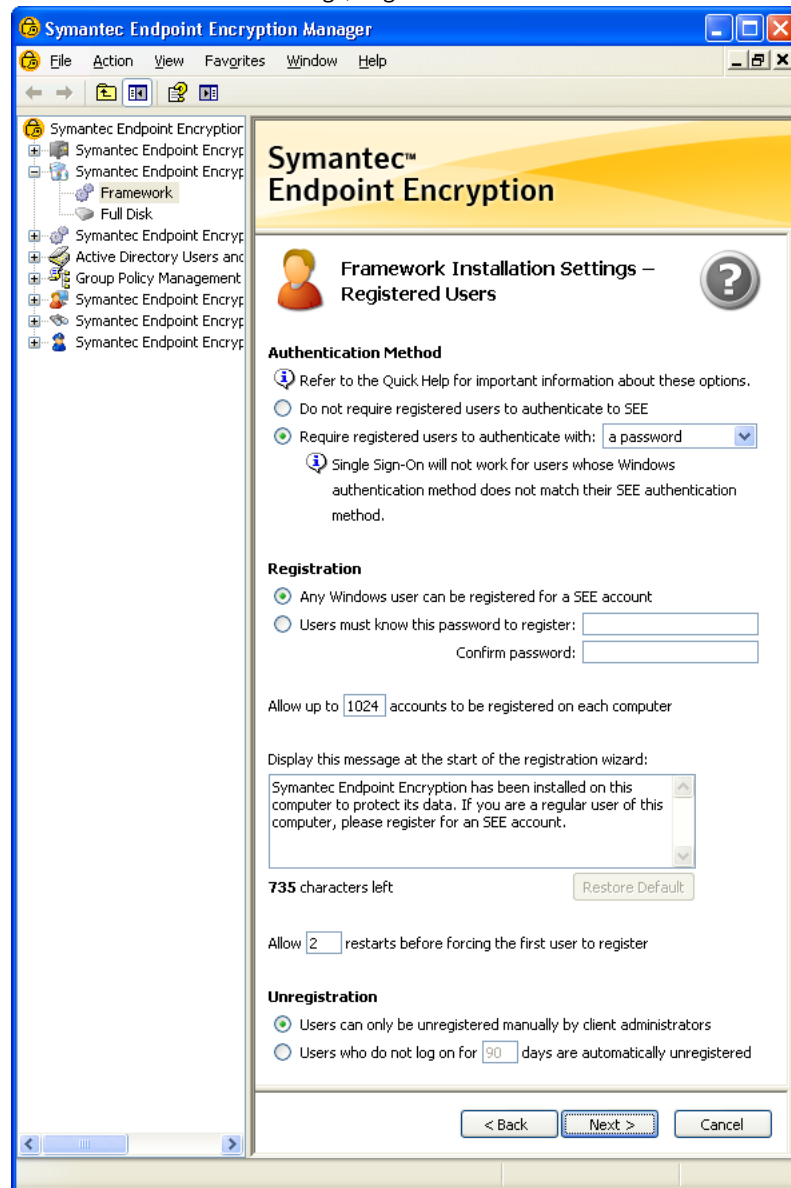
Registered Users

Basics

Use the Registered Users panel to specify settings related to the Symantec Endpoint Encryption user registration process, including the authentication method, registration password, maximum number of registered users allowed, custom registration message, number of grace restarts, and unregistration.

Registered user settings will not be included in the Mac client installation package.

Figure 4-4 Framework Installation Settings, Registered Users



Authentication Method

The first option on this panel allows you to define how users authenticate to Symantec Endpoint Encryption.

- Select **Do not require registered users to authenticate to Symantec Endpoint Encryption** to enable automatic authentication. This option is designed for kiosk environments. If it is selected, users will not need to provide valid credentials to Full Disk before Windows loads and your organization will rely on Windows for user authentication. It will reduce the security of the Client Computer but increase the transparency of the user experience. The registration process will be silent and automatic as well—unless a registration password is specified (see next section). Coupling automatic authentication with a registration password serves to avoid reaching the maximum registered user limit and to limit the number of users that can gain access to the User Client Console. When you select **Do not require registered users to authenticate to Symantec Endpoint Encryption**, the **Single Sign-On** and **Authentication Assistance** panels will be skipped in the sequence of wizard panels.
- Select **Require registered users to authenticate with** to specify using the drop-down menu whether users authenticate to Symantec Endpoint Encryption with a password, a token, or either. The

drop-down menu will be unavailable if password authentication was selected when the Manager Console was installed. Note that when Single Sign-On is active ([“Single Sign-On”](#) on page 56), the authentication method chosen for Symantec Endpoint Encryption must match the method specified in Windows.

Registration

The **Registration** section defines which users will be allowed to become Symantec Endpoint Encryption registered users. To allow any Windows user the ability to register, click the option **Any Windows user can be registered for a SEE account**. To allow only those users who know a special registration password to be able to register, click **Users must know this password to register**, and type the password in the adjacent field and again to confirm. Each user will be required to know the administrator-defined registration password before they can register for a Symantec Endpoint Encryption account.

Specify the maximum number of Symantec Endpoint Encryption registered user accounts which can be created on each computer. New users will not be permitted to register after the maximum number of accounts has been reached.

Specify a custom message users will see when they are forced to register after grace restarts expire. The custom message can be from 0–900 characters in length, or you can use the default message. Note that the custom registration message field ignores any carriage returns you type or paste in.

Specify the number of grace restarts, i.e., the number of times, from 0–99, that the computer can restart before the first user who logs on will be forced to register for a Symantec Endpoint Encryption account and see the custom registration message. This setting can effectively allow users to defer registration. To force the first user to register immediately, set this value to zero.

Unregistration

Unregistration selects whether to allow users to only be unregistered manually by Client Administrators, or whether to also automatically unregister users who do not log on after a specified period, from 1–365 days. This setting is useful in a kiosk environment where many infrequent users can fill up the maximum number of available Symantec Endpoint Encryption accounts on a given computer. Use caution with this setting so that users do not have their accounts deleted unexpectedly.

Next Button

If you chose token or password authentication, clicking **Next** will advance to the **Single Sign-On** panel discussed in the next section. If you chose automatic authentication, clicking **Next** will advance to the Communication panel (see [“Communication”](#) on page 63).

Single Sign-On

The Single Sign-On panel will only be shown if you chose **Require registered users to authenticate with** in the Registered Users panel ([“Authentication Method”](#) on page 55).

Your selection in this panel will not be included in the Mac client installation package.

Figure 4-5 Framework Installation Settings, Single Sign-On

If Single Sign-On is enabled, users log on once in pre-Windows and are authenticated both to Symantec Endpoint Encryption and Windows. In addition, users will be able to access the User Client Console without an additional logon, after they log on the first time. This installation setting can be changed later using a policy.

To enable Single Sign-On, select the **Enable Single Sign-On** check box.

Note: If Single Sign-On is enabled, password changes must be initiated by the user on the local workstation. Administrators cannot reset users' passwords from the server. Third party password change tools such as SSPRM are not supported.

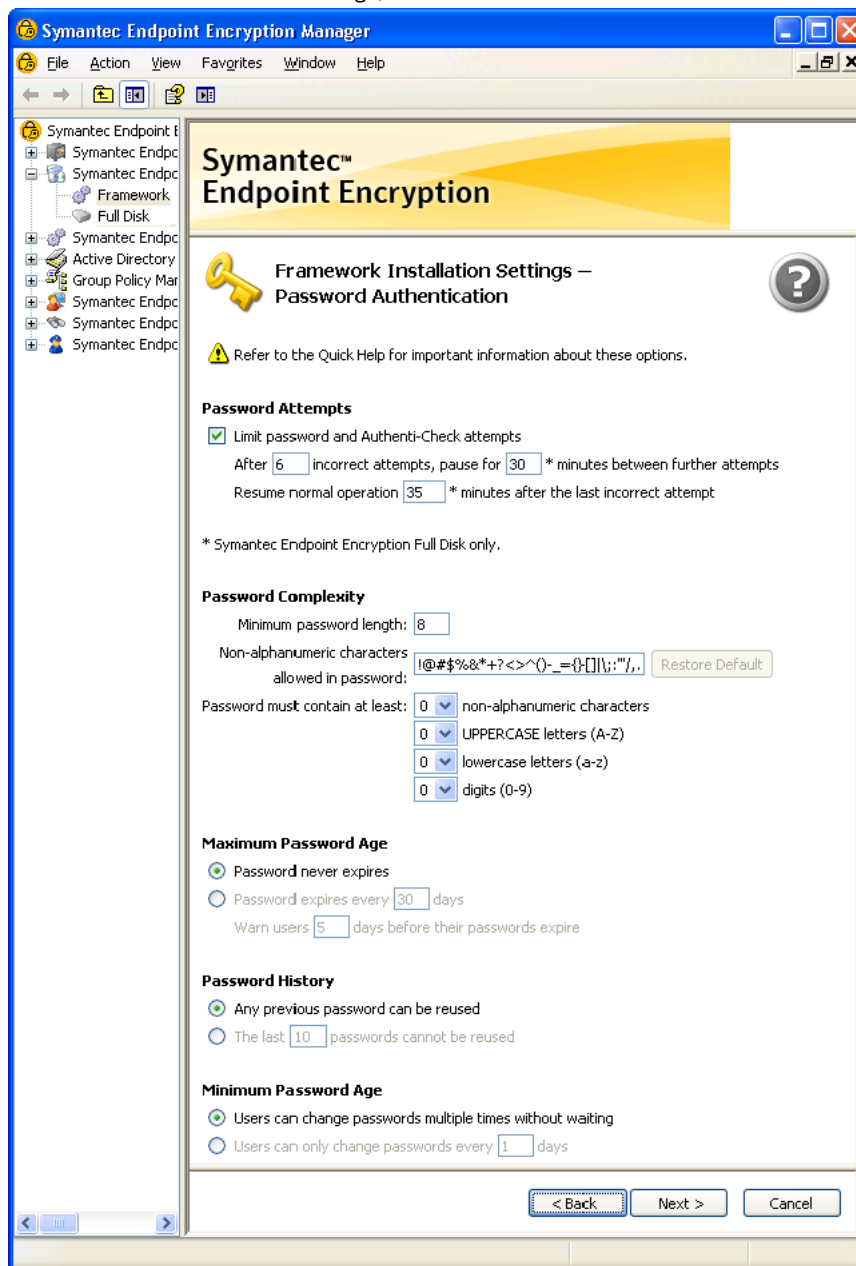
Click **Next** to advance to the next panel.

Password Authentication

Basics

Use the Password Authentication panel to configure settings for the passwords used to authenticate to Symantec Endpoint Encryption and to encrypt/decrypt Removable Storage files.

Figure 4-6 Framework Installation Settings, Password Authentication



Password Attempts

Use the **Password Attempts** area to configure a logon delay to protect against dictionary attack tools.

To perform this procedure

- 1 In the **After** box, type the number of incorrect password attempts and/or incorrect Authenticator attempts that will be allowed to occur before the delay is instituted.
- 2 Type the length of the delay in the **pause for** box.
- 3 Type the length of time that must elapse between incorrect logon attempts before the delay is lifted in the **Resume normal operation** box. This number must be equal to or greater than the number in the **pause for** box.

To understand the interrelationship among the three settings, consider the following example. An administrator sets the **After** box to 6, the **pause for** box to 30, and the **Resume normal operation** box to 35. A user types an incorrect password six times, trying to log on to the User Client Console. The computer institutes the logon delay, preventing anyone from logging on to the Client Console for 30 minutes. Four minutes after the logon delay is lifted, the user enters another incorrect password. A logon delay of 30 minutes is instituted.

Note: Mac clients ignore these settings.

Password Complexity

In the **Password Complexity** area:

- 1 In the **Minimum password length** box, type the number of characters users' Symantec Endpoint Encryption passwords must contain.
- 2 In the **Non-alphanumeric characters** box, enter the set of non-alphanumeric characters users must have in their passwords.
- 3 For the **Password must contain at least** settings, select the number from each list box to define the **minimum number of non-alphanumeric characters**, **UPPERCASE letters (A-Z)**, **lowercase letters (a-z)**, and **digits (0-9)** that users must have in their passwords.

If Single Sign-On is enabled, the **Password Complexity** settings will only be enforced for Removable Storage file encryption passwords.

Maximum Password Age

In the **Maximum Password Age** area, leave the default selection of **Password never expires** to not set an expiration date on user passwords.

If you want to set an expiration date on user passwords:

- 1 In the **Password expires every** box, type the number of days after which users' passwords will expire.
- 2 In the **Warn users** box, type the number of days in advance users will be prompted to change their expiring passwords.

If Single Sign-On is enabled, the **Maximum Password Age** settings will only be enforced for Removable Storage file encryption passwords.

Note: Mac clients ignore these settings.

Password History

In the **Password History** area, leave the default selection of **Any previous password can be used** to allow users to use any previously used Symantec Endpoint Encryption password.

To define a password history restriction:

- 1 In **The last** box, type the number of different passwords users must use before reverting to old passwords.

If Single Sign-On is enabled, the **Password History** setting will only be enforced for Removable Storage file encryption passwords.

Note: Mac clients ignore these settings.

Minimum Password Age

In the **Minimum Password Age** area, leave the default selection of **Users can change passwords multiple times without waiting** to allow users to change their Symantec Endpoint Encryption passwords as frequently as they wish. Note that leaving this option at the default effectively will override the password history feature, since a user could quickly cycle through the required number of new passwords in order to keep an old, favorite password.

To define a minimum age:

- 1 In the **Users can only change passwords every** box, type the minimum number of days that must pass before users can change their passwords.

If Single Sign-On is enabled, the **Minimum Password Age** setting will only be enforced for Removable Storage file encryption passwords.

Note: Mac clients ignore these settings.

Token Authentication

Use the Token Authentication panel shown in Figure 4.7 to control whether expired token certificates are allowed for authentication to Symantec Endpoint Encryption.

Your selection in the Token Authentication panel will not be included in the Mac client installation package.

Figure 4-7

Framework Installation Settings, Token Authentication



Select the **Users can authenticate to Symantec Endpoint Encryption with expired certificates** check box to allow users to authenticate to Symantec Endpoint Encryption after their certificates expire. Click **Next** to advance to the next panel.

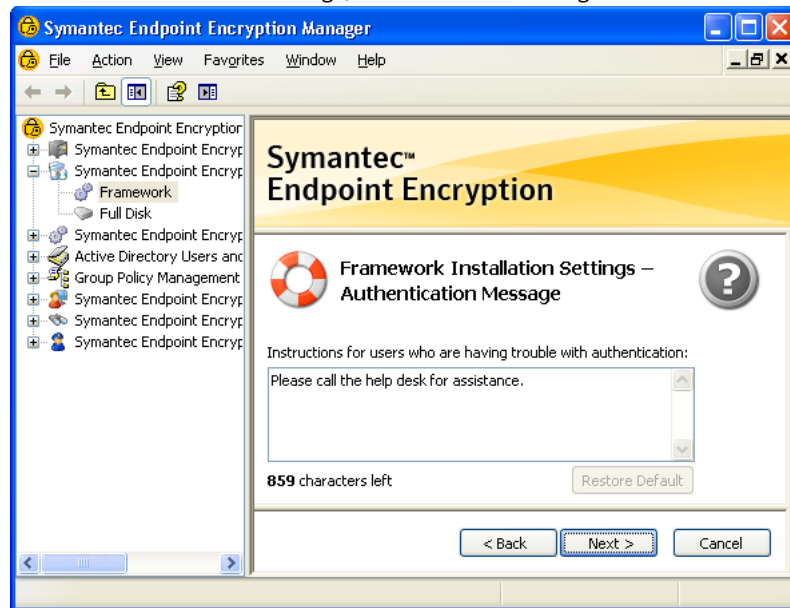
Authentication Message

The Authentication Message panel will only be shown if you chose **Require registered users to authenticate with** in the Registered Users panel (“[Authentication Method](#)” on page 55).

Use the Authentication Message panel to specify a custom authentication assistance message shown to users having trouble logging on.

The custom authentication message will be included in the Mac client installation package.

Figure 4-8 Framework Installation Settings, Authentication Message



The **Instructions for users who are having trouble with authentication** box allows you to specify a custom message of up to 900 characters in length which will be shown to users who have requested logon assistance during pre-Windows authentication. The message is also shown when errors occur during token user registration or pre-Windows authentication.

Click **Next** to advance to the next panel.

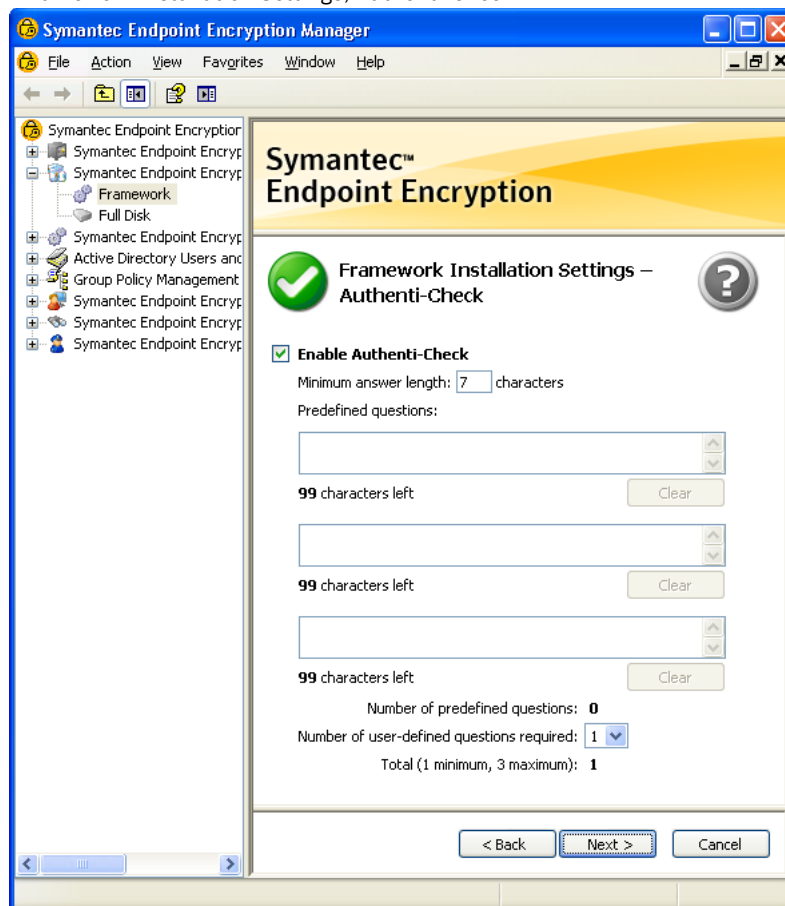
Authenti-Check

The Authenti-Check panel will only be shown if you chose **Require registered users to authenticate with** in the Registered Users panel ("[Authentication Method](#)" on page 55).

Authenti-Check allows users without credentials to gain access to their computers and/or the User Client Console without assistance. A set of up to three question-answer pairs authenticates the user.

Authenti-Check will not be available to Mac users and the settings from the Authenti-Check panel will not be included in the Mac client installation package.

Figure 4-9 Framework Installation Settings, Authenti-Check



Select the **Enable Authenti-Check** check box to make this authentication assistance method available.

Type a value in the **Minimum answer length** box to set the minimum number of characters, from 1–99, that users must include when answering Authenti-Check questions.

Type one, two, or three **Predefined questions**, 0–99 characters in length, that a user must correctly answer before the user authenticates.

The number displayed in the **Number of user-defined questions required** drop-down list is dynamically updated based on how many questions you have typed in the **Predefined questions** boxes. **Number of predefined questions** shows the number of predefined questions currently specified, while **Total** shows the combined total of the **Number of predefined questions** plus the **Number of user-defined questions required**.

Note that at least one question must be defined either by you or by the user.

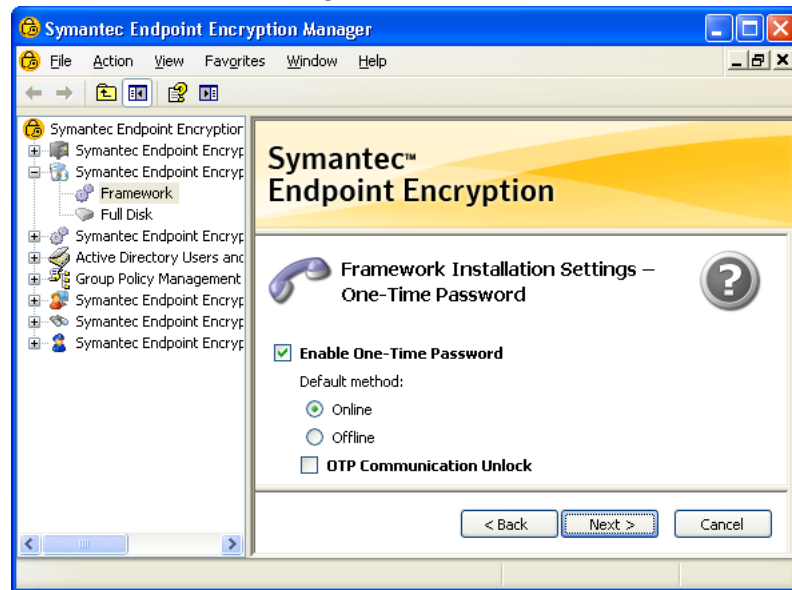
Click **Next** to advance to the next panel.

One-Time Password

The One-Time Password panel will only be shown if you chose **Require registered users to authenticate with** in the Registered Users panel ([“Authentication Method”](#) on page 55).

One-Time Password requires the user to communicate with a Policy Administrator. When One-Time Password activates, the user’s screen displays a code that the user provides to the Policy Administrator. The Policy Administrator types the code into the One-Time Password Program to generate a key that temporarily authenticates the user.

One-Time Password will not be available to Mac users and your selection in the One-Time Password will not be included in the Mac client installation package.

Figure 4-10 Framework Installation Settings, One-Time Password

Select the **Enable One-Time Password** check box to make this authentication assistance method available to Full Disk users.

Within the **Default method** area, select the default method that the Client Computers will begin with when initiating a One-Time Password recovery attempt. The online method is easier and more secure. Select **Online** unless the recipient clients are silent.

Select the **OTP Communication Unlock** check box to allow users who have been locked out of their computers for a failure to communicate to regain access using the One-Time Password Program.

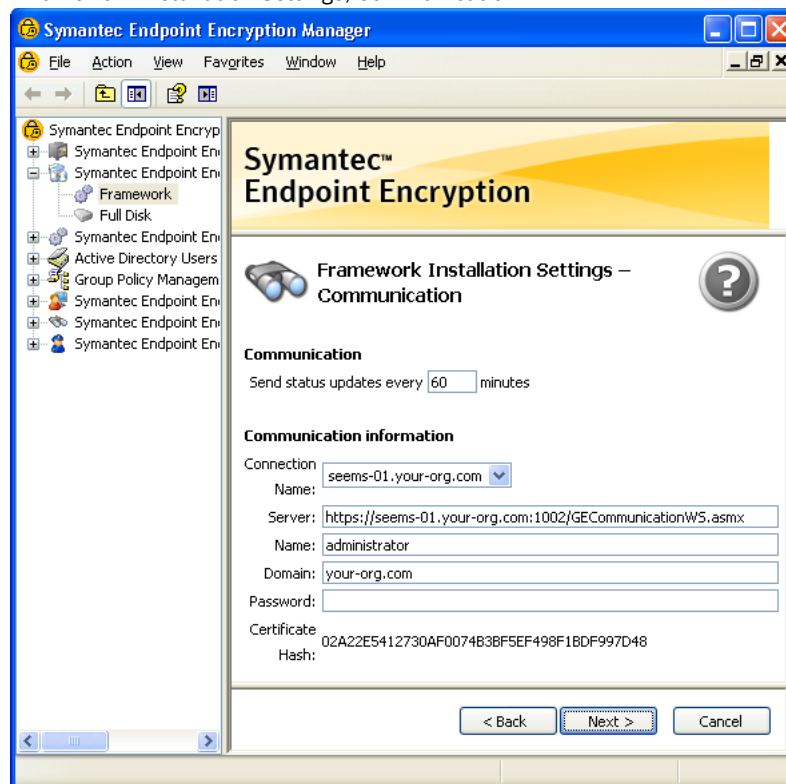
Click **Next** to advance to the next panel.

Communication

Use the Communication panel (see [Figure 4-11](#)) to specify how often client status data is reported, the Management Server that clients will report to, the shared domain account used for client-server communication, and the client-side certificate used for encrypted communication.

The settings from the Communications panel will be included in the Mac client installation package.

Figure 4-11 Framework Installation Settings, Communication



In the **Communication** area, specify the interval, in minutes, at which the Symantec Endpoint Encryption client reports any changes to its status data to the selected Management Server.

The **Communication information** area will update to reflect the configuration information of the currently selected Management Server. Use **Connection Name** to select from a list of available Management Servers, including any you have configured as an NLB cluster.

Note: Management Servers configured into an NLB cluster will be displayed in Connection Name using the FQDN of the cluster, for example, cluster1.your-org.com. This FQDN must match the FQDN specified in the server-side TLS/SSL certificate installed on all cluster members.

Server displays the URL of the web service running on the selected Management Server, including its NetBIOS name or FQDN and port number. This value is set during the installation of the Management Server ([“Web Service Configuration”](#) on page 31) and can be modified later using the Configuration Manager ([“Web Server Configuration”](#) on page 113). If the URL prefix is HTTP, it indicates that unencrypted client-server communication will be used. If the URL pre-fix is HTTPS, it indicates that encrypted client-server communication will be used. A hash of the client-side TLS/SSL certificate retrieved from the Symantec Endpoint Encryption database will be displayed in the **Certificate Hash** section.

Name and **Domain** are prefilled with the name and domain of the IIS client account (see Chapter 1 [“Required Accounts”](#) on page 11). Type the password of this account in the **Password** box.

Click **Next** to advance to the final panel of the wizard, the Encryption panel.

Note: If you are using encrypted Client Computer communications, the Manager Console will attempt to connect to the Management Server when you click Next. If the specified client-side TLS/SSL certificate is not also installed on this computer, the communication will fail and you will be unable to progress to the next panel (see Chapter 2 [“Configuring Encrypted Client Computer/Management Server Communications”](#) on page 18).

Encryption

Use the Encryption panel (see Figure 4.12) to specify the AES encryption strength, either 128-bit or 256-bit.

Note: This installation setting cannot be changed by policy or upgrade package.

Your selection in the Encryption panel will be included in the Mac client installation package.

Figure 4-12 Framework Installation Settings, Encryption



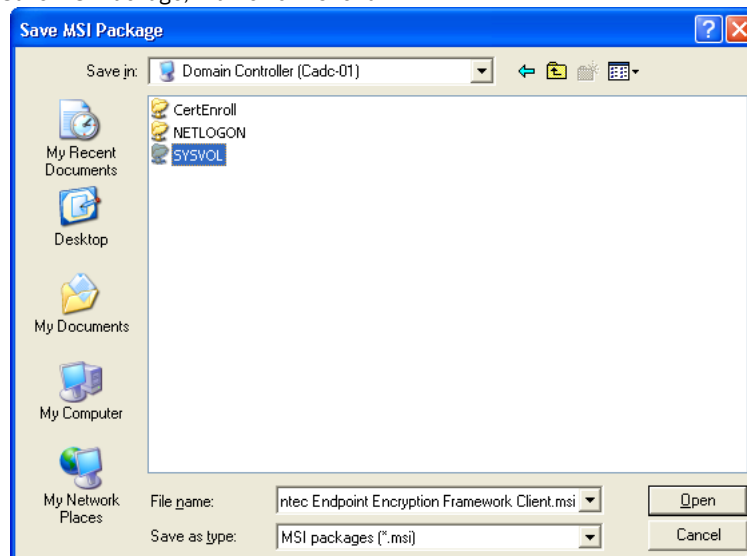
Full Disk will use this setting when encrypting fixed disks and partitions.

Once you have finished making changes to this final wizard panel, the Framework Installation Settings Wizard is complete. Click **Finish** to save the package.

Saving the Framework Client Installer MSI

You will next be presented with the **Save MSI Package** dialog prompting you for a location to save the Framework Client installers that reflect the settings you have just made.

Figure 4-13 Save MSI Package, Framework Client



You must save the Framework installation packages in a shared network location such as the domain controller's SYSVOL folder if you intend to deploy the Symantec Endpoint Encryption client installer packages using a Software Installation GPO.

Note: Because you cannot load a previously created client installer package to examine what settings were used, you should save each client installer package using a descriptive name, such as "Framework Client Installer for Sales OU (27-Mar-08)". This is especially helpful if you plan to deploy multiple sets of packages throughout your organization.

To help manage installation packages, the individual settings chosen for a given installation package are saved in a date and time stamped log file (Example: FrameworkSettings 6_28_2010-18.21.59.log). The log file is created in the same location that you specified when saving the package. Since the log file does not show the contents of completed password fields, all passwords you specify in an installation package should be separately recorded and stored in a secure location.

Navigate to the directory location in which you want to save the output MSI packages and type the new MSI package name, or accept the default name Symantec Endpoint Encryption Framework Client.msi and click **Save**. Two MSI packages will be saved: one for 32-bit editions of Windows and one for 64-bit editions of Windows. The 64-bit package will be appended with _x64. Click **Yes** to create the MSI packages, then click **OK** in the confirmation dialog that is displayed.

Full Disk Installation Settings Wizard

Basics

This section shows how to run the wizard that lets you select client installation settings specific to Symantec Endpoint Encryption Full Disk. When you reach the final panel of the wizard, you will be prompted for a location to save the Full Disk installation settings MSI package.

Open the Manager Console, and in the left pane, expand the **Symantec Endpoint Encryption Software Setup** container, and click on **Full Disk**.

Startup

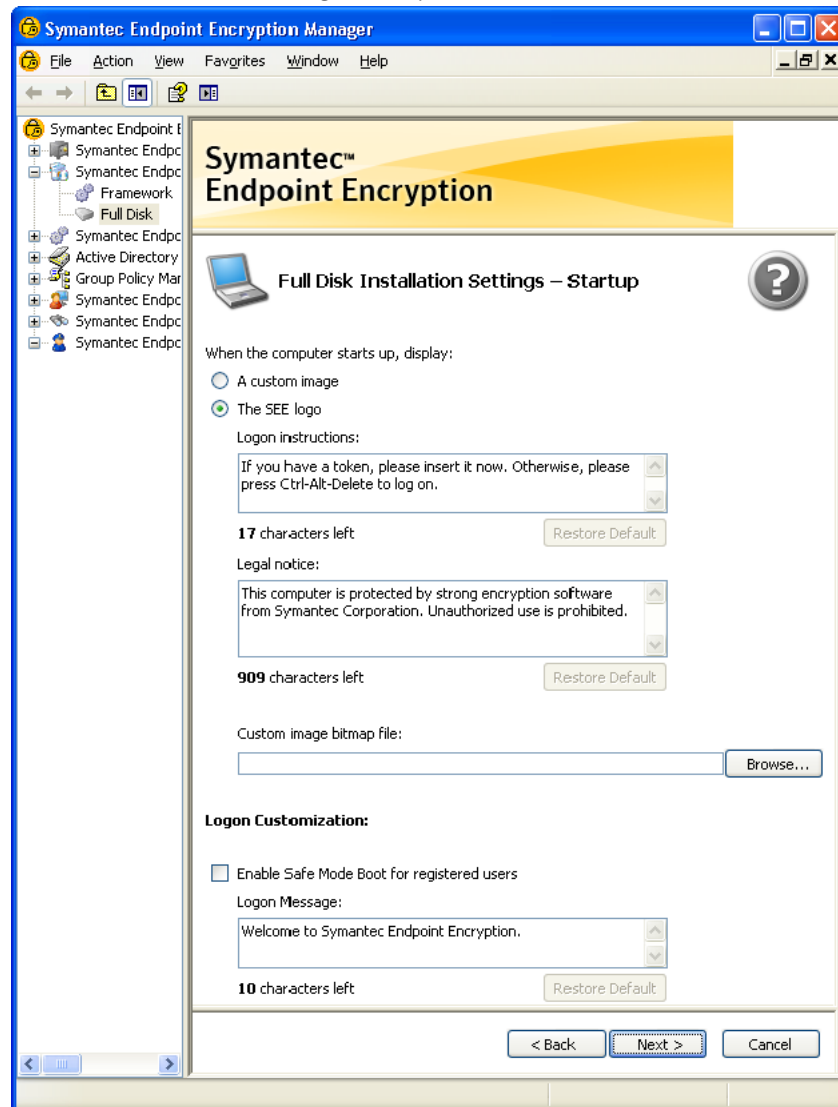
Basics

Use the Startup settings panel to customize the startup behavior on the Client Computer. You can specify:

- An optional graphics image displayed when Full Disk starts up.
- The logon instructions and legal notice messages displayed when Full Disk starts up.
- Whether registered users are allowed to start the Client Computer in safe mode.
- The logon message shown to registered users as they authenticate to Full Disk.

If you do not click **A custom image** and leave this panel at the default setting of **The SEE logo**, the Symantec Endpoint Encryption logo will be shown at startup. This default Symantec Endpoint Encryption logo will be overlaid with the text specified in the **Logon instructions** and **Legal notice** boxes.

Only the text in the **Logon instructions** box and **Legal notice** box will be included in the Mac client installation package. Custom images, safe mode boots, and logon messages are not supported for Mac clients.

Figure 4-14 Full Disk Installation Settings, Startup

Clicking the **Browse** button allows you to choose a BMP or PNG format graphics file to use for the custom startup image displayed on the Client Computer when Full Disk starts up. This image can be used to brand all Full Disk-protected Windows computers in your organization with your corporate logo, as well as for displaying a legal warning to those attempting to access a protected computer. If you do not select a custom image, the Symantec Endpoint Encryption logo will be used.

Note that a custom image can only be deployed as an installation setting, and cannot be added later on with a policy setting. A custom image could be effectively hidden at a later time by pushing out a Startup policy that causes the Symantec Endpoint Encryption logo to be displayed instead.

Guidelines for Creating a Custom Startup Image

Any image editing application which saves graphics files in the Windows Bitmap (BMP) or Portable Network Graphics (PNG) format can be used to create a custom image. One such application, Microsoft Paint (mspaint.exe), is included with Windows.

The dimensions of the custom image must be between 640 x 480 (VGA resolution) and 800 x 600 (SVGA resolution) pixels.

While the custom image can have a color depth of 8-bit (256-color or grayscale) or 24-bit (millions of colors), there is no guarantee that the display adapter of a Client Computer will start up in the highest color

depth it supports. A high bit-depth (24-bit) startup image may appear distorted when a Client Computer starts up in a lower color depth mode. For this reason, you may wish to limit the color depth of your custom image to 8-bit for maximum compatibility.

The custom image file must be no larger than 2,000,000 bytes in size.

16-bit color mode images are not supported.

Windows bitmap files must be saved as uncompressed. OS/2 BMP formats are not supported.

Note: If the user authenticates with a password, your custom image must contain text directing the user to press the CTRL+ALT+DELETE keys to log on to the computer. If you omit these instructions, the user may be unsure of how to log on.

Select the **Enable Safe Mode Boot for registered users** check box to allow registered users to start their desktop computers in safe mode.

Text you specify in the **Logon Message** box will be shown to registered users as they authenticate to Full Disk. Note that a custom logon message can only be deployed as an installation setting, and cannot be added later on with a policy setting.

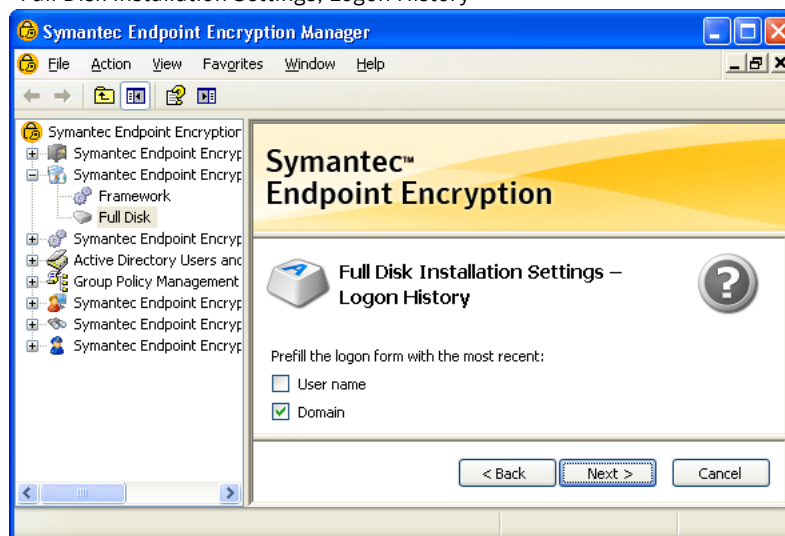
Click **Next** to advance to the Logon History panel.

Logon History

Use the Logon History settings panel to specify whether to prefill the Symantec Endpoint Encryption logon screen with the name and domain of the most recently logged on user.

The settings from the Logon History panel will not be included in the Mac client installation package.

Figure 4-15 Full Disk Installation Settings, Logon History



Selecting the **User name** check box allows users to see the name and domain of the last user who logged on at the Symantec Endpoint Encryption pre-Windows logon screen. This will reduce the security of your Client Computers, so Symantec recommends deselecting both the **User name** and **Domain** check boxes.

Note: If you are deploying Full Disk to computers operated by visually impaired users who will be using audio cues in pre-Windows, ensure that the User name check box is deselected and that the Domain check box is selected. This will allow the user to log on using the audio cues.

Click **Next** to advance to the Encryption panel.

Encryption

Initial encryption takes place transparently in the background, allowing users to continue working normally while fixed disks and partitions are being encrypted.

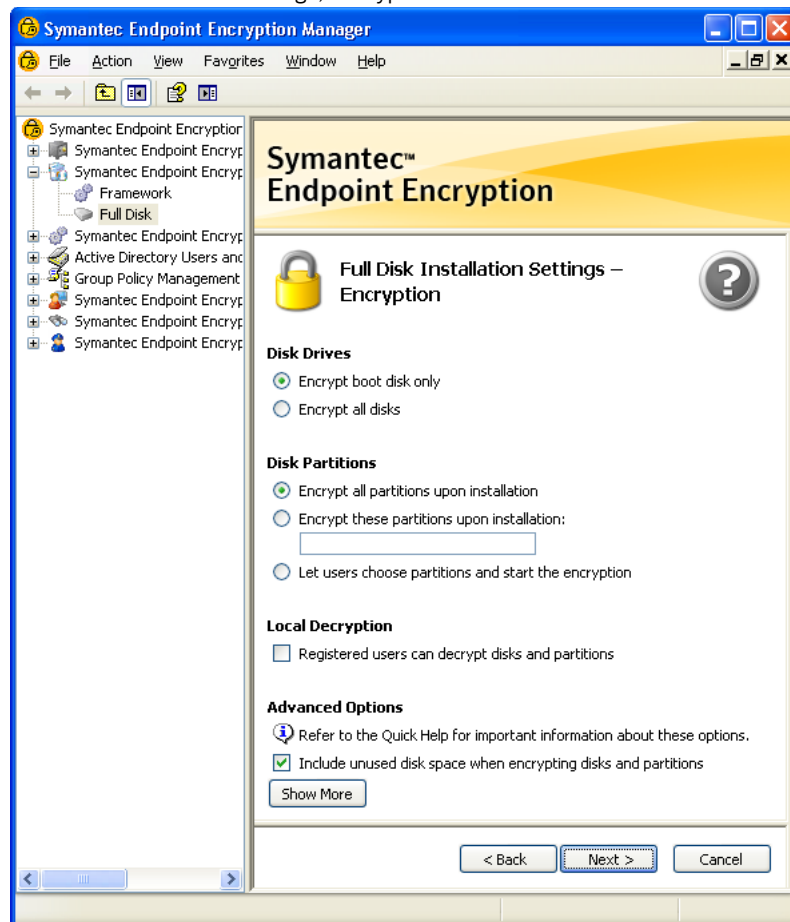
Note: The settings on this panel do not apply to Opal-compliant drives. Opal-compliant drives are always encrypted.

Use the Encryption panel to specify which fixed disks and partitions on the Client Computer will be encrypted, whether initial encryption will begin immediately or can be initiated by users, and whether unused sectors will be encrypted. Further advanced options are available which affect encryption/decryption time. This panel also allows you to specify whether registered users will be allowed to decrypt an encrypted disk or partition.

Note: These installation settings cannot be changed by policy or upgrade package.

On the Mac, encryption must be initiated manually, using a user account. The settings in the Encryption panel will not be included in the Mac client installation package.

Figure 4-16 Full Disk Installation Settings, Encryption



The **Disk Drives** section allows you to choose whether to encrypt just the boot disk or all of the fixed disks that reside on the Client Computer.

The **Disk Partitions** section lets you specify the partitions on the specified drive(s) that should be encrypted, or whether to leave it up to the user.

- Select the **Encrypt all partitions upon installation** option to ensure that all partitions on the specified drive(s) are encrypted. Encryption will begin as soon as the computer reboots after installation.
- Select the **Encrypt these partitions upon installation** option to specify up to 26 individual partitions to encrypt, from A–Z. Encryption will begin as soon as the computer reboots after installation.
- Select the **Let users choose partitions and start the encryption** option, users can select the individual partitions to encrypt on the specified drive(s) by accessing the **Encryption** panel of the User Client Console. Note that this option allows users to defer the initial encryption process.

Use the **Local Decryption** area to specify whether registered users are allowed to decrypt local disk partitions. Select the **Registered users can decrypt disks and partitions** option in the **Local Decryption** section to allow registered users will be able to decrypt disks or partitions by accessing the **Decryption** panel of the User Client Console.

Use the **Advanced Options** area to select whether to encrypt all portions of the drive including empty sectors and sectors containing deleted data. If you select this option, the entire disk or partition will be encrypted, including any disk sectors marked as unused, but which may still contain previously erased data. Use this option when deploying Full Disk to computers which have already been in service and whose hard disk sectors may contain deleted data. This option increases the amount of time necessary to complete the initial encryption operation. Click **Show More** to reveal the following advanced options:

- **Include unused disk space when encrypting partitions** ensures that all of the partition sectors will be encrypted, including any marked as “unused” that may still contain previously erased data. This setting increases the amount of time necessary to complete the initial encryption operation. Keep this option on for recipient computers that have already been in service. You may turn it off if the recipient computers are new.
- **Double-write sectors during partition encryption or decryption** guards against the remote possibility of losing a single data sector if power to the hard disk is interrupted at the exact moment the disk is physically writing to the sector. Selecting this option causes every data sector to be double-written during partition encryption or decryption and requires ten to twenty times as long to complete. Note that selecting this option does not affect the performance of on-the-fly encryption and decryption. Power loss protection is always enabled during partition encryption and decryption, and is not affected by this option. Should the computer power down or enter sleep or hibernation mode, the encryption or decryption process will continue automatically when power is restored.
- **Protect against cold boot attack** addresses a type of side channel attack in which an attacker with physical access to a computer is able to retrieve encryption keys from a running operating system by cold booting the machine. The attack relies on the data remanence property of DRAM and SRAM to retrieve memory contents seconds to minutes after power has been removed.

Click **Next** to advance to the Installer Customization panel.

Installer Customization

Use the Installer Customization settings panel to allow the client database files to be installed in their default location on the Client Computer (recommended), or else specify an alternate location (advanced). The client database files cannot be installed on removable media or on a secondary physical hard disk.

The settings from the Installer Customization panel will not be included in the Mac client installation package.

Figure 4-17 Full Disk Installation Settings, Installer Customization

By default, the client database files will be stored on the same partition as the Windows operating system.

Note: If the target computer has an Opal-compliant boot drive, ensure that Default is selected. Symantec does not support the selection of Custom for computers with Opal-compliant boot drives.

Select the **Custom** option to specify a fixed disk or partition other than the system disk or partition and/or to place the client database files inside of a subdirectory. Type the letter of the alternate fixed disk or partition in the box and/or the desired subdirectory structure. The client database files must be installed on the same physical drive that the Windows operating system resides on. If the installer is unable to store the client database files on the drive typed in the box, it will deposit them in the system partition.

Note: Full Disk uses the client database files for its internal operations. Once installed, the client database files should never be moved.

Click **Next** to advance to the next panel of the wizard, the Hardware Configuration panel.

Hardware Configuration

Do not modify any settings in the Hardware Configuration panel without referring to the Symantec Endpoint Encryption knowledge base:

http://www.symantec.com/business/support/index?page=content&key=55414&channel=TECHNICAL_SOLUTION

Note: Incorrect settings in the Hardware Configuration panel can render computers unbootable.

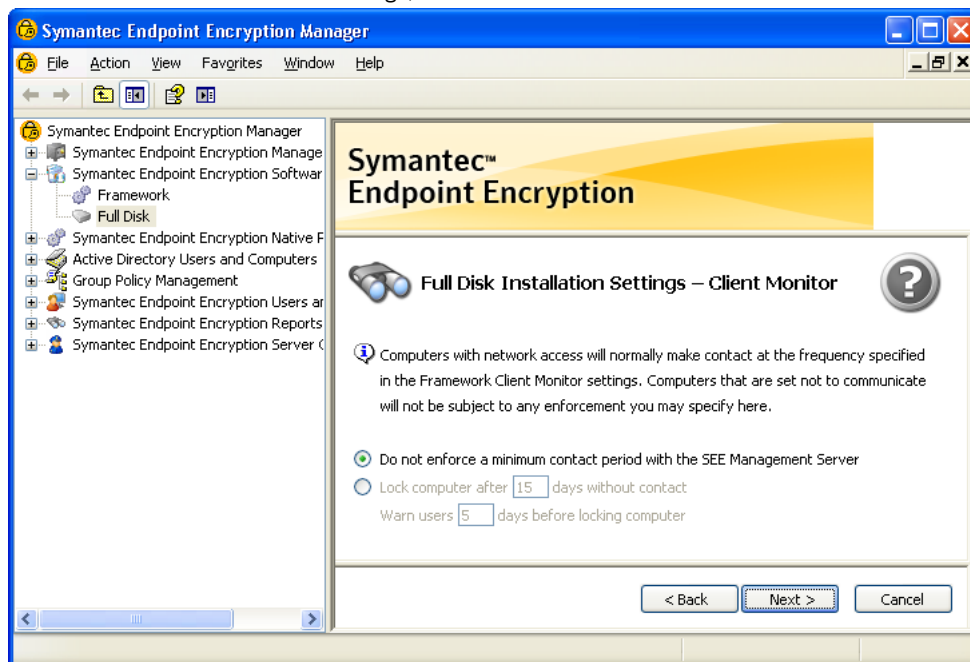
Click **Next** to advance to the final panel of the wizard, the Client Monitor panel.

Client Monitor

Use the Client Monitor settings panel to force a Full Disk-protected computer to periodically report its status. If contact is not made within the designated interval, users will be locked out and unable to access their computers.

The settings from the Client Monitor panel will not be included in the Mac client installation package.

Figure 4-18 Full Disk Installation Settings, Client Monitor



Click **Do not enforce a minimum contact period with the Symantec Endpoint Encryption Management Server** if you do not want to enforce regular network contact.

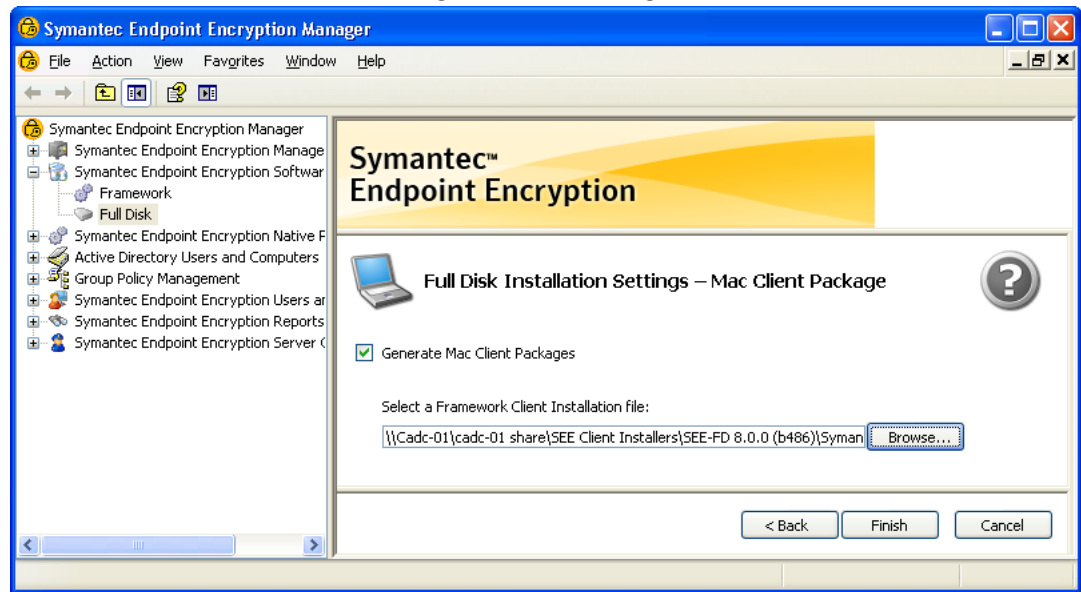
Click **Lock computer after** to force a computer lockout after a specified number of days without network contact. If you select this option, you can specify the number of days a computer may remain without network contact, from 0–365. You can also specify how many days in advance, from 0–365, that users will be warned to connect to the network and avoid a lockout.

Note that the values you type in these two boxes are validated to ensure that users will always be warned prior to a lockout. For example, you will be prevented from specifying that the computer should be locked after five days without contact, and that the users should be warned 15 days before being locked out. If this case were allowed, the user could run the risk of being locked out 10 days before the warning is displayed.

Click **Next** to advance to the Mac Client Package panel.

Mac Client Package

Use the Mac Client Package panel to generate a client installation package suitable for Macs.

Figure 4-19 Full Disk Installation Settings, Mac Client Package

If you don't want to generate a Mac package at this time, deselect **Generate Mac Client Packages**.

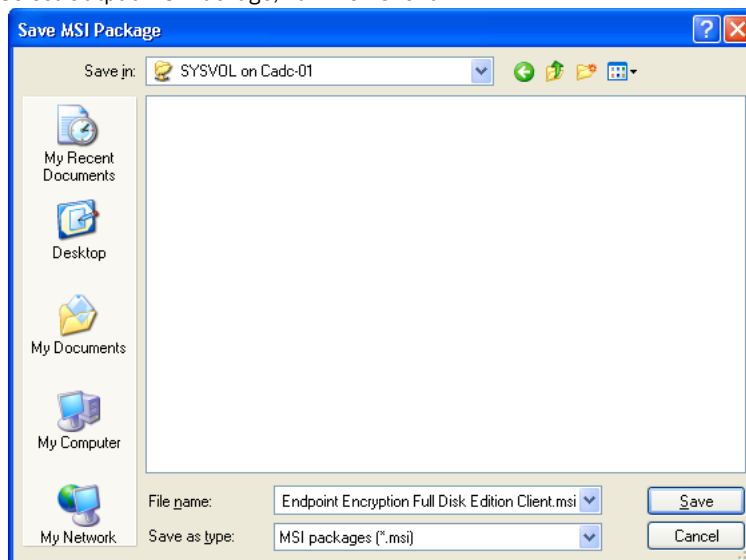
To generate a client installation package for Macs, leave **Generate Mac Client Packages** selected. Then click **Browse** and navigate to the location of the Framework MSI.

Once you have completed your selections, click **Finish**.

Saving the Full Disk Client Installer MSI

Once you have finished making changes to this final panel, the Symantec Endpoint Encryption Full Disk Installation Settings Wizard is complete. When you click **Finish**, a dialog box appears prompting you for a location to save the Symantec Endpoint Encryption Full Disk client installers which reflect the settings you have just made.

Figure 4-20 Select Output MSI Package, Full Disk Client



Note: You must save the Full Disk client installer packages in a shared network location, such as the domain controller's SYSVOL folder, if you intend to deploy the Symantec Endpoint Encryption client installer packages using a Software Installation GPO. Symantec Corporation recommends that you accept the default package name. The Microsoft Windows Installer (MSI) has a limitation when performing minor upgrades that requires the new package name to be exactly the same as the name of the originally installed package.

To help manage installation packages, the individual settings chosen for a given installation package are saved in a date and time stamped log file (Example: FullDiskSettings 6_28_2011-18.25.1.log). The log file is created in the same location that you specified when saving the package. Since the log file does not store the contents of completed password fields, any passwords you specify in an installation package should be securely archived elsewhere.

Navigate to the directory location in which you want to save the output MSI package, accept the default name Symantec Endpoint Encryption Full Disk Edition Client.msi, and click **Save**. Two MSI packages will be saved: one for 32-bit editions of Windows and one for 64-bit editions of Windows. The 64-bit package will be appended with **_x64**. If you chose to generate a Mac client installation package, a ZIP file will also be created. Click **Yes** to create the MSI packages, then click **OK** in the confirmation dialog that is displayed.

Client Installations

This chapter includes the following topics:

- [Overview](#)
- [Manual Mac Client Installations](#)
- [Deploying Client Installer Packages](#)
- [Manual Client Installations](#)

Overview

Basics

This section describes how to install a new deployment of the Symantec Endpoint Encryption client software.

Windows Clients

Client installation can be accomplished from either a central location (see [“Deploying Client Installer Packages”](#) on page 76) or from the local computer (see [“Manual Client Installations”](#) on page 79).

You can install the Symantec Endpoint Encryption client software using any of the following methods:

- Installation using a third-party deployment tool (recommended) ([“Third-Party Tool Deployment”](#) on page 76),
- Installation from Active Directory using a software installation computer policy ([“Group Policy Deployment”](#) on page 77), or
- Manual installation by double-clicking the client installer packages at the Client Computer ([“Manual Client Installations”](#) on page 79).

MSI packages represent a target for analysis in that they are unencrypted and can be intercepted in transit. Symantec recommends using a third party deployment tool with features to protect the MSI packages.

At the conclusion of the installation package creation wizard, two MSI packages will be created. Both will contain the same settings, but one will be appropriate for 64-bit systems and the other appropriate for 32-bit systems. The package appropriate for 64-bit systems will contain _x64 at the end of its file name, e.g., Symantec Endpoint Encryption Framework Client_x64.msi. You can either deploy both packages to all clients or deploy 32-bit packages to 32-bit clients and 64-bit packages to 64-bit clients. A Symantec Endpoint Encryption client installer package will fail to install on a computer running an incompatible version of Windows.

Regardless of the deployment method, the Framework client installer package must be installed before the Full Disk package.

Note: Symantec recommends that you defragment all fixed disks and partitions on the Client Computer prior to installation of Symantec Endpoint Encryption Full Disk.

Mac Clients

The Mac client installation package must be executed from the Mac client ("[Manual Mac Client Installations](#)" on page 76 for instructions).

Manual Mac Client Installations

To install Symantec Endpoint Encryption Full Disk on a Mac client, complete the following steps.

To perform this procedure

- 1 Ensure that the Mac client can access the Mac client installation package (Symantec Endpoint Encryption Full Disk Edition Client_MAC.zip), either by placing it on a network share or on removable media.
- 2 Log on to the Mac client using an account with administrative privileges.
- 3 Close all applications.
- 4 Double-click the Symantec Endpoint Encryption Full Disk Edition Client_MAC.zip file.
- 5 Open the pgpdesktop directory.
- 6 Double-click PGP.pkg.
- 7 Click through the pages of the installation wizard.
- 8 Provide administrative credentials when prompted.
- 9 You will be notified that the computer will be restarted to complete the installation. Click **Continue Installation**.
- 10 Once the installation concludes successfully, click **Restart**.
- 11 You may receive a **Certificate Trust** prompt after the Mac restarts. Provide administrative credentials and accept the changes.

Deploying Client Installer Packages

Third-Party Tool Deployment

Basics

Installation of the Symantec Endpoint Encryption client packages can be accomplished using any third-party deployment tool that supports the MSI format. To avoid installation errors, make sure that when you create the client installer packages that you save them to a local hard disk or other volume which has **Full Control** permissions set. The client installer packages can then be copied to removable media, a network volume accessible to the client, or the local hard disk of the Client Computer. For large scale deployments, you can use the command-line method as a basis for scripted installations.

Note: Framework must be installed first.

Syntax

To execute the appropriate MSI, the following syntax should be used:

MSIEXEC /i "[path]\name of client installation package.msi" parameter

Table 5-1 describes the parameters and variables in greater detail.

Table 5-1 MSIEXEC Variables and Parameters for Installations

Variables/Parameters	Description	Default(s)/Example(s)
[path]	The local or network path where the MSI resides. Path is optional when the MSI file is executed from the current directory.	\\CADC-01\SYSVOL\PACKAGES\
name of client installation package.msi	The name of the MSI file you wish to execute	Symantec Endpoint Encryption Framework Client.msi Symantec Endpoint Encryption Framework Client_x64.msi Symantec Endpoint Encryption Full Disk Edition Client.msi Symantec Endpoint Encryption Full Disk Edition Client_x64.msi
parameter	The MSIEXEC parameter to be used	/q /qb /q /norestart* /q REBOOT=ReallySuppress

* Not available in MSIEXEC 2.0.

Examples

The following lines could be placed in a batch file to accomplish the installation of **Full Disk**.

MSIEXEC /i "\\CADC-01\SYSVOL\PACKAGES\Symantec Endpoint Encryption Framework Client_x64.msi" /q REBOOT=ReallySuppress

MSIEXEC /i "\\CADC-01\SYSVOL\PACKAGES\Symantec Endpoint Encryption Full Disk Edition Client_x64.msi" /q

Group Policy Deployment

This section describes how to use Active Directory's software distribution capabilities to push client installation packages out to the Client Computers for automatic installation.

Note: When using Active Directory to deploy client installer packages, you must create separate GPOs for 32-bit and 64-bit packages. Never mix 32-bit and 64-bit client packages in the same GPO.

Note: When using Active Directory to deploy the client installer packages, they must be installed as part of a software installation computer policy and not as part of a software installation user policy.

To perform this procedure

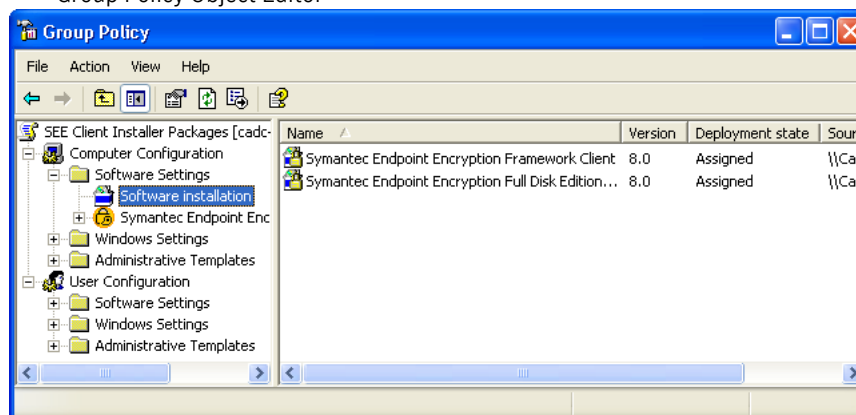
- 1 Open the Manager Console. In the left-hand navigation pane, click the Group Policy Management container and expand the entire container hierarchy to reveal the Group Policy Objects container.
- 2 Right-click **Group Policy Objects** and select **New**. A New GPO window displays. Type **SEE Client Installer Packages** in the **Group Policy Object** box and click **OK** to save the new policy. Right-click the new policy and choose **Edit**. The Group Policy Object Editor will display.
- 3 Expand **Computer Configuration**, **Software Settings**, then **Software installation**.

- 4 Right-click **Software Installation** and select **New** then **Package**. Click **My Network Places**, and navigate to the Microsoft Windows Network\your-org\Cadc-01\SYSVOL location or alternate location where you previously saved the two Symantec Endpoint Encryption client packages.

Note: If you do not select the install packages by navigating to them using My Network Places, Client Computers receiving the policy will be unable to locate the install packages and the software installation policy will fail to be applied.

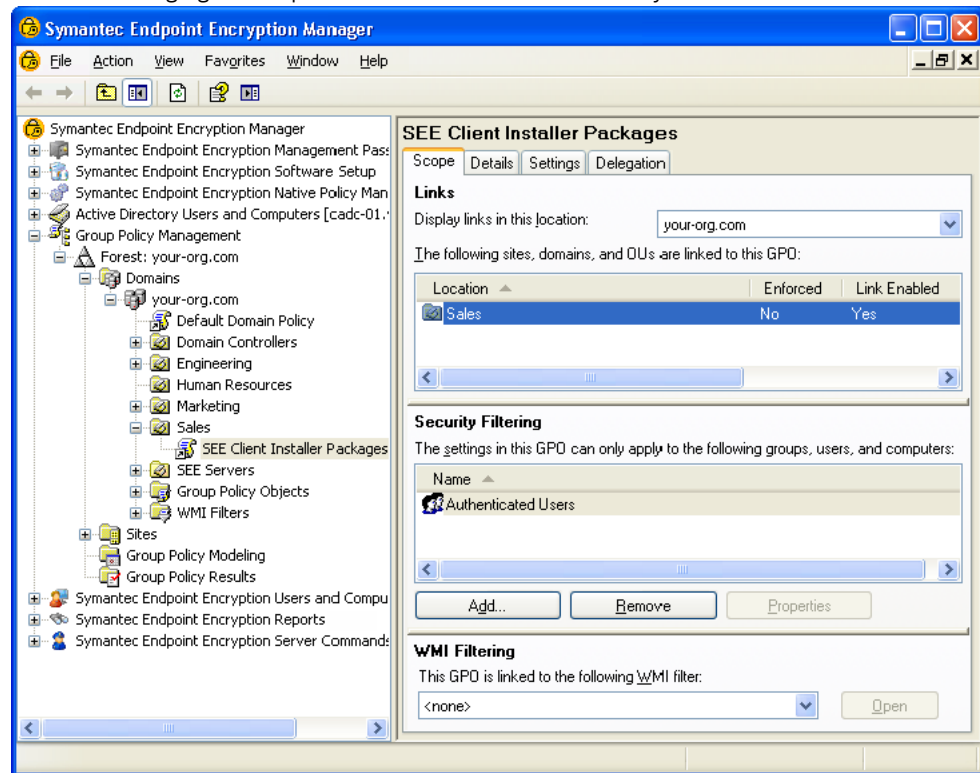
- 5 Select the Framework Client package, and click **Open**.
- 6 A confirmation screen will appear. Click **OK** to accept the default value of **Assigned** for that package.
- 7 Right-click **Software Installation** and select **New** then **Package**. Click **My Network Places**, and navigate to the Microsoft Windows Network\your-org\Cadc-01\SYSVOL location or alternate location where you previously saved the two Symantec Endpoint Encryption client packages.
- 8 Select the Full Disk Client package, and click **Open**.
- 9 A confirmation screen will appear. Click **OK** to accept the default value of **Assigned** for that package.

Figure 5-1 Group Policy Object Editor



- 10 Close the Group Policy Object Editor.
- 11 In the Manager Console, select the group policy you just created, then drag the group policy and drop it into the organizational unit (OU) or other object containing the computers you are deploying the client installer packages to.
- 12 A confirmation dialog appears. Click **OK** to confirm linking the policy to the specified location.

Figure 5-2 Changing the Scope of the Software Installation Policy



The new Group Policy, SEE Client Installer Packages, is now linked to the domain your-org.com as shown in Figure 5.2.

Once the software installation GPO has been linked, it can take between 90 and 120 minutes before it is processed by a Client Computer connected to the domain. In addition to this policy processing delay, the Client Computer must be restarted to begin the installation.

Note: Some users simply log off rather than perform a complete shut down, resulting in computer policies not being fully processed. Best practices can help mitigate this condition. For example, you can implement scripts to either periodically restart the Client Computer during off-peak hours or when a user logs off.

To accelerate the GPO update process and to initiate a manual restart, refer to the *Policy Administrator Guide*.

After the software installation computer policy has been applied and the Client Computer has been restarted, the Framework and the Full Disk installations will begin.

Depending on the MSIEXEC parameters specified, the Client Computer can automatically restart when the client packages have finished installing.

Manual Client Installations

Basics

In cases where only a few clients need to be installed or an infrastructure-based deployment is impractical, the Symantec Endpoint Encryption client software can be manually installed on individual Client Computers by executing the Framework and then the Full Disk client installer packages.

To perform this procedure

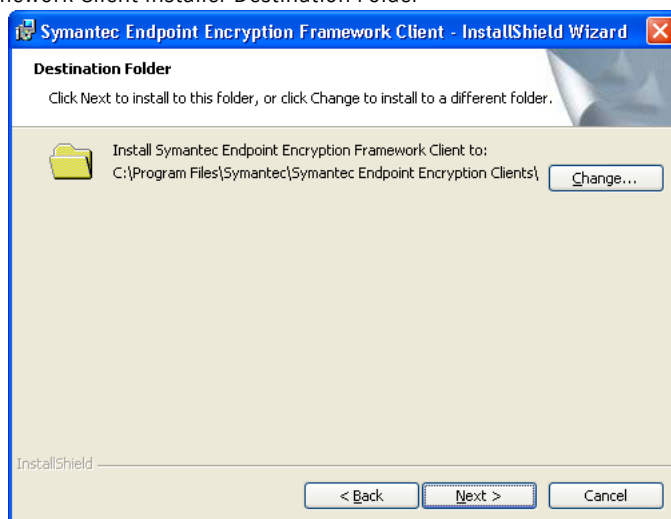
- 1 Determine whether the Client Computer is running a 32-bit version of Windows or a 64-bit version of Windows.
- 2 Locate the Framework and Full Disk client installation packages appropriate to the version of Windows running on the Client Computer. The package appropriate for 64-bit systems will contain _x64 at the end of its file name, e.g., Symantec Endpoint Encryption Framework Client_x64.msi.
- 3 Ensure that the client installation packages are accessible to the Client Computer, either from a network share or removable media.
- 4 Log on to the target computer using an administrator account possessing sufficient rights for installing software.

Framework Install

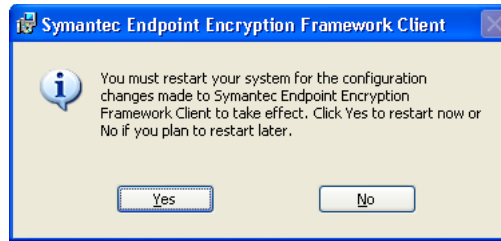
To perform this procedure

- 1 Navigate to the file Framework client installation package (e.g., Symantec Endpoint Encryption Framework Client.msi or Symantec Endpoint Encryption Framework Client_x64.msi) and double-click. The InstallShield Wizard for Framework Client will launch.
- 2 Click **Next**. The **Destination Folder** page will display.

Figure 5-3 Framework Client Installer Destination Folder



- 3 Click **Change** to install the client to a location other than the default. Click **Next** to install the Framework Client to the location shown. The **Ready to Install the Program** page will display.
- 4 The installation can now begin. This is your last chance to change the installation location you established in the previous screens. Use the **Back** button to review and select a different installation location if necessary. Once you are satisfied and are ready to begin the installation, click **Install**. The **Installing Framework Client** page will display.
- 5 The InstallShield Wizard will display status information during the installation process and will display a success confirmation screen once the installation process has successfully completed.
- 6 Click **Finish** to exit the InstallShield wizard.
- 7 The Symantec Endpoint Encryption installer will display an alert dialog prompting you to restart.

Figure 5-4 Framework Client Installer Restart

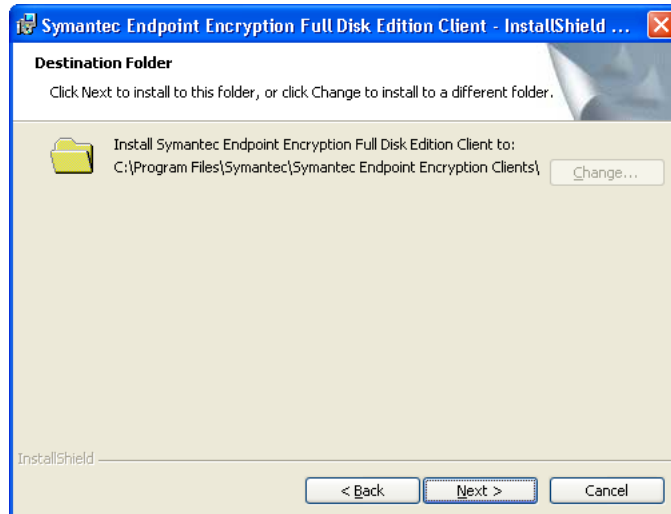
- 8 Click **No** to defer system restart until after you have completed installation of the Full Disk Client in the following steps.

With the Framework client package now installed, you can now install the Full Disk Client package.

Full Disk Install

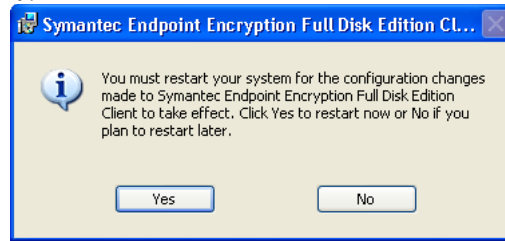
To perform this procedure

- 1 Navigate to the Full Disk client installation package (e.g., Symantec Endpoint Encryption Full Disk Edition Client.msi or Symantec Endpoint Encryption Full Disk Edition Client_x64.msi) and double-click. The InstallShield Wizard for Symantec Endpoint Encryption Full Disk Edition Client will launch.
- 2 Click **Next**. The InstallShield Wizard will display the **Destination Folder** page.

Figure 5-5 Full Disk Client Installer Destination Folder

- 3 The Full Disk Client installer uses the installation location specified during installation of the Framework. The **Change** button will be unavailable. Click **Next**. The **Ready to Install the Program** page will display.
- 4 Click **Install**. The **Installing Symantec Endpoint Encryption Full Disk Client** page will display.
- 5 The InstallShield Wizard will display status information during the installation process and will display a success confirmation screen once the installation process has successfully completed.
- 6 Click **Finish** to exit the InstallShield wizard.
- 7 The Symantec Endpoint Encryption installer will display an alert dialog prompting you to restart.

Figure 5-6 Full Disk Encryption Client Installer Restart



8 Click **Yes** if you are finished installing all software, or click **No** to defer system restart until later.

Once the computer has restarted, Full Disk will be fully installed. Note that depending on the values chosen for the authentication method and grace restarts option (available in the Framework Installation Settings – Registered Users settings panel), users may be immediately forced to register for a Symantec Endpoint Encryption account at the next Windows login. For information about the grace restarts option, see [“Registered Users”](#) on page 54.

Upgrades

This chapter includes the following topics:

- [Overview](#)
- [Symantec Endpoint Encryption Management Server](#)
- [Symantec Endpoint Encryption Manager](#)
- [Upgrading Windows Clients](#)
- [Upgrading Mac Clients](#)

Overview

This chapter describes how to upgrade to the latest version. Upgrades must be performed in the following sequence:

- 1 Symantec Endpoint Encryption Management Server ([“Symantec Endpoint Encryption Management Server”](#) on page 83),
- 2 Manager Console ([“Symantec Endpoint Encryption Manager”](#) on page 89), and
- 3 Symantec Endpoint Encryption Client Computers ([“Upgrading Windows Clients”](#) on page 92 and [“Upgrading Mac Clients”](#) on page 96).

Symantec Endpoint Encryption Management Server

Basics

Upgrades of the Management Server differ according to the type of database utilized by the version you are upgrading from.

- Active Directory Application Mode (ADAM) database—Symantec Endpoint Encryption version numbers less than 7.0.0 and GuardianEdge Framework version numbers less than 9.2.0 utilize an ADAM database. Refer to [“From Versions that Utilize an ADAM Database”](#) on page 86.
- SQL database—Symantec Endpoint Encryption version numbers that are equal to or greater than 7.0.0 and GuardianEdge Framework version numbers that are equal to or less than 9.2.0 rely on an SQL database. If you are upgrading from a version that utilizes an SQL database, continue to the next section.

Note: Before you begin, back up your database.

For the upgrade to be successful, ensure that the custom database name does not contain the “GEMSDb” string concatenated to it using special characters. For example, if the custom database name is GEMSDb_abc or abc@GEMSDb, the upgrade will not be successful. However, if the database name is GEMSDbabc or abcGEMSDb, the upgrade will succeed.

From Versions that Utilize an SQL Database

Basics

If you only have one Management Server, skip to “[Single Management Server](#)” on page 84. Otherwise, continue to the next section.

Preliminary Steps For Multiple Management Servers

If you have multiple Management Servers, perform the following steps:

- 1 Open the **Internet Information Service (IIS) Manager** snap-in. Expand the Management Server computer. For Windows Server 2003, expand **Web Sites**, right-click **Symantec Endpoint Encryption Services** or **GuardianEdge Services** and click **Stop**. For Windows Server 2008, expand **Sites**, right-click **Symantec Endpoint Encryption Services** or **GuardianEdge Services**, point to **Manage Web Site** and click **Stop**.
- 2 Verify that the web service is stopped. For Windows Server 2003, the text of web site **Symantec Endpoint Encryption Services** or **GuardianEdge Services** will change to **Symantec Endpoint Encryption Services (Stopped)** or **GuardianEdge Services (Stopped)** to indicate that the web service has stopped. For Windows Server 2008, the icon of web site **Symantec Endpoint Encryption Services** or **GuardianEdge Services** will change to indicate that the web service has stopped.
- 3 Open the Configuration Manager, located on the Management Server at C:\Program Files\Symantec\Symantec Endpoint Encryption Management Server\Services\Symantec.Endpoint.Encryption.ConfigManager.exe.
If you are upgrading a GuardianEdge installation, the Configuration Manager is located at C:\Program Files\GuardianEdge\Management Server\Services\GuardianEdge.GEMSConfigManager.exe.
The Configuration Manager is displayed.
- 4 Click the **Directory Sync Service Status** tab. The current status of synchronization will be shown under the **Active Directory** and **Novell eDirectory** sections. A status of **Running** indicates that the particular synchronization service is active. For each active synchronization service, click **Stop** to stop the synchronization service. The status for that synchronization service will change to **Stopped**.

Proceed to the next section, which discusses how to upgrade a single Management Server. Each of your Management Servers should be upgraded simultaneously, or as soon as possible in sequence.

Single Management Server

If your database upgrade account (Chapter 1 “[Required Accounts](#)” on page 11) is a Windows account, log on to the Management Server using this account. This account must have read and write permissions to the database.

If you are upgrading Windows server 2008 or later, click the **Start** button. Expand **Accessories**. Right-click **Command-prompt**. Select **Run as administrator**. Provide the credentials of a domain administrator account with sufficient rights for installing software at the prompt.

Note: GuardianEdge Framework versions prior to 9.4.0 and Symantec Endpoint Encryption versions prior to 7.0.4 do not support Windows Server 2008. Therefore, if you upgrade the operating system prior to upgrading the Symantec Endpoint Encryption Management Server, your system could experience failure. Ensure that you upgrade to GuardianEdge Framework 9.4.0 or later or Symantec Endpoint Encryption 7.0.4 or later prior to upgrading the operating system.

To upgrade from a version that utilizes an SQL database, execute Symantec Endpoint Encryption Management Server.msi from the command line or by double-clicking the file.

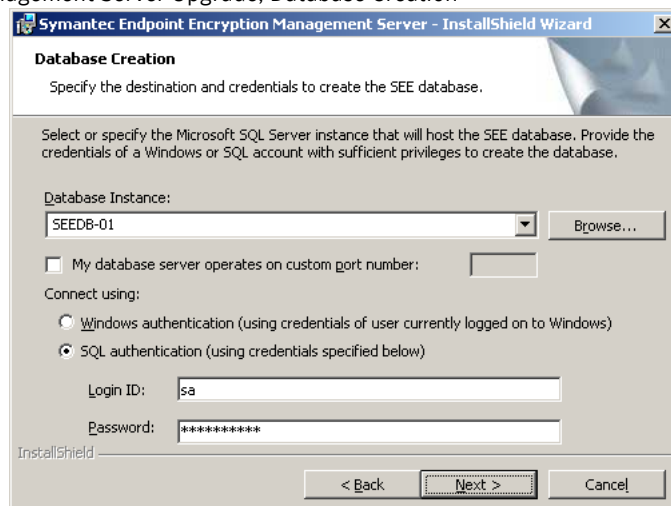
The installer will detect the presence of a previous version of the Management Server and the **Welcome to the Upgrade Wizard for Symantec Endpoint Encryption Management Server** page appears. Click **Next**.

Figure 6-1 Management Server Upgrade, Welcome



The **License Agreement** page appears. Select the option **I accept the terms in the license agreement**, then click **Next**. The **Database Creation** page appears.

Figure 6-2 Management Server Upgrade, Database Creation



Click **Browse** to select the database instance on which your existing Symantec Endpoint Encryption database resides from a list of available instances, or type the NetBIOS name of the instance.

If your database server has been configured to use a custom port, select the **My database server operates on a custom port** check box and type the port number.

The **Connect using** section allows you to select the database upgrade account (see [“Required Accounts”](#) on page 11). If your database upgrade account is a Windows account and you are logged on using this account, use the default setting of **Windows authentication**. If your database creation account is an SQL account, select **SQL authentication** and type the account credentials in the **Login ID** and **Password** boxes.

Note: If you have multiple Management Servers, ensure that all the parameters on this page are identical to those specified during installation.

Click **Next**.

The installer will attempt to authenticate to the instance.

If you are upgrading from an installation of the GuardianEdge Management Server, the **Destination Folder** page will appear, allowing you to choose the location of your Symantec Endpoint Encryption Management Server installation files. Click **Change** to choose a different location to install the Symantec Endpoint Encryption Management Server files, or click **Next** to accept the default installation location.

The **Ready to Install Program** page will appear. Click **Install**.

During the upgrade process, only the database schema will be updated. All existing data will remain unchanged.

After the **Symantec Endpoint Encryption Management Server InstallShield Wizard Completed** page appears, click **Finish**.

Note: If you are upgrading multiple Management Servers, do not use the Configuration Manager until all Management Servers have been upgraded.

Concluding Steps for Multiple Management Servers

Once you have upgraded all of your Management Servers, complete the following steps:

- 1 Open the **Internet Information Service (IIS) Manager** snap-in. Expand the Management Server computer. For Windows Server 2003, expand **Web Sites**, right-click **Symantec Endpoint Encryption Services** or **GuardianEdge Services** and click **Start**. For Windows Server 2008, expand **Sites**, right-click **Symantec Endpoint Encryption Services** or **GuardianEdge Services**, point to **Manage Web Site** and click **Start**.
- 2 Verify that the web service has started. For Windows Server 2003, the text of the web site will change from **Symantec Endpoint Encryption Services (Stopped)** or **GuardianEdge Services (Stopped)** to **Symantec Endpoint Encryption Services** or **GuardianEdge Services** to indicate that the web service has started. For Windows Server 2008, the icon of web site **Symantec Endpoint Encryption Services** or **GuardianEdge Services** will change to indicate that the web service has started.
- 3 Open the Configuration Manager, located on the Management Server at C:\Program Files\Symantec\Symantec Endpoint Encryption Management Server\Services\Symantec.Endpoint.Encryption.ConfigManager.exe. If you are upgrading a GuardianEdge installation, the Configuration Manager is located at C:\Program Files\GuardianEdge\Management Server\Services\GuardianEdge.GEMSConfigManager.exe. The Configuration Manager is displayed.

Click the **Directory Sync Service Status** tab. The current status of synchronization will be shown under the **Active Directory** and **Novell eDirectory** sections. A status of **Stopped** indicates that the particular synchronization service is inactive. For each synchronization service that you require, click **Start** to start the synchronization service. The status for that synchronization service will change to **Running**.

From Versions that Utilize an ADAM Database

Basics

If you are upgrading from a version that utilizes an ADAM database, you must migrate critical encryption keys from the SEE Server or GuardianEdge Server (ADAM) to the Symantec Endpoint Encryption database (SQL).

Note: If you do not successfully migrate the encryption keys from the SEE Server/GuardianEdge Server to the Symantec Endpoint Encryption database before creating client upgrade packages, your upgraded clients will be unable to communicate with the Symantec Endpoint Encryption Management Server.

The steps for upgrading the SEE Server/GuardianEdge Server to the Symantec Endpoint Encryption Management Server follow:

- 1 Ensure that your SEE Server/GuardianEdge Server is and remains operational throughout the procedure.
- 2 Install the Symantec Endpoint Encryption Management Server (Chapter 2 “[Installing the Symantec Endpoint Encryption Management Server](#)” on page 17).
- 3 Copy the key exporter script from the Symantec Endpoint Encryption Management Server to the SEE Server or GuardianEdge Server.
- 4 If your database creation account (Chapter 1 “[Required Accounts](#)” on page 11) is a Windows account, log on to the Symantec Endpoint Encryption Management Server using this account.
- 5 Run the key exporter script.
- 6 Verify that the critical keying data was successfully migrated to the Symantec Endpoint Encryption database.
- 7 Install the Symantec Endpoint Encryption Manager, and create and deploy the client upgrade packages.

The remainder of this section details how to run the key exporter script and verify its success (steps 4 and 5).

Prerequisites

Your default script host must be set to either cscript or wscript. Before running the script, make sure you have the following information:

- The NetBIOS name or IP address of the computer hosting the Symantec Endpoint Encryption database;
- If the default instance name was not used during installation of Microsoft SQL Server, the name that was used;
- The ADAM Admin credentials of your existing ADAM-based SEE Server or GuardianEdge Server;
- The Windows or SQL credentials of a user with administrative privileges for the Symantec Endpoint Encryption database;
- The port number of the ADAM instance;
- The distinguished name (DN) of the ADAM instance’s application partition.

Running the Key Exporter Script

The key exporter script must be run from the ADAM-based SEE Server or GuardianEdge Server. Do not run the key exporter script multiple times. The script should be run only once.

To perform this procedure

- 1 Log on to the Symantec Endpoint Encryption Management Server and locate the key exporter script, KeyExport.vbs.
On 32-bit versions of Windows Server, the script will be located in C:\Program Files\Symantec\Symantec Endpoint Encryption Management Server\Services.
On 64-bit versions of Windows Server, the script will be located in C:\Program Files (x86)\Symantec\Symantec Endpoint Encryption Management Server\Services.
- 2 Copy the key exporter script to a location on the network that is also accessible to the existing ADAM-based SEE Server or GuardianEdge Server.
- 3 Log on to the existing ADAM-based SEE Server or GuardianEdge Server and copy the key exporter script from the accessible network location to the local computer.
- 4 Open a command prompt and use the CD command to change to the directory where you copied the key exporter script.

- 5 At the command prompt, type the following command and press **Enter**:
KeyExport.vbs Database_Host Database_Name Uid=Username;Pwd=Password Port
Application_Partition_Name ADAMAdmin_Username DN_of_Domain ADAMAdmin_Password

Table 6-1 Parameters of the Key Export Script

Parameters	Description/Use Case	Usage
<i>Database_Host</i>	When Microsoft SQL Server was installed, the default instance was selected as the instance name	<i>Server Name</i> or <i>Server IP Address</i> , i.e. SEEDB-01 or 10.0.3.8
	When Microsoft SQL Server was installed, a named instance was selected as the instance name	<i>Server Name\Instance Name</i> or <i>Server IP Address\Instance Name</i> , i.e. SEEDB-01\SQL2005 or 10.0.3.8\SQL2005
	The Symantec Endpoint Encryption database is running on SQL Server 2005 Express Edition	<i>Server Name\SQLEXPRESS</i> , i.e. SEEDB-01\SQLEXPRESS
<i>Database_Name</i>	The name of the Symantec Endpoint Encryption database	SEEMSDb
<i>Username and Password</i>	To use SQL credentials to authenticate to the Symantec Endpoint Encryption database	Uid= <i>Username</i> ;Pwd= <i>Password</i> , i.e. Uid=Administrator;Pwd=pass@word1
	To authenticate to the Symantec Endpoint Encryption database with the credentials of the currently logged on Windows user	NULL
<i>Port</i>	The port of the ADAM Instance	389 is the default port of the ADAM Instance
<i>Application_Partition_Name</i>	The distinguished name (DN) of the application partition name of the ADAM instance	DC=EncryptionAnywhere,DC=com is the default DN of the application partition name of the ADAM instance
<i>ADAMAdmin_Username</i>	User name of an account with administrative privileges over the ADAM application partition	<i>User Name</i> , i.e. ADAMAdmin
<i>DN_of_Domain</i>	Distinguished Name (DN) of the domain that the ADAMAdmin account is member of	<i>Distinguished Name</i> , i.e. DC=your-org,DC=com
<i>ADAMAdmin_Password</i>	Password of the domain that the ADAMAdmin account is member of	<i>Password</i> , i.e. pass@word1

Examples

KeyExport.vbs SEEDB-01\SQL2005 SEEMSDb Uid=Administrator;Pwd=pass@word1 389
dc=EncryptionAnywhere,dc=com ADAMAdmin dc=your-org,dc=com pass@word1

This command line shows the following:

- The Symantec Endpoint Encryption database is being hosted on a server named SEEDB-01 where Microsoft SQL Server was installed with a named instance of SQL2005.
- The credentials of an SQL database account will be used to authenticate to the Symantec Endpoint Encryption database.
- The credentials and domain of the ADAM Administrator account

KeyExport.vbs SEEDB-01\SQLEXPRESS SEEMSDb NULL 389 dc=EncryptionAnywhere,dc=com ADAMAdmin dc=your-org,dc=com pass@word1

This command line shows the following:

- The Symantec Endpoint Encryption database is located on an SQL Server 2005 Express Edition instance.
- The credentials of the currently logged on Windows account will be used to authenticate to the Symantec Endpoint Encryption database.

Success

After the script has successfully completed, the following message will be displayed at the command line:

SUCCESS: Migrated encryption info into SQL Database.

You must now verify that the key info was successfully migrated to the Symantec Endpoint Encryption database.

Verification

Access the Symantec Endpoint Encryption database using the Microsoft SQL Server Management Studio (part of an optional install of tools for SQL Server 2005) using administrator-level privileges, and verify that the SEEMSDb database has been populated with a table named dbo.GEMSDeploymentKeys.

Note: If the dbo.GEMSDeploymentKeys table did not get created in the SEEMSDb database, do not run the key export script a second time. Contact Symantec technical support for instructions on how to proceed.

With the migration of the key info from the ADAM-based SEE Server or GuardianEdge Server to the Symantec Endpoint Encryption database now complete, you can continue on to the installation of the Manager Console and the creation and deployment of the client upgrade packages. At this time, you should also perform a backup of the Symantec Endpoint Encryption database.

Note: If you are prompted for the Management Password during an install or upgrade of the Symantec Endpoint Encryption Manager, it means that the key export operation failed. Contact Symantec technical support for instructions on how to proceed.

Symantec Endpoint Encryption Manager

Basics

Review the following important points before upgrading the Manager Computer:

- Determine whether the Manager Computer is running a 32-bit Edition of Windows or a 64-bit Edition of Windows, then select the compatible Manager Console package versions. 64-bit installer packages can be identified by the file name suffix x64.
- The latest version of Framework is only compatible with the latest versions of Full Disk and Removable Storage. All three must be upgraded.
- You should always be running the latest version of the Manager Console on all Manager Computers.
- Framework must always be upgraded first.

Version Number Determination

To perform this procedure

- 1 Open the Manager Console. In the navigation pane on the left, expand **Symantec Endpoint Encryption Software Setup** and click **Framework**. On the **Help** menu, click **About Framework**.
- 2 The **About Framework** window displays showing the current version of the Framework component.
- 3 Expand **Symantec Endpoint Encryption Software Setup** and click **Full Disk**. On the **Help** menu, click **About Full Disk**.

Framework Upgrade

To perform this procedure

- 1 Before starting the upgrade, close all instances of the Microsoft Management Console (MMC) currently running on the Manager Computer you are upgrading.
- 2 Transfer the installer packages comprising the latest release of the Manager Console (Symantec Endpoint Encryption Framework.msi and Symantec Endpoint Encryption Full Disk Edition.msi, or if you are installing the 64-bit package versions, Symantec Endpoint Encryption Framework x64.msi and Symantec Endpoint Encryption Full Disk Edition x64.msi), along with any other Manager Console components you want to install, to removable media or a designated network share.
- 3 Log on to the Manager Computer using an administrator account possessing sufficient rights for installing software.
- 4 Locate the Symantec Endpoint Encryption Manager installer packages on the removable media or network share and copy them to the local hard disk.
- 5 With the Symantec Endpoint Encryption Manager installer packages copied to the Manager Computer, upgrade Framework first by invoking the Windows Installer with the following command-line parameters:
MSIEXEC /i "[path]\Symantec Endpoint Encryption Framework[x64].msi" REINSTALL="ALL" REINSTALLMODE="vomus"
 Substitute *[path]* with the actual path on the Manager Computer where the package was copied to, and where
[x64] optionally specifies the 64-bit package version.

Full Disk Upgrade

To upgrade Full Disk use the following command-line parameters.

MSIEXEC /i "[path]\Symantec Endpoint Encryption Full Disk Edition[x64].msi" REINSTALL="ALL" REINSTALLMODE="vomus"

Substitute *[path]* with the actual path on the Manager Computer where the package was copied to, and where

[x64] optionally specifies the 64-bit package version.

Note: If the operating system is 32-bits, install Symantec Endpoint Encryption Full Disk EditionSymantec Endpoint Encryption Full Disk Edition.msi. If the operating system is 64-bits, install Symantec Endpoint Encryption Full Disk EditionSymantec Endpoint Encryption Removable Storage Edition x64.msi.

One-Time Password Program Upgrade

From Symantec Endpoint Encryption Full Disk 8.0.0

To upgrade the Symantec Endpoint Encryption Help Desk Program, use the following command-line:

MSIEXEC /i "[path]\Symantec Endpoint Encryption Help Desk[x64].msi" REINSTALL="ALL" REINSTALLMODE="vonus"

Substitute *[path]* with the actual path on the Manager Computer where the package was copied to, and where

[x64] optionally specifies the 64-bit package version.

Note: If the operating system is 32-bits, use Symantec Endpoint Encryption Help Desk.msi. If the operating system is 64-bits, use Symantec Endpoint Encryption Help Desk x64.msi.

From Symantec Endpoint Encryption Full Disk 7.0.8

To perform this procedure

- 1 To upgrade the Symantec Endpoint Encryption Help Desk Program, use the following command-line:

MSIEXEC /i "[path]\Symantec Endpoint Encryption Help Desk[x64].msi" REINSTALL="ALL" REINSTALLMODE="vonus"

Substitute *[path]* with the actual path on the Manager Computer where the package was copied to, and where

[x64] optionally specifies the 64-bit package version.

Note: If the operating system is 32-bits, use Symantec Endpoint Encryption Help Desk.msi. If the operating system is 64-bits, use Symantec Endpoint Encryption Help Desk x64.msi.

- 2 Select **Add/Remove Snap-In** from the **File** menu of the Manager Console.
- 3 In the **Add/Remove Snap-In** dialog, select the One-Time Password Program, and click **Remove**.
- 4 Click **Add**.
- 5 In the **Add Standalone Snap-In** dialog, highlight **SEE Help Desk**, and click **Add**.
- 6 In the **Add/Remove Snap-In** dialog, click **OK**.

From Symantec Endpoint Encryption Full Disk 7.0.7 and Earlier or any Version of GuardianEdge Hard Disk

To perform this procedure

- 1 To upgrade the Symantec Endpoint Encryption Help Desk Program, use the following command-line:

MSIEXEC /i "[path]\Symantec Endpoint Encryption Help Desk[x64].msi" REINSTALL="ALL" REINSTALLMODE="vonus"

Substitute *[path]* with the actual path on the Manager Computer where the package was copied to, and where

[x64] optionally specifies the 64-bit package version.

Note: If the operating system is 32-bits, use Symantec Endpoint Encryption Help Desk.msi. If the operating system is 64-bits, use Symantec Endpoint Encryption Help Desk x64.msi.

- 2 Select **Add/Remove Snap-In** from the **File** menu of the Manager Console.

- 3 In the **Add/Remove Snap-In** dialog, click **Add**.
- 4 In the **Add Standalone Snap-In** dialog, highlight **SEE Help Desk**, and click **Add**.
- 5 In the **Add/Remove Snap-In** dialog, click **OK**.

Upgrading Windows Clients

About Upgrading Windows Clients

Always upgrade Framework first.

Note: The Encryption Anywhere brand was phased out on August 28, 2007. If you have any Encryption Anywhere clients, before attempting to upgrade to this release, ensure that the following minimum version is installed: Encryption Anywhere Hard Disk 8.2.0.

Note: The Encryption Anywhere brand was phased out on August 28, 2007. If you have any Encryption Anywhere clients, before attempting to upgrade to this release, ensure that the following minimum versions are installed: Encryption Anywhere Framework 8.7.2 and Encryption Anywhere Removable Storage 2.0.0 or 2.1.0.

The latest version of Framework is only compatible with the latest versions of Full Disk and Removable Storage. All three must be upgraded.

To upgrade a client, perform the following steps:

- 1 Launch the latest version of the Manager Console.
- 2 Step through the client installation package creation wizard. Most of the settings chosen when creating the client upgrade package will overwrite the existing installation settings, except for the following:
 - Framework Installation Settings – Encryption,
 - Full Disk Installation Settings – Encryption, and
 - Full Disk Installation Settings – Installer Customization.If the upgrade package contains a change to the user's method of authentication and a policy is not in effect on the client, the user may be forced to re-register following the application of the upgrade package. See the *Policy Administrator Guide* for details on the user's experience following a change in authentication method.
- 3 Save the client installation package to a local or network volume with **Full Control** permissions set in the properties sheet. This ensures the success of the upgrade package, as it will retain the Windows permissions of the location to which it is saved. Two MSI packages will be saved: one for 32-bit versions of Windows and one for 64-bit versions of Windows.
- 4 Deploy the MSI appropriate to the version of Windows running on the Client Computer. Three methods are discussed in the following sections:
 - Installation using a third-party deployment tool ("[Upgrading Windows Clients Using a Third Party Tool](#)" on page 93);
 - Installation from Active Directory as an upgrade to an existing software installation computer policy ("[Upgrading Windows Clients Using a GPO](#)" on page 94); or
 - Manual installation using a Windows Installer command line at the Client Computer ("[Performing a Manual Upgrade of a Windows Client](#)" on page 96).

Note: When upgrading clients created from a serverless installation of the Manager Console to clients created from a default mode installation of the Manager Console, ensure that the Full Disk Client Monitor lockout policy is not enforced on those clients prior to performing the upgrade. If a lockout policy is in effect, the client machines could be subject to lockout immediately after the upgrade.

Note: Clients without Opal-compliant drives and less than 128, 256, 384, 512, 640, 768, or 896 Client Administrators must be rebooted before additional Client Administrators can log on. For example, if 512 Client Administrators exist and a policy adds one more, the 513th Client Administrator cannot log on until after the client completes a reboot.

Upgrading Windows Clients Using a Third Party Tool

Basics

Ensure that the packages reside in a location that is accessible to the recipient computers.

Syntax

To execute the appropriate MSI, the following syntax should be used:

MSIEXEC /i "[path]\name of client upgrade package.msi" parameter

[Table 6-2](#) describes the parameters and variables in greater detail.

Table 6-2 MSIEXEC Variables and Parameters for Upgrades

Variables/Parameters	Description	Default(s)/Example(s)
<i>[path]</i>	The local or network path where the MSI resides. Path is optional when the MSI file is executed from the current directory.	\\CADC-01\SYSVOL\PACKAGES\
<i>name of client installation package.msi</i>	The name of the MSI file you wish to execute	Symantec Endpoint Encryption Framework Client.msi Symantec Endpoint Encryption Framework Client_x64.msi Symantec Endpoint Encryption Full Disk Edition Client.msi Symantec Endpoint Encryption Full Disk Edition Client_x64.msi
<i>parameter</i>	The MSIEXEC parameters to be used	REINSTALL="ALL" REINSTALLMODE="vomus"

Examples

The following examples could be placed in a batch file to accomplish the upgrade of **Full Disk**.

MSIEXEC /i "\\CADC-01\SYSVOL\PACKAGES\Symantec Endpoint Encryption Framework Client_x64.msi" REINSTALL="ALL" REINSTALLMODE="vomus"

MSIEXEC /i "\\CADC-01\SYSVOL\PACKAGES\Symantec Endpoint Encryption Full Disk Edition Client_x64.msi" REINSTALL="ALL" REINSTALLMODE="vomus"

Upgrading Windows Clients Using a GPO

The method described here assumes that you deployed the Symantec Endpoint Encryption client installer packages as part of a Software Installation GPO using Active Directory, and that the policy is still in place. Do not manually upgrade a GPO deployment of Symantec Endpoint Encryption client installer packages, and do not upgrade a manual deployment of Symantec Endpoint Encryption client installer packages using a Software Installation GPO.

Note: Windows 2000 computers installed with Symantec Endpoint Encryption software deployed using a GPO cannot be upgraded using the method described here. To upgrade Windows 2000 computers, you must replace the original client package referenced by the GPO with the new upgrade package, making sure that the two file names are identical. To complete the upgrade process, you must edit the GPO, right click the client package, choose All Tasks, click Redeploy application, then close the GPO editor to apply the policy. Note that the product name and version information shown in the GPO editor will reflect those of the original package and not the upgrade package.

Because the upgrade involves creating a new set of client installer packages, you will need the following credentials to be able to complete the Framework Installation Settings Wizard:

- Credentials of the Policy Administrator account, and
- Credentials of the IIS client account.

You will create a new set of client installer packages for upgrading the existing client installer packages. As you did with the existing client installer packages, you will save the new set of client installer packages to the SYSVOL folder where they will be referenced by the software installation GPO. This will allow all Client Computers processing the policy to be able to access and apply the client installer upgrades.

Note: Always deploy the Symantec Endpoint Encryption client installer packages as part of a software installation computer policy and never as a software installation user policy.

To perform this procedure

- 1 On the Manager Computer, click **Start**, point to **All Programs**, then click **Symantec Endpoint Encryption Manager Console**.
- 2 The Manager Console opens. In the navigation pane on the left, expand **Symantec Endpoint Encryption Software Setup** and click **Framework**.
- 3 In the **Framework Installation Settings Wizard** panel on the right, enter the required information and click **Next**.
- 4 When you reach the final panel of the Wizard, click **Finish**. A success confirmation dialog will display. Click **OK**. You will be prompted to specify a location in which to save the Symantec Endpoint Encryption Framework Client.msi file. Navigate to the SYSVOL folder.
If the SYSVOL folder already contains a file named Symantec Endpoint Encryption Framework Client.msi (this is the existing Framework client installer package), change the default name of the new client installer package (to, for example, Symantec Endpoint Encryption Framework Client2.msi) and click **OK**.
- 5 Repeat steps 3 and 4 to create the Full Disk client installer upgrade package using the **Full Disk Installation Settings Wizard**. Rename the resulting Full Disk client installer package to Symantec Endpoint Encryption Full Disk Edition Client2.msi and also save the file in the SYSVOL folder.
- 6 In the navigation pane of the Symantec Endpoint Encryption Manager, expand the **Group Policy** snap-in to reveal the existing GPOs. Locate the GPO you created for deploying the Symantec Endpoint Encryption client installer packages, select it, right-click, and choose **Edit**.
- 7 The Group Policy Object Editor (GPOE) opens. Expand **Computer Configuration**, then expand **Software Settings**.

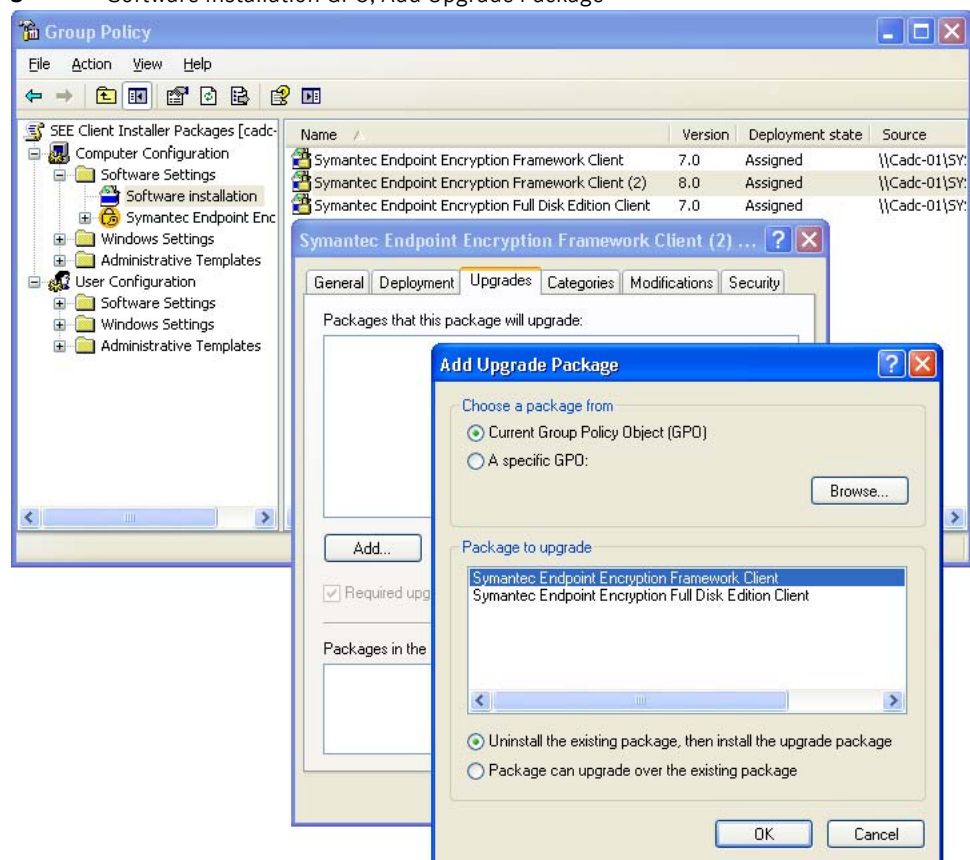
- 8 Right-click **Software Installation**, point to **New**, then click **Package**. Click My Network Places, and navigate to the location **Microsoft Windows Network\your-org\Cadc-01\SYVOL** where you previously copied the client installer upgrade packages, for example, Symantec Endpoint Encryption Framework Client2.msi and Symantec Endpoint Encryption Full Disk Edition Client2.msi.
- 9 Click to select the client installer upgrade, Symantec Endpoint Encryption Framework Client Installer2.msi, and click **Open**.
- 10 A confirmation screen will appear. Click **OK** to accept the default value of **Assigned** for that package.

Note: Ensure that you select a compatible version of the client installer package. You cannot upgrade a 32-bit client installer package using a 64-bit client installer package, and you cannot upgrade a 64-bit client installer package using a 32-bit client installer package. 64-bit client installer packages can be identified by the file name suffix `_x64`.

Note: If you do not select the client module upgrade template package by navigating to it using My Network Places, Client Computers receiving the policy will be unable to locate the install package and the software installation policy will fail to be applied.

- 11 The new package will appear in the pane on the right as **Symantec Endpoint Encryption Framework Client (2)**. Select it, right-click, and choose **Properties**.
- 12 The **Properties** window opens. Click the **Upgrade** tab, then click **Add**.
- 13 In the **Package to upgrade** box, choose **Symantec Endpoint Encryption Framework Client**.
- 14 Choose **Package can upgrade over the existing package**. Click **OK**, click **Apply**, then **OK**.
- 15 Repeat steps 8 through 14 to assign the new Full Disk client installer package Symantec Endpoint Encryption Full Disk Edition Client2.msi as an upgrade to the existing package.

Figure 6-3 Software Installation GPO, Add Upgrade Package



- 16 Finally, close the GPOE window to apply the policy. Note that Client Computers targeted by this computer policy must be restarted in order to install the upgrade.

Performing a Manual Upgrade of a Windows Client

To perform a manual upgrade of a Symantec Endpoint Encryption Windows client:

- 1 Click **Start**, click **Run**, type **cmd**, then click **OK** to open a new command prompt window.
- 2 Invoke the Windows Installer (msiexec.exe) with the command-line parameters from Table 6.2, for example:
MSIEXEC /i "\\CADDC-01\SYSVOL\PACKAGES\Symantec Endpoint Encryption Framework Client_x64.msi" REINSTALL="ALL" REINSTALLMODE="vonus"
This command line shows the following:
 - The 64-bit version of the **Symantec Endpoint Encryption Framework Client** upgrade package is located in the SYSVOL folder.
 - The client upgrade package was saved with the default name.
 - The client will be upgraded by reinstalling all features of the product.
- 3 When the Windows Installer finishes executing, the upgrade for the Framework client will be installed, and a completion dialog will display. Click **OK**.
- 4 Upgrade Full Disk by invoking the Windows Installer with the command-line parameters from Table 6.2, for example:
MSIEXEC /i "\\CADDC-01\SYSVOL\PACKAGES\Symantec Endpoint Encryption Full Disk Edition Client_x64.msi" REINSTALL="ALL" REINSTALLMODE="vonus"
This command line shows the following:
 - The 64-bit version of the **Symantec Endpoint Encryption Full Disk Edition Client** upgrade package is located in the SYSVOL folder.
 - The client upgrade package was saved with the default name.
 - The client will be upgraded by reinstalling all features of the product.
- 5 When the Windows Installer finishes executing, a dialog prompting you to restart the computer will display. Click **Yes** to restart the computer.

Upgrading Mac Clients

You cannot upgrade a Symantec Endpoint Encryption Full Disk Mac client during encryption or decryption. Wait for the encryption or decryption process to complete before upgrading.

To upgrade a Mac client:

- 1 Ensure that the Mac client can access the Mac client installation package (Symantec Endpoint Encryption Full Disk Edition Client_MAC.zip), either by placing it on a network share or on removable media.
- 2 Log on to the Mac client using an account with administrative privileges.
- 3 Close all applications.
- 4 Double-click the Symantec Endpoint Encryption Full Disk Edition Client_MAC.zip file.
- 5 Open the pgpdesktop directory.
- 6 Double-click PGP.pkg.
- 7 Click through the pages of the installation wizard.
- 8 Provide administrative credentials when prompted.

- 9 You will be notified that the computer will be restarted to complete the upgrade. Click **Continue Installation**.
- 10 Once the upgrade concludes successfully, click **Restart**.
- 11 You may receive a **Certificate Trust** prompt after the Mac restarts. Provide administrative credentials and accept the changes.

Encryption Plus Hard Disk Migration

This chapter includes the following topics:

- [Overview](#)
- [Client Migration Package Preparation](#)
- [Client Migration Package Deployment](#)
- [Utility Analogs](#)

Overview

This release of Symantec Endpoint Encryption Full Disk features the ability to migrate Encryption Plus Hard Disk clients. The migration process is a seamless process very similar to an upgrade and does not require decryption of the clients or uninstallation of Encryption Plus Hard Disk. Following a successful migration, users will be prompted to register with Full Disk.

The Encryption Plus Management Console Client will be uninstalled following a successful migration, as it will become irrelevant in the context of Full Disk.

The steps to migrate are as follows:

- 1 Inventory your system and ensure that it complies with the system requirements (Chapter 1 [“System Requirements”](#) on page 3).
- 2 Provision the required accounts (Chapter 1 [“Required Accounts”](#) on page 11).
- 3 Install the Management Server (Chapter 2 [“Installing the Symantec Endpoint Encryption Management Server”](#) on page 17).
- 4 Install the Manager Console (Chapter 3 [“Installing the Symantec Endpoint Encryption Manager Console”](#) on page 35).
- 5 Create and deploy your client migration packages (discussed in this chapter and in Chapter 5 [“Client Installations”](#) on page 75).

Client Migration Package Preparation

No Encryption Plus Hard Disk User Program Setup settings will be recognized or carried forward during migration. Encryption Plus Hard Disk event logs will not be migrated to Full Disk.

You must specify your desired settings manually when creating the client migration packages. Use the Client Installation Package Creation snap-in to specify the client settings (Chapter 4 [“Client Installation Package Creation”](#) on page 51).

Encryption Plus Hard Disk clients that are encrypted will remain encrypted at the encryption strength that they were encrypted with. The Full Disk advanced encryption options (Chapter 4 “Encryption” on page 65) will only be used if the Client Computer is decrypted and re-encrypted.

Client Migration Package Deployment

Once you have created your client migration packages, apply them to your Encryption Plus Hard Disk Clients using your choice of MSI distribution methods: third party tool, Active Directory, or manual. Refer to Chapter 5 “Deploying Client Installer Packages” on page 76 and Chapter 5 “Manual Client Installations” on page 79 for detailed instructions on each method.

Utility Analogs

Note: Symantec recommends that you avail of the security features of the third-party tool of your choice to protect your MSI packages.

This section compares Encryption Plus Hard Disk utilities with Full Disk utilities.

Table 7-1 Encryption Plus Utilities and their Symantec Endpoint Encryption Analogs

Encryption Plus Utility	Symantec Endpoint Encryption Analog
Access Utility (16-bit)	Full Disk Access Utility
Access Utility (32-bit)	Full Disk Access Utility
AdminPPKP	OTP Key Changer
Audit Trail Data Exporter	Full Disk audit logs are stored in the Windows System Event Viewer. Various third-party tools enable centralized management of Windows System Events. Some events can be viewed from the Manager Console.
Autologon	Autologon policy
EPHD Detect	Manager Console
Recover Program	Recover Program
WEK Backup Utility	Clients that are not silent will send the encrypted WEK to the Symantec Endpoint Encryption Management Server automatically.

Uninstallation

This chapter includes the following topics:

- [Overview](#)
- [Symantec Endpoint Encryption Management Server](#)
- [Symantec Endpoint Encryption Manager Console](#)
- [Mac Client Computer](#)
- [Windows Client Computer](#)

Overview

This section describes how to uninstall the Symantec Endpoint Encryption Management Server, the Symantec Endpoint Encryption Manager, and the Symantec Endpoint Encryption client software.

Symantec Endpoint Encryption Management Server

Log on to Windows using a domain account that has sufficient privileges to uninstall software and system administrator privileges on the SQL Server instance. Alternately, log on to Windows using a local account that has sufficient privileges to uninstall software, then during uninstallation, provide credentials of an SQL account that has administrative privileges to the Symantec Endpoint Encryption database instance.

Click **Start**, then click **Control Panel**. Double-click **Add or Remove Programs**.

In **Currently installed programs**, select **Symantec Endpoint Encryption Management Server**. Click **Remove**.

The Add or Remove Programs Wizard displays a warning dialog. Click **Yes**.

The **Symantec Endpoint Encryption Management Server** dialog will display.

Figure 8-1 Symantec Endpoint Encryption Management Server Uninstallation Dialog



To preserve the existing Symantec Endpoint Encryption database and database communication account, leave the **Delete my Management Database and SQL User account** check box deselected, then click **Next**. Preserving the Symantec Endpoint Encryption database and the database communication account will allow you to reuse them should you plan to reinstall the Management Server later on. The credentials of the currently logged on Windows account will be used to uninstall the Management Server.

To delete the Symantec Endpoint Encryption database and database communication account, select the **Delete my Management Database and SQL User account** check box. If the Windows account you logged on with has administrative privileges to the Symantec Endpoint Encryption database instance, leave **Windows authentication** at the default state, otherwise click **SQL authentication** and enter the credentials of an SQL account that has administrative privileges to the Symantec Endpoint Encryption database instance. Clicking **Next** will remove the existing Symantec Endpoint Encryption database and all client data records, along with the database communication account.

Symantec Endpoint Encryption Manager Console

When uninstalling the Manager Console, always remember to uninstall the Framework package last.

To uninstall the Manager Console, do the following:

- 1 Log on to the Manager Computer using an administrator account or other account with sufficient privileges to uninstall software.
- 2 Click **Start**, click **Control Panel**. Double-click **Add or Remove Programs**.
- 3 In **Currently installed programs**, select **Symantec Endpoint Encryption Help Desk Program**. Click **Remove**.
- 4 A confirmation message box displays. Click **Yes**. A progress box briefly displays.
- 5 In **Currently installed programs**, select **Symantec Endpoint Encryption Full Disk Edition**. Click **Remove**.
- 6 A confirmation message box displays. Click **Yes**. A progress box briefly displays.
- 7 With **Add or Remove Programs** still open, select **Symantec Endpoint Encryption Framework**. Click **Remove**.
- 8 A confirmation message box displays. Click **Yes**. A progress box briefly displays.

Mac Client Computer

To uninstall Symantec Endpoint Encryption Full Disk from a Mac, log on to the Mac using an account with administrative credentials. If the disk is not already decrypted, decrypt it.

Open the PGP application by clicking the PGP toolbar menu icon or from the Applications folder.

Select **Uninstall** from the **PGP** menu.

Provide administrative credentials if prompted.

Windows Client Computer

Basics

When uninstalling client installer packages, Symantec Endpoint Encryption Framework must be uninstalled last.

Note: Before you begin, ensure that all fixed disks are fully decrypted. Should an unavoidable issue prevent you from decrypting a secondary drive, a manual uninstallation will be necessary. See [“Manual”](#) on page 104.

For information on how to remotely decrypt all fixed disks and partitions on the Client Computer using a policy, refer to the *Policy Administrator Guide*. For information on how a Client Administrator can decrypt fixed disks and partitions locally, refer to the *Client Administrator Guide*.

Note: If this is a Symantec Endpoint Encryption managed computer, you should manually delete it from the Manager Console following uninstallation. See the Policy Administrator Guide for more details.

Third Party Tool

Uninstallation of the Symantec Endpoint Encryption client packages can be accomplished using any third-party deployment tool that supports the MSI format.

For large scale deployments, you can use the command-line method as a basis for scripted upgrades.

For example, you could create a batch file to invoke the Windows Installer (msiexec.exe). This batch file would contain the following lines:

```
MSIEXEC /x "[path]\Symantec Endpoint Encryption Full Disk Edition Client[_x64].msi"  
REBOOT=ReallySuppress
```

```
MSIEXEC /x "[path]\Symantec Endpoint Encryption Framework Client[_x64].msi"  
REBOOT=ReallySuppress
```

where *[path]* is the actual path on the Client Computer where the package was copied to, and where *[_x64]* optionally specifies the 64-bit package version.

Note: Uninstallation will fail if all drives are not fully decrypted.

Client Packages Deployed Using a GPO

As is true of any software deployed using a Software Installation GPO, client packages should never be uninstalled manually at the client. Packages deployed using a Software Installation GPO should only be uninstalled by removing or changing the scope of the Software Installation GPO. Attempting to remove GPO-deployed client packages by manually uninstalling the packages using the **Add or Remove Programs**

control panel on the client while the Software Installation GPO is still in effect will result in the packages being reinstalled at the next restart. Further attempts to uninstall the client packages will result in an error. As a best practice, you should set the appropriate Windows policies to prevent users from manually removing the client packages.

Note: Uninstallation will fail if all drives are not fully decrypted.

Manual

Basics

As long as the client was not deployed by GPO, it can be uninstalled manually from the local workstation through Windows **Add/Remove Programs**.

If some unavoidable issue prevents you from decrypting a secondary drive, you will have the option to proceed with uninstallation. Refer to [“Encrypted Secondary Disk, Connected”](#) on page 104 and [“Encrypted Secondary Disk, Not Connected”](#) on page 105.

To uninstall Full Disk, do the following:

- 1 Log on to the client computer using an administrator account or other account with sufficient privileges to uninstall software.
- 2 Click **Start**, then click **Control Panel**.
- 3 For Windows XP, double-click **Add or Remove Programs**. For Windows 7 or Windows Vista, click **Classic View**, and double-click **Programs and Features**.
- 4 Select **Symantec Endpoint Encryption Full Disk Edition Client**. For Windows XP, click **Remove**. For Windows 7 or Windows Vista, click **Uninstall**.
- 5 A confirmation message box displays. Click **Yes**. A progress box briefly displays.
- 6 Select **Symantec Endpoint Encryption Framework Client**. For Windows XP, click **Remove**. For Windows 7 or Windows Vista, click **Uninstall**.
- 7 A confirmation message box displays. Click **Yes**. A progress box briefly displays.

Encrypted Secondary Disk, Connected

If you attempt to uninstall when an encrypted secondary drive is connected, the following warning will be displayed:

Figure 8-2 Uninstallation, Encrypted Secondary Disk Connected



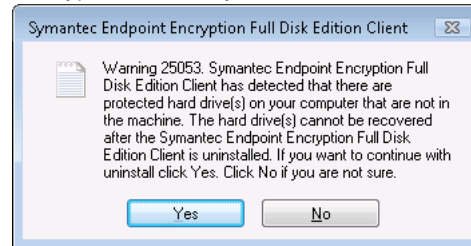
Click **Yes** to proceed with uninstallation. All data on the affected secondary drive(s) will be permanently lost and unrecoverable. Refer to [“Recovery of Secondary Disk Post-Uninstallation”](#) on page 105.

Click **No** to cancel uninstallation.

Encrypted Secondary Disk, Not Connected

If you attempt to uninstall when a previously connected encrypted secondary drive is not connected, the following warning will be displayed:

Figure 8-3 Uninstallation, Encrypted Secondary Disk Not Connected



Click **Yes** to proceed with uninstallation. All data on the affected secondary drive(s) will be permanently lost and unrecoverable. Continue to next section.

Click **No** to cancel uninstallation.

Recovery of Secondary Disk Post-Uninstallation

If a secondary disk was encrypted at the time that Full Disk was uninstalled and you chose to proceed with the uninstallation, you must follow the steps in this section to regain the ability to encrypt and manage the drive using Full Disk.

Before you begin, you will need to know the number assigned to this physical disk by the operating system. The numbering starts at 0 and increments sequentially. Visit the Windows Disk Management snap-in to obtain the number.

To perform this procedure

- 1 Reformat the secondary disk.
- 2 Obtain a Windows 98 boot CD and boot the client computer from the CD.
- 3 Type the following at the Windows 98 command prompt:
FDISK /CMBR drive number
where **drive number** denotes the drive number of the secondary drive.
- 4 Remove the Windows 98 boot CD and restart the client computer.

Following this procedure, you can reinstall **Full Disk and encrypt the secondary disk**.

Management Server Configuration

This chapter includes the following topics:

- [Overview](#)
- [Configuration Manager](#)
- [Symantec Endpoint Encryption Management Server Clusters](#)

Overview

This chapter describes how to change the configuration of the Symantec Endpoint Encryption Management Server.

Configuration Manager

Basics

Settings specified during the installation of the Management Server can later be modified using the Configuration Manager.

The Configuration Manager is placed on the Management Server during installation. It is located at C:\Program Files\Symantec\Symantec Endpoint Encryption Management Server\Services\Symantec.Endpoint.Encryption.ConfigManager.exe.

If you are using Windows authentication with your SQL Server instance, log on to the Management Server using the Management Server account or the database creation account (Chapter 1 “[Required Accounts](#)” on page 11).

If you are using mixed-mode authentication with your SQL Server instance, log on to the Management Server using a Windows account having the following characteristics:

- Local administrator rights on the Management Server
- Read/write permissions to the database

You can run the Configuration Manager only on the Management Server. Launch the executable to begin.

Database Configuration Tab

The Configuration Manager will launch with its first tab open. This tab allows you to view and/or modify the Symantec Endpoint Encryption database parameters.

Figure A-1 Configuration Manager, Database Configuration Tab

The screenshot shows the 'Database Configuration' tab of the 'SEE Management Server Configuration Manager'. The fields are as follows:

Field	Value
Database Server Name	SEEMSDb-01\NAMEDINSTANCE
Custom Port Number	1533
Schema Name	SEEMSDb
Authentication Mode	SQL Authentication
User Name	SEEMUSER
Password	XXXXXXXXXX
Confirm Password	XXXXXXXXXX
User Domain	

At the bottom right, there is an unchecked checkbox labeled 'Enable TLS/SSL' and two buttons: 'OK' and 'Cancel'.

Database Server Name will display the NetBIOS name of the computer currently hosting the Symantec Endpoint Encryption database. If you are using a named instance, this field will display the NetBIOS name and instance name, e.g., **SEEDB-01\NAMEDINSTANCE**. If the Symantec Endpoint Encryption database has been moved to a different computer, or if the computer hosting it has been renamed, edit the contents of this field.

If the Symantec Endpoint Encryption database was configured to use a custom port, the port number will be displayed in **Custom Port Number**. This field will be empty if the Symantec Endpoint Encryption database is using the default port number. If the Symantec Endpoint Encryption database port number has changed, type the new port number in this field.

The name of the Symantec Endpoint Encryption database will be displayed in **Schema Name**.

If the Management Server was configured to authenticate to the database using SQL authentication, **SQL Authentication** will be displayed in the **Authentication Mode** drop-down list, and the **User Domain** field will be empty. If the Management Server was configured to authenticate to the database using Windows authentication, **Windows Integrated Authentication** will be displayed in the drop-down list, and the **User Domain** field will contain the domain of the mapped Windows domain account.

If the Management Server was configured to authenticate to the database using SQL authentication, the account displayed in the **User Name** field will be the Microsoft SQL Server account created during the installation of the Management Server. If the Management Server was configured to authenticate to the database using Windows authentication, the account shown will be the mapped Windows domain account provisioned prior to installation.

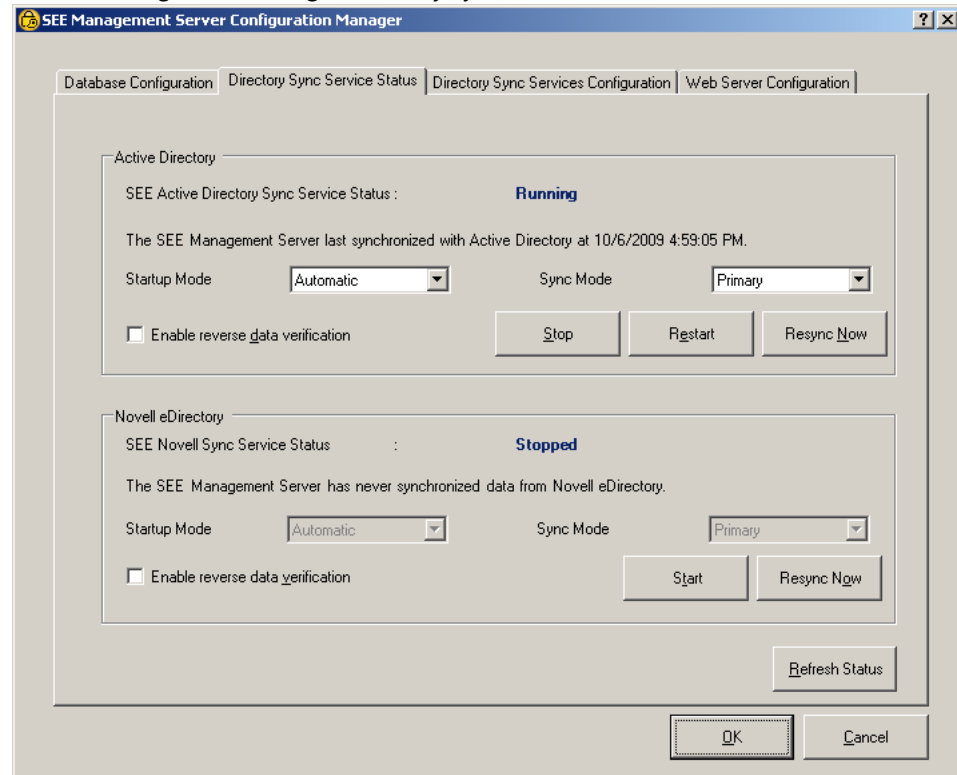
Asterisks representing the password used by the SQL account that the Management Server is using to communicate with the Symantec Endpoint Encryption database will be displayed in **Password** and **Confirm Password**.

Click **Enable TLS/SSL** to encrypt all traffic between the SQL database and the Management Server. Note that the use of this option requires properly installed and configured TLS/SSL certificates. See [“Configuring Encrypted Database Communications”](#) on page 18.

Directory Sync Service Status

Click the **Directory Sync Service Status** tab to view the status of the synchronization services and adjust their operation.

Figure A-2 Configuration Manager, Directory Sync Service Status Tab



The tab is divided into two main areas containing the options and status information related to each directory service.

The first field in each area will display the current status of synchronization with the directory service.

Table A-1 Synchronization Service Status Values

Value	Explanation
Running	The service is running.
Stopped	The service has been stopped.
Start Pending	A command to start the service has been issued and is in process.
Continue Pending	A command to restart the service has been issued and is in process.
Pause Pending	A command to stop the service has been issued and is in process.
Not Installed	The service has been manually removed. This represents an error condition as the service should only be removed during an uninstallation procedure.

Below the status value, a sentence will state either that synchronization with the directory service has never occurred, or the last time and date on which the synchronization occurred.

The status information for both areas is refreshed by clicking **Refresh Status**.

The display of the buttons will vary as appropriate to the current status of the directory service synchronization. If the service is stopped, click **Start** to start the service. Click **Stop** to stop the synchronization service. Click **Restart** to restart the service.

Click **Rebuild Table** to effect an immediate and complete synchronization. Normal synchronizations occur approximately every 15 minutes and only update data that has been changed since the last synchronization. The **Rebuild Table** button will effect a full and complete synchronization on an immediate basis. For large deployments, this operation can take an extended period of time to complete, and will temporarily increase the load on the Symantec Endpoint Encryption database and each directory service.

Startup Mode allows you to select whether each directory synchronization service starts automatically or manually.

Sync Mode controls whether the Management Server operates as a primary or a secondary synchronization source. This setting is pertinent for deployments in which you have created an NLB cluster of multiple Management Servers to provide hot failover capability. By default, each Management Server is installed as the primary synchronizer. When operating in a cluster of Management Servers, only one Management Server should be configured as the primary synchronizer, and all other Management Servers should be configured as secondary synchronizers. See [“Directory Sync Service Status”](#) on page 96.

To configure this Management Server to act as a primary synchronizer, choose **Automatic** from the **Startup Mode** list box, and choose **Primary** from the **Sync Mode** list box.

To configure this Management Server to act as a secondary synchronizer, choose **Secondary** from the **Sync Mode** list box, then choose **Automatic** from the **Startup Mode** list to run the service automatically at boot time. Choose **Manual** if you don't want the service to automatically run and begin synchronization at boot time.

Enable reverse data verification provides additional assurance that deleted directory objects will be properly synchronized with the Management Server. This setting is off by default. Be advised that turning on this setting doubles the number of times the directory is queried for changes, resulting in a decrease in network performance. Therefore, you may wish to analyze the directory synchronization network traffic prior to and after enabling this setting in order to assess its impact.

Directory Sync Services Configuration

Basics

Click the **Directory Sync Services Configuration** tab to view and/or modify your current synchronization settings.

Figure A-3 Configuration Manager, Directory Sync Services Configuration Tab

SEE Management Server Configuration Manager

Database Configuration | Directory Sync Service Status | **Directory Sync Services Configuration** | Web Server Configuration

Active Directory Configuration

☒ Activate Active Directory Synchronization 1/1 AD Forest

Active Directory Forest Name: your-org.com

Preferred Global Catalog Server: cadc-01.your-org.com

Active Directory User Name: adsyncuser

Password: [masked] Confirm Password: [masked]

User Domain: your-org.com

☐ Enable TLS/SSL

Configure Domain Filter Delete Prev Add

Novell Configuration

☐ Activate Novell eDirectory Synchronization

Novell Tree Name: [empty]

LDAP Host Server IP: [empty] LDAP Port: 389

User Distinguished Name: [empty]

Password: [empty] Confirm Password: [empty]

Delete Prev Add

OK Cancel

This tab displays the current settings for directory synchronization and allows you to configure directory synchronization with multiple forests and/or trees. For Active Directory synchronization, you can configure domain filtering, as well as enable TLS/SSL. When you have completed all fields, click **OK**. Once the information has been successfully validated, it will be stored in the Symantec Endpoint Encryption database.

Select **Activate Microsoft Active Directory Synchronization** and/or **Activate Novell eDirectory Synchronization** to enable the respective synchronization services on the Management Server.

Active Directory Configuration Area

If you selected Active Directory synchronization at installation time, the Management Server was configured to synchronize with one or more Active Directory forests. To synchronize with additional Active Directory forests, click **Add**. The status text above the right side of the **Active Directory Forest Name** field will update to display **2/2 AD Forest**, indicating that the configuration settings for the second of a total of two forests are currently displayed. Type the configuration information for the new forest:

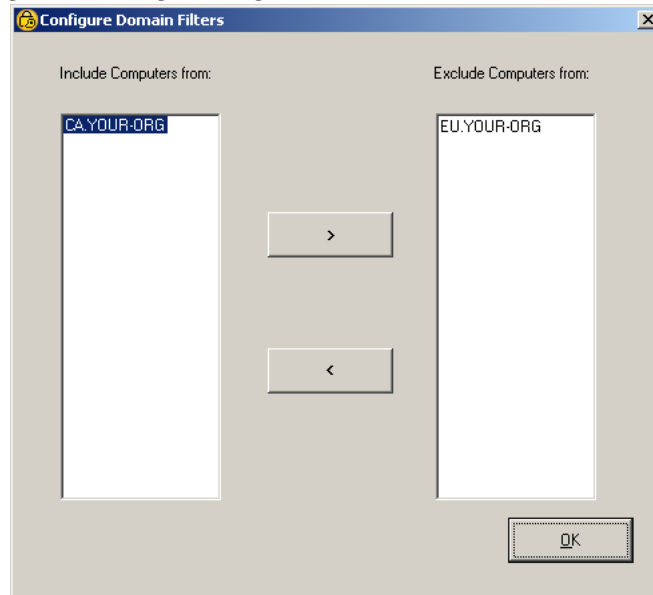
- **Active Directory Forest Name** is the name of the specified forest.
- **Preferred Global Catalog Server** is the name of a computer configured as a global catalog server for the specified forest.
- **Active Directory User Name** and **Password** are the credentials of the Active Directory synchronization account.
- **User Domain** is the NetBIOS name of the Active Directory synchronization account.

Click **Delete** to remove the configuration information for the currently displayed forest, or click **Prev** to view the configuration information for the previous forest.

Domain filtering allows you to exclude specific Active Directory domains from synchronization while including others. For example, there may be domains within your forest(s) that do not contain Symantec Endpoint Encryption Client Computers. To improve performance and usability, you can exclude these domains from being synchronized.

To use the domain filter, click **Configure Domain Filter**.

Figure A-4 Configuration Manager, Configure Domain Filters



In the **Include Computers from** column on the left, select a domain you wish to exclude, then click > to move the domain into the **Exclude Computers from** column on the right. Moving a parent domain from the **Include Computers from** column to the **Exclude Computers from** column will also move all child domains of that parent domain. In a typical deployment, you would exclude the top level of a domain, then include only those child domains containing Client Computers. Click **OK** when finished.

Click **Enable TLS/SSL** to encrypt all synchronization traffic between Active Directory and the Management Server. Note that the use of this option requires properly installed and configured TLS/SSL certificates. See [“Configuring Encrypted Active Directory Synchronization Communications”](#) on page 19.

Novell Configuration Area

If you selected eDirectory synchronization at installation time, the Management Server was configured to synchronize with one or more eDirectory trees. To synchronize with additional eDirectory trees, click **Add**. The status text above the right side of the **Novell Tree Name** field will update to display **2/2 Novell Tree**, indicating that the configuration settings for the second of a total of two trees are currently displayed. Type the configuration information for the new tree:

- **Novell Tree Name** is the name of the specified tree
- **LDAP Host Server IP** and **LDAP Port** are the IP and port of the eDirectory host for the specified tree.
- **User Distinguished Name** and **Password** are the distinguished name (DN) and password of the Novell synchronization account. Note that providing the DN and password is optional.

Click **Delete** to remove the configuration information for the currently displayed tree, or click **Prev** to view the configuration information for the previous tree.

Policy Priority Settings Area

When you select both the **Activate Microsoft Active Directory Synchronization** and the **Activate Novell eDirectory Synchronization** check boxes, the policy priority settings area will be displayed. When Active Directory and eDirectory are both present, a Client Computer can potentially be a member of both, thus receiving two sets of potentially conflicting Symantec Endpoint Encryption policies. To mitigate potential policy conflicts, you must choose the directory service whose policies will have priority. Select either **Use AD Policy** or **Use Novell Policy**.

Web Server Configuration

Click the **Web Server Configuration** tab to view and/or modify the protocol and/or port used for communications between the Client Computers and the Management Server.

Figure A-5 Configuration Manager, Web Server Configuration Tab

The screenshot shows the 'SEE Management Server Configuration Manager' window with the 'Web Server Configuration' tab selected. The window contains several input fields and sections:

- Web Server Name:** A text box containing 'seems-01'.
- IIS Client Account Credentials:** A group box containing:
 - Account Name:** 'administrator'
 - Password:** An empty text box.
 - Domain:** 'your-org.com'
- Protocol:** Two radio buttons: 'HTTP' (unselected) and 'HTTPS' (selected). To the right are two text boxes: 'HTTP Port' with '1001' and 'HTTPS Port' with '1002'.
- Client Computer Communications:** A group box containing:
 - Client-Side TLS/SSL Certificate:** A 'Browse' button and a text box showing 'Certificate Hash: 02A22E5412730AF0074B38F5EF498F1BDF997D48'.
 - Server-Side TLS/SSL Certificate:** A 'Browse' button and a text box showing 'Certificate Hash: CE516002E22AE68B2E0F5E6185CBABB422E555DB'.

At the bottom right are 'OK' and 'Cancel' buttons.

Web Server Name displays the name of the computer hosting the Management Server. The NetBIOS name is displayed by default after installation, but this field will also accept an FQDN. You will need to adjust this value if you:

- The computer name of the Management Server has been changed.
- DNS configuration issues prevent the NetBIOS name from resolving and an FQDN is more appropriate to your network environment.
- You will use an NLB cluster of Management Servers. You must edit this value on each cluster member so that it contains the FQDN of the cluster. See [“Symantec Endpoint Encryption Management Server Clusters”](#) on page 101.

Note: If you intend to use HTTPS communication between Client Computers and the Management Server, this name must match the common name (CN) specified in the server-side TLS/SSL certificate exactly. Refer to Chapter 2 [“Server-Side TLS/SSL Certificate Requirements”](#) on page 18.

Account Name and **Domain** display the name and domain of the IIS client account. If you are changing the IIS client account, type the credentials of this account. To complete any changes on this tab, you must enter the password of the IIS client account in **Password**, then click **OK**.

Once you have completed the entry of the IIS client account credentials, to change the protocol itself, select the relevant option button. If **HTTPS** is selected, an **HTTPS Port** field will be displayed, along with the **Client Computer Communications** area.

Type the number of the TCP port on the Management Server that should be used for the unencrypted client communications in the **HTTP Port** box. A TCP port for unencrypted communications will be required even if the HTTPS option is selected. IIS requires this information, but Symantec Endpoint Encryption will not

use this port. If you selected the HTTPS option, type the TCP port on the Management Server that should be used for the encrypted client communications in the **HTTPS Port** box.

To select or change the client-side TLS/SSL certificate Symantec Endpoint Encryption Client Computers use for encrypted communication with the Management Server, click the **Browse** button adjacent to the text **Client-Side TLS/SSL Certificate**. A **Choose SSL certificate file** dialog will be displayed, listing the certificates available in the personal certificate store of the local computer (i.e., the Management Server). Navigate to the location of a CER file suitable for use as a client-side TLS/SSL certificate, then click **Open**. The certificate hash string will be displayed below the **Browse** button.

To select or change the server-side TLS/SSL certificate the web service of the Management Server uses for encrypted communication with Symantec Endpoint Encryption Client Computers, click the **Browse** button adjacent to the text **Server-Side TLS/SSL Certificate**. The **Certificate selection** dialog will display a list of certificates found in the local certificate store. Select a certificate suitable for use as a server-side TLS/SSL certificate, then click **OK**. The certificate hash string will be displayed below the **Browse** button.

Note: Selecting the server-side TLS/SSL certificate in the Configuration Manager is equivalent to assigning the server-side TLS/SSL certificate to the Symantec Endpoint Encryption Services website using the IIS Manager snap-in.

Symantec Endpoint Encryption Management Server Clusters

Basics

Multiple Management Servers can be configured into an NLB cluster for hot failover capability. Clustering provides additional assurance that Symantec Endpoint Encryption client computers will maintain contact with Management Server at all times.

Creating the Cluster

While detailed instructions for creating an NLB cluster are beyond the scope of this Guide, here is an outline of the necessary steps. Refer to Microsoft documentation for in-depth instructions on how to configure an NLB server cluster using the Network Load Balancing Manager snap-in.

To perform this procedure

- 1 Create an address ("A") record in the DNS dedicated to the cluster, for example, *cluster1.your-org.com*.
- 2 Create a new cluster using the Network Load Balancing Manager snap-in. Specify the network and naming settings that correspond to the DNS entry you reserved for the cluster.
- 3 Populate the cluster with individual Management Server hosts.

Note: If you plan to configure the Management Server for HTTPS client-server communication, you must configure all Management Servers in the cluster with TLS/SSL certificates that specify the FQDN of the cluster, for example, *cluster1.your-org.com*.

- 4 On each cluster host, open the Management Server Configuration Manager and click on the **Directory Sync Services** tab. On the primary host, set **Sync Mode** to **Primary** and click **OK**. On all other hosts, set **Sync Mode** to **Secondary** and click **OK**.

Verifying Successful Cluster Failover

After you have configured all Management Server hosts into an NLB cluster, you'll need to test cluster failover functionality.

To perform this procedure

- 1 Create a Framework client package configured to report to the Symantec Endpoint Encryption Management Server cluster at a one minute interval. Deploy this client package to one or more client computers.
- 2 On each host of the cluster, configure the Windows System Monitor to display Symantec Endpoint Encryption Services website network traffic.
- 3 Launch the Performance snap-in. Click **Start**, point to **Programs**, point to **Administrative Tools**, then click **Performance**. In the left pane, click **System Monitor**. In the right pane, click the **New Counter Set** button, then click the **Add** button to display the **Add Counters** dialog.
- 4 Leave **Select counters from computer** at the default setting of the name of computer you are logged on to. In **Performance object**, select **Web Service**, and in **Select instances from list**, select **Symantec Endpoint Encryption Services**. Leave **Select counters from list** at the default setting of **Bytes Total/sec**. This configures the counter to display the total amount of bytes transferred by the Symantec Endpoint Encryption Services website. Click **Add**, then click **Close**.
- 5 On the primary host, the System Monitor should display a periodic burst of data traffic corresponding to the client check-in interval, while all other hosts in the cluster should display a smooth line, indicating no data traffic to the Symantec Endpoint Encryption web service on that host.
- 6 Induce a communication failure in the primary host by disconnecting it from the network.
- 7 On the secondary host, the System Monitor should display a periodic burst of data traffic corresponding to the client check-in interval, indicating that successful failover has occurred. Other hosts in the cluster should display a smooth line, indicating no traffic to that host.
- 8 Induce a communication failure in the secondary host and verify that client traffic is now flowing to the tertiary host. Repeat steps 6 and 7 for all other hosts in the cluster to verify that failover is working. Finally, reconnect the primary host to the network and verify that clients are once again connecting to the primary host rather than other hosts in the cluster.

Extending Domain User Rights with DSACLS

This chapter includes the following topics:

- [Overview](#)
- [Prerequisites](#)
- [Summary of Steps](#)
- [Install ADAM Administrator Tools](#)
- [Grant List Children & Read Property Access Permissions](#)
- [Testing AD Synchronization](#)

Overview

Although assigning modified permissions can be done in a variety of ways, the technique presented here uses the dscls.exe utility, a separate download and install. The dscls.exe utility is included with the ADAM administrator tools as part of the ADAM SP1 installer.

This technique is discussed in the Microsoft knowledgebase article at the following URL:

<http://support.microsoft.com/kb/892806>

Prerequisites

Before you begin, you'll need:

- The Active Directory synchronization account (see Chapter 1 “[Synchronization Accounts](#)” on page 12).
- The ADAM SP1 installer (32-bit version).
- A Windows Server 2003 machine.

The ADAM SP1 installer may be downloaded from the Microsoft website at the following URL:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=9688F8B9-1034-4EF6-A3E5-2A2A57B5C8E4&displaylang=en>

Make sure that you download the 32-bit version of ADAM SP1 (ADAMSP1_x86_English.exe).

Note: A full installation of ADAM is not required. Only the ADAM administration tools must be installed in order to make the DSACLS utility available.

Summary of Steps

Using a modified non-administrator account with the Active Directory synchronization service requires the following steps:

- 1 Launch the ADAM Setup Wizard and install the ADAM administrator tools only.
- 2 Modify the access permissions for the Active Directory synchronization account using the dscls.exe utility.
- 3 Install the Management Server, and specify the Active Directory synchronization account in the **Directory Service Synchronization** page of the Management Server InstallShield Wizard.
- 4 Test the proper functioning of the Active Directory synchronization service running with the modified non-administrator account.

In the following steps of the Management Server install process, you will set the permissions on the Active Directory synchronization account. You will do this by logging on the domain controller as a domain administrator and executing the dscls.exe utility two times with two sets of parameters.

Install ADAM Administrator Tools

From your Windows Server 2003 machine, launch the ADAM SP1 installer application (ADAMSP1_x86_English.exe). Click **Next**. The **License Agreement** page of the ADAM Setup Wizard appears. Select the option **I Agree**, then click **Next**. Select **ADAM administration tools only**, and then click **Next**. On the final installation screen, click **Finish**.

Grant List Children & Read Property Access Permissions

When you execute the dscls.exe utility, you will grant the ability of the designated domain user account to read and list the children of all objects in Active Directory, including the deleted objects container. Applying this permission is necessary to allow the proper functioning of the Active Directory synchronization service.

The permissions string ("**LCRP**") in the following command line represents the list of granted operations. These operations are:

- List the children of an object, and
- Read property.

Log on to the domain controller using the domain administrator account. Click **Start**, click **Run**, type **cmd**, then click **OK** to open a new command prompt window.

To perform this procedure

- 1 At the **C:\WINDOWS\ADAM>** command prompt, type the following command and press **Enter**:
dscls.exe "CN=Deleted Objects,dc=your-org,dc=com" /takeownership

Be sure to replace the *dc=your-org,dc=com* entry with the distinguished name of your own domain.

- 2 At the **C:\WINDOWS\ADAM>** command prompt, type the following command, and press **Enter**:
dscls.exe "CN=Deleted Objects,dc=your-org,dc=com" /G "your-org\adsyncuser":LCRP

Be sure to replace the *dc=your-org,dc=com* entry with the distinguished name of your own domain, and replace the **your-org\adsyncuser** entry with the domain name and user name of your own Active Directory synchronization account.

Having modified the Active Directory synchronization account, you can now proceed to the Management Server installation, and enter this account in the Directory Service Synchronization page of the Management Server InstallShield Wizard.

Testing AD Synchronization

In order to verify the proper functioning of the Active Directory synchronization service, perform the following steps:

- 1 Create a new computer object in Active Directory.
- 2 Access the Symantec Endpoint Encryption database using the Microsoft SQL Server Management Studio (part of an optional install of tools for SQL Server 2005) using system administrator-level privileges, and verify that the newly created computer object is present in the dbo.ADComputers table of the SEEMSdb database.
- 3 Delete the new computer you just created.
- 4 Either wait for synchronization to occur, or force synchronization to take place using the Configuration Manager. See [“Directory Sync Service Status”](#) on page 109.
- 5 Using Microsoft SQL Server Management Studio, verify that the newly created computer object has been deleted from the dbo.ADComputers table of the SEEMSdb database.

Certificates & Token Software Settings

This chapter includes the following topics:

- [Overview](#)
- [Symantec Endpoint Encryption Authentication Certificates](#)
- [Required Token Software Configuration](#)
- [Recommended Token Software Configuration](#)

Overview

This appendix details the required key usage extensions for certificates used to authenticate to Symantec Endpoint Encryption.

In addition, this appendix details required and recommended settings for the token software.

Symantec Endpoint Encryption Authentication Certificates

Issuance from Windows Server 2003

If the operating system of the certificate authority machine is Windows Server 2003, ensure that you have downloaded and applied the following Microsoft patch before issuing the certificates:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=FFAEC8B2-99E0-427A-8110-2F745059A02D&displaylang=en>

Single Certificate on Token

If multiple certificates with the required key usages and extended key usages reside on a single token, the user will be prompted to select the appropriate certificate when they register and each time they log on to the User Client Console. The Client Administrator will be prompted to select the certificate when logging on to the Administrator Client Console. Refer to the *User Guide* and *Client Administrator Guide* for more details about the appearance and presentation of the **Certificate Selection** dialog.

The manual selection of the appropriate certificate is not only cumbersome for the individual user and Client Administrator, it also introduces the possibility of human error. To avoid this, ensure that only a single certificate with the required key usage and extended key usage extensions exists on each token.

Required Key Usage

The key usage on the certificate to be used for authentication to Symantec Endpoint Encryption must be set as described in the following table. While the certificate must possess these key usages, additional key usages will not prevent the certificate from being used for authentication.

Table C-1 Required Key Usage for Symantec Endpoint Encryption Authentication Certificates

Token Type	Name	Also Known As
RSA SID800	keyEncipherment	Key Encipherment
Smart card	dataEncipherment	Data Encipherment
Aladdin eToken		
Common Access Card (CAC)	keyEncipherment	Key Encipherment
SafeSign v2.1		
Personal Identity Verification (PIV)	digitalSignature	Digital Signature

Required Extended Key Usage

The extended key usage (sometimes called “enhanced key usage”) on the certificate to be used for authentication to Symantec Endpoint Encryption must be set as described in the following table. While the certificate must possess these extended key usages, additional extended key usages will not prevent the certificate from being used for authentication.

Table C-2 Required Extended Key Usage for Symantec Endpoint Encryption Authentication Certificates

Token Type	OID	Name	Also Known As
RSA SID800	1.3.6.1.5.5.7.3.4	emailProtection	Email Protection
Smart card			Secure Email
Aladdin eToken			
Common Access Card (CAC)	—	—	—
Personal Identity Verification (PIV)	1.3.6.1.5.5.7.3.2	clientAuth	Client Authentication

Required Token Software Configuration

When installing the Access Client, select the **Custom** option on the **Setup Type** page and ensure that the settings shown in Table C.3 are selected.

Table C-3 Access Client Token Software Settings

Option	Value
Card Authentication Management	This feature will not be available
CMC Administrator	This feature will be installed on local hard drive
COVE Administrator	This feature will be installed on local hard drive
Reflex Tools	This feature will be installed on local hard drive
Smart Card Credential Provider*	This feature will be installed on local hard drive

** This option is displayed only when you are installing the Access Client on a Windows Vista or Windows 7 workstation.*

Note: After completing the installation of Axalto Access Client 5.3, open the Axalto installation directory. By default, this will be C:\Program Files\Axalto\Access Client\v5\. Locate the following files: xltccc.dll and xltGscProxy.dll. Copy these files to the Windows Clipboard. Paste them into the \Windows\System32\ directory.

Recommended Token Software Configuration

Basics

The token software should be configured to ensure that certificates are inserted into the Windows certificate store upon user logon or token insertion, and removed from the certificate store upon user logoff or token removal.

In addition, the token software should be configured to disallow PIN caching. Otherwise, users could gain access to the User Client Console even after providing an invalid PIN.

The following sections detail the settings that should be made within the client token software to achieve both of these ends.

Note: The settings are unavailable on the RSA client software. Please refer to the RSA documentation for the best method of ensuring that the certificates and PINs are not cached.

ActivClient

When installing ActivClient, select the **Custom** option on the **Setup Type** page and ensure that the **Advanced Configuration Manager** is selected to be installed.

Following installation, configure the ActivClient software as shown in Table C.4.

Table C-4 ActivClient Token Software Settings

Area Configured	Parameter	Value
Certificate Availability	Make certificates available to Windows on card insertion	Yes
	Remove certificates from Windows on smart card removal	Yes
	Remove certificates from Windows on logoff	Yes

eToken PKI Client

Configure the Aladdin eToken PKI Client software as shown in Table C.5.

Table C-5 Aladdin eToken PKI Client Token Software Settings

Panel	Tab	Parameter	Value
eToken PKI Client Settings	Advanced	Copy user certificates to a local store	Selected
		Enable Single Sign-On mode	Deselected

Mapped Windows Domain Account Privileges

This chapter includes the following topics:

- [Overview](#)
- [Prerequisites](#)
- [Summary of Steps](#)
- [Add Metabase Permissions](#)
- [Add Other Permissions](#)

Overview

The Symantec Endpoint Encryption Management Server can be configured during setup to authenticate to the database using Windows authentication. This is to accommodate environments that restrict the use of SQL authentication and SQL servers operating in mixed mode.

To use Windows Authentication, you must provision a Windows domain account with special privileges prior to installation of the Symantec Endpoint Encryption Management Server.

Prerequisites

Before you begin, you must:

- Configure your SQL server to use Windows Authentication mode.
- Designate a Windows domain account for use as the Management Server account.

Summary of Steps

Preparing a Windows domain account for use as the Management Server account requires the following steps:

- 1 Add metabase permissions for the account using the `aspnet_regiis.exe` utility.
- 2 Add folder permissions for the account.

Add Metabase Permissions

Use the ASP.NET IIS Registration Tool (`aspnet_regiis.exe`) to grant the account access to the IIS metabase and other directories used by ASP.NET. Execution of this command will also add the account to the `IIS_WPG` group and grant the account “log on as a batch job” permission.

Log on to the Management Server using a domain administrator account. Click **Start**, click **Run**, type **cmd**, then click **OK** to open a new command prompt window.

To perform this procedure

- 1 At the command prompt, change to the following directory:
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727
- 2 At the command prompt, type the following command and press **Enter**:
aspnet_regiis.exe -ga domain_name\user_name

Be sure to replace the *domain_name\user_name* entry with the Windows domain name.

Add Other Permissions

Grant the account read and write access to the following directories:

- %SystemRoot%\Temp
- %SystemRoot%\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files

Grant the account “log on as a service” permission.

Grant the account read and write access to the registry.

Grant the account read and write access to the log directory. The logs are located at:

C:\Program Files\Symantec\Symantec Endpoint Encryption Management Server\Services\Logs

Log on to the Management Server using a domain administrator account and apply the permissions using the method of your choice.

Having modified the account, you can now proceed to the Management Server installation and specify this account for use as the Management Server account in the Management Server InstallShield Wizard.

Installation Settings Honored by Mac Clients

Refer to the following table for the installation settings that are honored by Mac clients.

Table E-1 Installation Settings Honored by Mac Clients

Policy Panel	Ignored	Honored	Partially Honored	Notes
Framework – Client Administrator			•	Only the default Client Administrator account.
Framework – Registered Users	•			
Framework – Single Sign-On	•			
Framework – Password Authentication			•	Only the settings in the Password Complexity area.
Framework – Token Authentication	•			
Framework – Authentication Message		•		
Framework – Authenti-Check	•			
Framework – One-Time Password	•			
Framework – Communication		•		
Framework – Encryption		•		
Full Disk – Startup			•	Only the text in the Logon instructions and Legal notice boxes.
Full Disk – Logon History	•			
Full Disk – Encryption	•			
Full Disk – Installer Customization	•			
Full Disk – Hardware Configuration	•			
Full Disk – Client Monitor	•			

Taking Additional Drives Under Full Disk Management

This chapter includes the following topics:

- [About Taking Additional Drives Under Full Disk Management](#)
- [Adding the Physical Disk Drive](#)
- [Configuring the Logical Drives](#)
- [Creating the Framework Client Upgrade Package](#)
- [Creating the Full Disk Client Upgrade Package](#)
- [Creating the Removable Storage Client Upgrade Package](#)
- [Deploying the Client Upgrade Packages](#)
- [Verifying That the Additional Drives Have Been Taken Under Management](#)

About Taking Additional Drives Under Full Disk Management

After installing Full Disk on a Windows client, you may need to add one or more fixed drives. For example, the client may run out of hard disk space and need a secondary drive added. Complete the following steps to take additional drives under Full Disk management.

Table F-1 Process for Taking Additional Drives Under Full Disk Management

Step	Task
1	Add the drive to your computer. See “Adding the Physical Disk Drive” on page 130.
2	Configure the new physical disk. See “Configuring the Logical Drives” on page 130.
3	Create a Framework Client upgrade package. See “Creating the Framework Client Upgrade Package” on page 130.
4	Create a Full Disk upgrade package. See “Creating the Full Disk Client Upgrade Package” on page 130.
5	Create a Removable Storage upgrade package, if needed. See “Creating the Removable Storage Client Upgrade Package” on page 131.
6	Deploy the package or packages to the computer with the new disk drive. See “Deploying the Client Upgrade Packages” on page 131.
7	Verify that the new drive is managed. See “Verifying That the Additional Drives Have Been Taken Under Management” on page 131.

Note: This procedure details how to add a physical disk drive to a Windows computer. Adding secondary disks to a Mac OS X computer is not supported.

Adding the Physical Disk Drive

To add the physical disk drive:

- 1 Power off.
- 2 Follow the instructions from the hardware manufacturer for adding an internal, secondary, fixed disk drive.

Configuring the Logical Drives

To configure the logical drives:

- 1 Power on.
- 2 Follow the instructions from Microsoft configure the newly added physical disk into one or more logical drives.
- 3 Ensure that the new disk is formatted and partitioned to your permanent liking

Note: You won't be able to repartition, resize partitions, reformat the drive, or change the drive letter(s) after completing this procedure.

Creating the Framework Client Upgrade Package

To create a Framework client upgrade package:

- 1 Launch a Manager Console of version 8.2.0 or later.
- 2 Expand the **Symantec Endpoint Encryption Software Setup** snap-in and click **Framework**.
- 3 Select appropriate options in each panel, as they will overwrite the existing settings on the client (Chapter 4 "[Framework Installation Settings Wizard](#)" on page 52).

Note: The client will ignore the Encryption strength setting.

Creating the Full Disk Client Upgrade Package

To create a Full Disk client upgrade package:

- 1 Launch a Manager Console of version 8.2.0 or later.
- 2 Expand the **Symantec Endpoint Encryption Software Setup** snap-in and click **Full Disk**.
- 3 Select appropriate options in the Startup (Chapter 4 "[Startup](#)" on page 66) and Logon History (Chapter 4 "[Logon History](#)" on page 68) panels before clicking **Next**.
- 4 In the Encryption panel, select **Encrypt all disks** in the **Disk Drives** area to allow the potential encryption of the new logical drives.
- 5 Select the option in the **Disk Partitions** area that corresponds to your desired outcome:
 - To ensure the immediate encryption of all logical drives on the new physical drive, select **Encrypt all partitions upon installation**.

- To encrypt only certain logical drives on the new physical drive, select **Encrypt these partitions upon installation**. Then type the letters of the drives that should be encrypted in the box.
 - To allow users to manually initiate the encryption of the logical drives on the new physical drive, select **Let users choose partitions and start the encryption**.
- 6 Leave all other settings at the default as the client will ignore them.
 - 7 Click **Next**.
 - 8 Leave the settings in the Installer Customization panel at their defaults as the client will ignore them.
 - 9 Click **Next**.
 - 10 In the Client Monitor panel, select appropriate options (Chapter 4 “[Client Monitor](#)” on page 71) before clicking **Next**.
 - 11 In the Hardware Configuration panel, click **Next**.
 - 12 In the Mac Client Package panel, click **Finish**.

Creating the Removable Storage Client Upgrade Package

If the target client is running Removable Storage, create a Removable Storage client installation package as well. Framework, Full Disk, and Removable Storage must be upgraded together. If the client isn't running Removable Storage, you can skip this step.

Deploying the Client Upgrade Packages

To deploy the client upgrade packages:

- 1 Locate the MSI files appropriate to the operating system of the target computer.
 - For a client with 64-bit Windows, you'll need the MSI packages with `_64` suffixes, e.g., Symantec Endpoint Encryption Framework Client_64.msi and Symantec Endpoint Encryption Full Disk Edition Client_64.msi.
 - For a client with 32-bit Windows, you'll need the MSI packages without `_64` suffixes, e.g., Symantec Endpoint Encryption Framework Client.msi and Symantec Endpoint Encryption Full Disk Edition Client.msi.
- 2 Use one of the following methods to deploy the packages to the client in question
 - Chapter 6 “[Upgrading Windows Clients Using a Third Party Tool](#)” on page 93
 - Chapter 6 “[Upgrading Windows Clients Using a GPO](#)” on page 94
 - Chapter 6 “[Performing a Manual Upgrade of a Windows Client](#)” on page 96

Verifying That the Additional Drives Have Been Taken Under Management

To verify that the additional drives have been taken under management:

- 1 On the client, launch either the User Client Console or the Administrator Client Console and log on.
- 2 Click either the *Encryption* or the *Decryption* link in the navigation pane.
- 3 The additional drives should be listed in the upper section with check boxes beside them, indicating their availability for encryption or decryption. If the additional drives are listed in the **Partitions not Managed by SEE** area, the procedure was unsuccessful.

Glossary

Active Directory Policies	One of two types of policies that can be created and deployed from the Symantec Endpoint Encryption Manager. They feature seamless integration with well-known Active Directory toolsets and include user as well as computer policies.
Authenti-Check	Allows users on Windows endpoints to recover from forgotten credentials without help desk assistance. The user authenticates with a set of up to three question-answer pairs. Authenti-Check is not available to Client Administrators or Mac users.
Autologon	Allows Policy Administrators to remotely deploy software to computers protected by Full Disk. Software installations typically require several restarts, and Autologon allows pre-boot authentication to be bypassed, so that the computer does not require any credentials before loading Windows.
Autologon Utility	Used by administrators to configure and create Autologon MSI packages for deployment to Client Computers.
Automatic Authentication	<p>If a Client Computer is set for automatic authentication, Full Disk will not require a user to provide Symantec Endpoint Encryption credentials before allowing Windows to load. This option relies on Windows to authenticate users.</p> <p>In addition, users will be registered automatically unless a registration password is required. Requiring a registration password serves to avoid reaching the maximum registered user limit and to limit the number of users that can gain access to the User Client Console.</p> <p>The automatic authentication feature is not available for Mac endpoints.</p>
Client Administrator	<p>Provides local support to Symantec Endpoint Encryption users. The Policy Administrator assigns each Client Administrator account individual administrative privileges:</p> <ul style="list-style-type: none">■ <i>Unregister users</i>—allows Client Administrators to unregister registered users;■ <i>Decrypt drives</i>—provides Client Administrators with the right to decrypt drives encrypted by Symantec Endpoint Encryption Full Disk;■ <i>Extend lockout</i>—permits Client Administrators to extend the Client Computer's next communication date; and■ <i>Unlock</i>—enables Client Administrators to unlock Client Computers that have been locked for failure to communicate with the Symantec Endpoint Encryption Management Server. <p>Client Administrators are always able to authenticate to Client Computers and can always initiate encryption on a Windows client.</p> <p>Client Administrators cannot change their own passwords or use any password-recovery methods.</p>
Client Database	The client database consists of a series of volume files and is part of the Symantec Endpoint Encryption file system. Once the location of the client database files has been specified during the creation of the Client Computer installation packages and the installation has completed, these files must never be moved or disturbed.
Database Communication Account	An account created by a version of Symantec Endpoint Encryption Framework 7.0.8 or earlier during installation of the Symantec Endpoint Encryption Management Server.
Management Password	The Management Password controls administrator access to Recover /B, Recover /O, Recover /S, the Help Desk Program, and the Autologon utility.
Management Password Snap-in	The Management Password snap-in allows you to change the Management Password.

Management Server Account	A Microsoft SQL Server account or Windows domain account used for communication between the Symantec Endpoint Encryption Management Server and the Symantec Endpoint Encryption database, as well as for Management Server services. When SQL authentication is chosen during installation of the Management Server, a SQL Server account is created by the installer. This SQL Server account has execute permissions to the database catalog and has the following database roles: db_datareader, db_datawriter, and public. When Windows authentication is chosen during installation of the Management Server, you must specify a Windows domain account that you have already provisioned with special permissions. See Appendix D “ Mapped Windows Domain Account Privileges ” on page 125.
Native Policies	One of two types of policies that can be created and deployed from the Symantec Endpoint Encryption Manager. Native policies do not rely on any existing directory service and apply to computers only.
One-Time Password (OTP) Program	The One-Time Password (OTP) Program allows Full Disk users on Windows endpoints to recover from a forgotten password, PIN, or token with help desk assistance. Users can also use the OTP program to regain access to their Windows computer after it has been locked for a failure to communicate with the Symantec Endpoint Encryption Management Server. To complete the OTP process the user must contact the help desk.
OTP Key	A critical value used to ensure the identity of Client Computers during communication with the Symantec Endpoint Encryption Management Server and for the One-Time Password password recovery feature. When the Symantec Endpoint Encryption Manager is installed for the first time, it populates the Symantec Endpoint Encryption database with the OTP key.
Policy Administrator	<p>Performs centralized administration of Symantec Endpoint Encryption. Using the Manager Console and the Manager Computer, the Policy Administrator:</p> <ul style="list-style-type: none"> ■ Updates and sets client policies. ■ Issues commands to encrypt or decrypt endpoint drives and/or partitions. ■ Runs reports. ■ Changes the Management Password. ■ Runs the Help Desk Program. ■ Creates the computer-specific Recover DAT file necessary for Recover /B, for Recover /O, and Recover /S. <p>Domain or higher-level administrators can restrict access to Symantec Endpoint Encryption snap-ins when assigning specific Policy Administrator duties.</p>
Pre-Windows Environment	The Pre-Windows environment loads upon reboot, before the Windows operating system. This environment helps protect the Client Computer’s hard disks by requiring authentication before a user gains access to Windows.
Recover Program	<p>Used when a Windows Client Computer encounters a serious error and cannot load Windows. Client Administrators should first use the Recover Program to repair the Symantec Endpoint Encryption client database files (Recover /A and /O). Should this fail, the Recover Program offers additional options for non-Opal-compliant drives:</p> <p>An emergency decryption of the hard disk (Recover /D).</p> <p>A restoration of the encryption keys (Recover /B).</p> <p>The Recover Program also offers a secure erase function for Opal-compliant drives (Recover /S).</p>
Registration	During registration, users set their credentials so that they can authenticate in pre-Windows. In addition, users may be asked to set password recovery information. Registration may be configured to occur with or without the user’s intervention. The first user is required to register after the designated number of grace restarts has expired.
Server-Based Command	<p>A command issued from a Symantec Endpoint Encryption Manager Console snap-in to encrypt or decrypt fixed disk drives on endpoints that:</p> <p>Are running Windows,</p> <p>Have no Opal-compliant drives, and</p> <p>Are installed with Symantec Endpoint Encryption Full Disk 8.2.0 or later.</p> <p>Clients receive commands when they check in with the Management Server. Commands expire in 30 days. Commands can be cancelled if they have not yet been received.</p>

Serverless Mode	A type of Symantec Endpoint Encryption Manager installation that requires no connection to a Symantec Endpoint Encryption database. Client packages created from a serverless Symantec Endpoint Encryption Manager produce Windows clients that do not communicate with a Symantec Endpoint Encryption Management Server. For more information, refer to the <i>Serverless Mode Supplement</i> .
Silent Client	A silent client is a Client Computer installed from a Framework Client package created from a Symantec Endpoint Encryption Manager Console whose installation mode does not require connection to Symantec Endpoint Encryption Management Server. Silent clients do not communicate with the Symantec Endpoint Encryption Management Server. If the computer has never checked in, the online method of the One-Time Password recovery method and the Recover /B, Recover /O, and Recover /S hard disk recovery options—which require computer-specific data stored in the database during check-in—are not available.
Single Sign-On (SSO)	If SSO is enabled, the user logs on once in pre-Windows and is then authenticated to Windows.
Symantec Endpoint Encryption Database	Created on the designated Microsoft SQL Server instance by the Symantec Endpoint Encryption Management Server installer. It is populated and kept up to date by the Symantec Endpoint Encryption Management Server which communicates with the Client Computers and directory service servers (if any).
Symantec Endpoint Encryption Framework	Provides Symantec Endpoint Encryption-wide features, such as authentication methods and settings, as well as registered user and Client Administrator accounts and information.
Symantec Endpoint Encryption Management Server	Acts as both a web and application server. It enables all aspects of Symantec Endpoint Encryption policy management and application, stores data reported by Client Computers in the Symantec Endpoint Encryption database, and (optionally) synchronizes information from Active Directory and/or eDirectory with the Symantec Endpoint Encryption database.
Symantec Endpoint Encryption Multi-Factor Authentication	Allows organizations to achieve two-factor authentication on Windows endpoints with support for X.509 certificates, a variety of tokens and smart cards, as well as both USB and PCMCIA readers.
Symantec Endpoint Encryption Password	Used by users and Client Administrators for Pre-Windows authentication and Client Console logons. Also used by Client Administrators to authenticate to Recover /A and Recover /D.
Symantec Endpoint Encryption Software Setup Snap-in	Allows Symantec Endpoint Encryption client software to be customized before deployment.
User	<p>At least one user must register with Symantec Endpoint Encryption on each Client Computer. A wizard guides the user through the registration process, which involves a maximum of five screens. The registration process can also be configured to occur without user intervention.</p> <p>Users authenticate to Full Disk in one of three ways:</p> <ul style="list-style-type: none"> ■ <i>Single Sign-On enabled</i>—The user is prompted to authenticate each time they restart their computer. ■ <i>Single Sign-On not enabled</i>—The user must log on twice: once to Full Disk and then separately to Windows. ■ <i>Automatic authentication enabled</i>—The user is not prompted for Full Disk credentials; the authentication process is transparent. This option relies on Windows to validate the user's credentials. <p>On Mac endpoints, the first user account is created at the time that encryption of the disk is manually initiated. Additional user accounts can be added later.</p>

Index

A

- Active Directory
 - domain 3
- administrative templates 47-49
- Authenti-Check 61-62
- automatic authentication 15, 55, 133, 135

C

- Client Administrator
 - accounts
 - creation of 53
 - authentication method (password or token) 53
 - single-source passwords 13
- Client Computer
 - installation of 51, 75-81
 - keyboard support 6, 7
 - system requirements 6
 - token reader support 10-11
 - token support 8
 - uninstallation 103
- client installation packages
 - creation 52-74
 - GPO deployment 66
 - protection of 75
 - third party tool deployment 76, 103
 - upgrades and 94
- client packages
 - deploying by GPO 77
 - uninstalling 103
- Common Access Card (CAC) 40

D

- database communications account 25

E

- Encryption
 - Full Disk installation settings 69
- encryption method
 - selecting 70

F

- Framework installation settings
 - Authentication Message 60
 - Authenti-Check 61
 - Client Administrators 52
 - Communication 63
 - Encryption 65
 - One-Time Password 62
 - Password Authentication 57
 - Registered Users 54
 - Single Sign-On 57
 - Token Authentication 60

- Full Disk installation settings
 - Client Monitor 71
 - Encryption 69
 - Installer Customization 70
 - Logon History 68
 - Startup 66

G

- Grace restarts 56
- Group Policy Object Editor 77

H

- Hardware Configuration
 - Full Disk installation settings 71

I

- installation
 - completion tasks 42
- Installer Customization
 - Full Disk installation settings 70
- installing
 - client packages 70

L

- Logon History
 - Full Disk installation settings 68

M

- Management Password
 - changing 42
 - complexity requirements 42
 - use of 133
- Management Server account
 - choose database authentication type 24
 - defined 134
 - with SQL authentication 11
 - with Windows authentication 11
- Manager Console
 - add forest 46
 - location of 2

O

- OTP communication unlock installation setting 63

P

- Password aging 59, 60
- Password Authentication
 - installation settings 57
- Password complexity 59
- Password history 59
- Port/Protocol 3

R

- Recover Program 133
 - /B, /O, and /S options 135
- Registered Users
 - installation settings 54
- Restarts
 - grace 56
- restricting access to snap-in extensions 48

S

- Safe Mode Boot for registered users installation setting 68
- SEE roles 13
- segmenting support duties 50
- Single Sign-On
 - installation settings 57
- snap-in extensions
 - restricting access to 48
- Startup
 - Full Disk installation settings 66

T

- token authentication certificate
 - required key usage 11, 122

U

- uninstalling
 - client packages 103
- users
 - local administrative rights and 15