EMC® VMAX® Family

Security Configuration Guide

REV 03

EMC²

Copyright © 2002 - 2014 EMC Corporation. All rights reserved. Published in the USA.

Published November, 2014

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided as is. EMC Corporation makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date regulatory document for your product line, go to the technical documentation and advisories section on the EMC online support web site.

CONTENTS

Preface

Chapter 1 Overview

What's new 13
Other security documentation 13

Chapter 2 Security Configuration Checklists

Solutions Enabler checklist 16
Unisphere for VMAX checklist 19
vApp Manager checklist 19
SMI-S checklist 20

Chapter 3 Solutions Enabler security configuration tasks

SYMAPI home and bin directory locations 21
Security controls map 22
Access control 23
Host-based access control 23
User-based access control 28
Log files and settings 30
Managing log file retention 32
Assigning a custom audit log activity ID 34
Port usage 34
Options to modify port settings 36
Solutions Enabler client/server security settings 36
Securing remote connections using SSL 37
Configuring the Solutions Enabler server host 38
Configuring the Solutions Enabler client host 40
Secure session configuration summary 41
Managing certificate files 42
Managing certificate files 48
Managing the Solutions Enabler server 52
Data security settings 57
Securing Solutions Enabler configuration files 58
Running commands as a non-privileged user 58
Managing the encrypted lockbox 58
About lockbox passwords 59
Changing the lockbox password/SSVs 60
Daemon security settings 61
Daemon identity on UNIX 62
Securing host directories 62
Authorizing daemon connections 64
Securing SRM operations 65
Authorizing SRM daemon connections 65
Setting operating-system-level permissions for SRM 66
Connecting to the SRM database 66
Database start-up options 67
Maintenance: back up Solutions Enabler state 69

Chapter 4 Unisphere for VMAX security configuration tasks

Security controls map ... 72
Unisphere access control ... 72
User-based access control ... 73
About user authorization ... 76
Assigning user authorization ... 76
Using the encrypted lockbox ... 78
Resetting the host system SSVs ... 79
Replacing the Unisphere for VMAX server certificate ... 79
Other security settings ... 81
Port usage ... 82
Link-and-launch security ... 82
Unisphere data security ... 83
Security alert system ... 83
Session timeout ... 83
Root access requirements ... 83

Chapter 5 vApp Manager security configuration tasks

Security controls map ... 85
Secure deployment settings ... 86
User-based access control ... 86
Component access control ... 87
Log files and settings ... 87
Log file management ... 88
Port usage ... 88
Manage SSL certificates ... 88
Data security settings ... 89
Secure serviceability ... 89
Alerts ... 89
Managing Clam anti-virus ... 90
Maintenance ... 91

Chapter 6 SMI-S security configuration tasks

Security controls map ... 93
User-based access control ... 94
User authorization ... 94
User authentication ... 94
Administrator user account ... 95
Component access control ... 97
Log files and settings ... 97
Displaying log files ... 97
Port usage ... 97
Network encryption ... 97
VMAX3, SMI-S Group Replication and Solutions Enabler GNS Global Mode 98
Securely deploying SMI-S ... 99
Manage the encrypted lockbox ... 99
Create the CST lockbox ... 99
Other security settings ... 100
Security alerts ... 100

Chapter 7 Embedded NAS

Security controls map 101

PREFACE

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your EMC representative if a product does not function properly or does not function as described in this document.

Note: This document was accurate at publication time. New versions of this document might be released on EMC Online Support at www.support.EMC.com. Check EMC Online Support to ensure that you are using the latest version of this document.

Purpose

This guide helps you to securely deploy and maintain VMAX arrays, including Solutions Enabler version 8.0.1 (Solutions Enabler), Unisphere® for VMAX® version 8.0.1 (Unisphere), SMI-S, and vApp Manager. This guide provides references to VNX documentation to help you securely deploy embedded NAS.

Audience

This manual provides reference information for configuring and managing security on VMAX arrays.

Related documentation

Solutions Enabler

The following documents provide additional information about Solutions Enabler:

- *EMC Solutions Enabler Release Notes* — Describes the contents of your kit and how to prepare for an installation. These release notes identify any known functionality restrictions and performance issues that may exist with the current version and your specific storage environment.
- *EMC Solutions Enabler Installation Guide* - Provides host-specific installation instructions.
- *EMC Solutions Enabler CLI Command Reference* - Documents the SYMCLI commands, daemons, error codes and option file parameters provided with the Solutions Enabler man pages.
- *EMC Solutions Enabler Array Management CLI User Guide* - Describes how to configure array control, management, and migration operations using SYMCLI commands.
- *EMC Solutions Enabler SRM CLI User Guide* - Provides Storage Resource Management (SRM) information related to various data objects and data handling facilities.

VMAX platform

- *EMC VMAX3 Family Documentation Set* — Contains the product guide, physical planning guide, and power documentation for the VMAX3 arrays.

- *EMC VMAX3 Family with HYPERMAX OS Product Guide* - Describes the VMAX3 platform and software products.
- *EMC Solutions Enabler Documentation Set* — Contains all the product guides and installation manuals needed to manage your array using the Solutions Enabler SYMCLI mechanisms.
- *EMC VMAX3 Family HYPERMAX OS Release Notes* — Identifies any known functionality restrictions and performance issues that may exist with the current version and your specific storage environment.

Additional information

- *EMC VMAX Family Viewer for Desktop and iPad®* - Illustrates system hardware, incrementally scalable system configurations, and available host connectivity offered for VMAX arrays.
- E-Lab™ Interoperability Navigator (ELN) - Provides a web-based interoperability and solution search portal. You can find the ELN at https://elabnavigator.EMC.com.
- SolVe Desktop - Provides links to documentation, procedures for common tasks, and connectivity information for 2-site and 3-site SRDF configurations. To download the SolVe Desktop tool, go to EMC Online Support at https://support.EMC.com and search for SolVe Desktop. Download the SolVe Desktop and load the VMAX Family and DMX procedure generator.

  Note: You need to authenticate (authorize) your SolVe Desktop. Once it is installed, please familiarize yourself with the information under Help tab.

Conventions used in this document

EMC uses the following conventions for special notices:

Note: A note presents information that is important, but not hazard-related.

IMPORTANT

An important notice contains information essential to software or hardware operation.

NOTICE

NOTICE is used to address practices not related to personal injury.

Typographical conventions

EMC uses the following type style conventions in this document:

Normal	Used in running (nonprocedural) text for: • Names of interface elements, such as names of windows, dialog boxes, buttons, fields, and menus • Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, functions, and utilities • URLs, pathnames, file names, directory names, computer names, links, groups, service keys, file systems, and notifications
Bold	Used in running (nonprocedural) text for names of commands, daemons, options, programs, processes, services, applications, utilities, kernels, notifications, system calls, and man pages Used in procedures for: • Names of interface elements, such as names of windows, dialog boxes, buttons, fields, and menus • What the user specifically selects, clicks, presses, or types
Italic	Used in all text (including procedures) for: • Full titles of publications referenced in text • Emphasis, for example, a new term • Variables
`Courier`	Used for: • System output, such as an error message or script • URLs, complete paths, file names, prompts, and syntax when shown outside of running text
`Courier bold`	Used for specific user input, such as commands
`Courier italic`	Used in procedures for: • Variables on the command line • User input variables
< >	Angle brackets enclose parameter or variable values supplied by the user
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections — the bar means “or”
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Revision history

Table 1 lists the revision history of this document.

Table 1

Revision	New/revised content
03	New content describing security procedures for SMI-S and an introduction to Embedded NAS: • "SMI-S checklist" • "SMI-S security configuration tasks" • "Embedded NAS"
02	New title: EMC VMAX Family Security Configuration Guide. New content describing security procedures for vApp Manager: • "vApp Manager checklist" • "vApp Manager security configuration tasks" Updates for Solutions Enabler 8.0 and Unisphere for VMAX 1.6: • "Solutions Enabler 8.0 multiple authorization roles", • "Unisphere 1.6 multiple authorization roles", • "Managing the encrypted lockbox"(Solutions Enabler), • "Using the encrypted lockbox" (Unisphere)
01	EMC Symmetrix Security Configuration Guide for Solutions Enabler 7.6 and Unisphere for VMAX 1.5.

Where to get help

EMC support, product, and licensing information can be obtained on EMC Online Support as described next.

Note: To open a service request through EMC Online Support, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or to answer any questions about your account.

Product information — For documentation, release notes, software updates, or for information about EMC products, licensing, and service, refer to EMC online support.

Technical support — For technical support, go to EMC online support. On the Support page, you will see several options, including one for making a service request. Note that to open a service request, you must have a valid support agreement. Please contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

SolVE Desktop — A tool, the replacement for the Interactive Procedure Generators (IPG), provides procedures for common tasks and automatically provides relevant alerts from the EMC knowledgebase and FCOs.

Note: The executable date does not reflect the version of the generators.

Hardware Documentation Viewer — Located within the SolVe Desktop the Viewer includes the documents required by Customer Engineers. To access the Symmetrix Hardware Document Viewer go to EMC Online Support and enter Solve Desktop in the Search and change Scope by resource to Support Tools in the pull down selection.

Select the SolVe Desktop link. If it is your first time accessing the SolVe Desktop application it may be necessary to get authorized.

System Viewer — Illustrates the system hardware, incrementally scalable system configurations, and available host connectivity offered for Symmetrix VMAX systems, go to the EMC online support, and download this stand-alone utility.

eLicensing support

To activate your entitlements and obtain your license files, visit the Service Center on `http://support.EMC.com`, as directed on your License Authorization Code (LAC) letter emailed to you.

For help with missing or incorrect entitlements after activation (that is, expected functionality remains unavailable because it is not licensed), contact your EMC Account Representative or Authorized Reseller.

For help with any errors applying license files through Solutions Enabler, contact the EMC Customer Support Center.

If you are missing a LAC letter, or require further instructions on activating your licenses through EMC Online Support, contact EMC's worldwide Licensing team at licensing@emc.com or call:

- North America, Latin America, APJK, Australia, New Zealand: SVC4EMC (800-782-4362) and follow the voice prompts.
- EMEA: +353 (0) 21 4879862 and follow the voice prompts.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to:

VMAXContentFeedback@emc.com

CHAPTER 1
Overview

This section lists links to checklists and tasks to complete security activities, describes changes to the guide since the previous revision, and lists further reading for VMAX security.

The guide is organized as high-level checklists of security-related activities for Solutions Enabler, Unisphere for VMAX, Virtual Appliance (vApp) Manager, and SMI-S:

- Solutions Enabler checklist 16
- Unisphere for VMAX checklist 19
- vApp Manager checklist 19
- SMI-S checklist 20

and procedures to help you complete the activities:

- Solutions Enabler security configuration tasks 21
- Unisphere for VMAX security configuration tasks 71
- vApp Manager security configuration tasks 85
- SMI-S security configuration tasks 93

What's new

The following topics are new in this revision:

- SMI-S Provider - SMI-S defines the open storage management interface that enables the interoperability of multiple vendor's storage management technologies. The following topics describe securing your SMI-S deployment:
  - "SMI-S checklist"
  - "SMI-S security configuration tasks"
- Embedded NAS - Embedded NAS (eNAS) provides the full suite of block and file services of EMC'S VNX Control Station. The following topic describes eNAS:
  - "Embedded NAS"

Other security documentation

"Related documentation" on page 7 lists additional documentation for Solutions Enabler, VMAX platform, and Unisphere for VMAX.

SAN security

Securing SAN networks, deterring common attacks, mechanisms to enhance SAN security, and insight on implementing product-specific security are described in *EMC Building Secure SANs TechBook*, version 4.0.

Unisphere for VMAX

- Unisphere user roles, group roles, user IDs, and managing user account settings are described in *Unisphere for VMAX Installation Guide* and the *EMC Unisphere for VMAX* online help.
- Procedures to use EMC Unisphere for VMAX for storage system configuration, management, and monitoring are described in *EMC Unisphere for VMAX Documentation Set*.
- The contents of your kit and how to prepare for an installation are described in *EMC Unisphere for VMAX Release Notes*. These release notes identify any known functionality restrictions and performance issues that may exist with the current version and your specific storage environment.

vApp Manager

vApp Manager for Solutions Enabler online help describes the following procedures:

- Manage user authentication
- Download log files
- Manage certificate files
- Manage Clam Anti-Virus

Device masking and IPSec

Device masking and IPSec are described in *EMC Solutions Enabler Array Management CLI User Guide*.

IMPORTANT

IPSec is not supported in HYPERMAX OS or later.

SMI-S Provider

Securely deploying ECOM is described in *EMC Common Object Manager (ECOM) Toolkit Deployment and Configuration Guide*.

Embedded NAS

Security features to control user and network access, monitor system access and use, and support the transmission of encrypted data are described in *EMC VNX Series Security Guide for VNX.*

CLI commands to manage access control, certificates, LDAP configuration, and other security-related commands are described in *EMC VNX Series Command Line Interface Reference for File.*

CHAPTER 2
Security Configuration Checklists

The following checklists summarize the security-related tasks you should perform to improve the security of your deployment including:

- Solutions Enabler checklist 16
- Unisphere for VMAX checklist 19
- vApp Manager checklist 19
- SMI-S checklist 20

Solutions Enabler checklist

Table 2 Solutions Enabler security configuration checklist (page 1 of 3)

Purpose of activity	Task	Where to learn more
Host-based access control		
Restrict which hosts may access specific functionality.	Configure SYMAPI options. Use the `symacl` command to generate unique ID for each management host.	• "Host-based access control" on page 23 • *EMC Solutions Enabler Array Management CLI User Guide*
Restrict actions hosts can execute.	Configure SYMAPI options and use the `symacl` command to enable use of Alternate Access IDs. Define Access Control Groups, Pools, and Hosts to control what actions management hosts can execute.	• "Host access IDs" on page 23 • "Alternate access IDs" on page 24 • "Enabling alternate access IDs" on page 24 • "Enabling alternate access IDs using a passphrase" on page 25
Restrict which hosts and users may perform management operations.	Use access control or user authorization to restrict hosts.	• "Host-based access control" on page 23 • "User-based access control" on page 28
User-based access control		
Restrict user access to specific functionality.	Use the `symauth` command to limit which users can access specific functionality.	"User-based access control" on page 28
Log files and settings		
Limit the amount of disk space used by Solutions Enabler log files.	Set log file size and configure a log rotation/removal schedule.	• "Log files and settings" on page 30 • "Managing log file retention" on page 32 • *EMC Solutions Enabler Installation Guide*
Conserve disk space used by security logs.	Configure a log rotation/removal schedule.	"Managing log file retention" on page 32
Client/server security settings		
Reduce local attachments between hosts and VMAX arrays.	Use Solutions Enabler in client/server mode to a storsrvd running on a remote host locally attached to the storage.	• *EMC Solutions Enabler SYMCLI Command Reference* • *EMC Solutions Enabler Installation Guide*
Protect access to Solutions Enabler resources through firewalls and NATs.	If a firewall or NAT router is used to protect network resources, you may need to: • Configure the network resources to allow access to specific ports. • Modify related settings in daemon_options.	"Port usage" on page 34
Certificate files		

Table 2 Solutions Enabler security configuration checklist (page 2 of 3)

Purpose of activity	Task	Where to learn more
Require client authentication by the server using client certificates.	Set security_clt_secure_lvl=MUSTVERIFY in the `daemon_options` file.	• "Solutions Enabler client/server security settings" on page 36 • "security_clt_secure_lvl" on page 39
Strengthen your authentication by using custom certificates.	Replace SYMAPI-generated security certificates with more secure customer-supplied certificates.	"Replacing SYMAPI-generated certificates:" on page 48
On client hosts		
Control ports used by the client-side event daemon (`storevntd`).	Modify the port on which the client-side `storevntd` listens.	"Port usage" on page 34
Specify the host (HostName) and port (NNNN) on which the server daemon is listening.	For SYMCLI users, modify the `netcnfg` file with the hostnames or IP addresses of your servers.	"Options to modify port settings" on page 36
On server hosts		
Control the port used by the server daemon (`storsrvd`).	Modify the port on which `storsrvd` listens (resolve port conflicts).	"Options to modify port settings" on page 36
Control startup of the server daemon (`storsrvd`).	Use the `stordaemon install` command to configure storsrvd be started automatically at system boot.	"Starting the Solutions Enabler server" on page 53

Limit the set of client hosts that the server will accept connections from.	Configure the following:
	• `<SYMAPI_HOME>/config/nethost` file,
	• The following entries in the `<SYMAPI_HOME>/config/daemon_options` file:
	`max_sessions`
	`max_sessions_per_host`
	`max_sessions_per_user`
		"Restricting access to the Solutions Enabler server " on page 53

Restrict the functionality that the `storsrvd` daemon is allowed to perform on behalf of remote client hosts.	Edit the following entries in the `<SYMAPI_HOME>/config/options` file:
	`SYMAPI_ACC_ADMIN_VIA_SERVER`
	`SYMAPI_ACC_DISPLAY_VIA_SERVER`
	`SYMAPI_ALLOW_SCRIPTS_VIA_SERVER`
	`SYMAPI_CTRL_VIA_SERVER`
		• "Restricting functionality in the Solutions Enabler server" on page 56
		• "IBM z/OS-specific behavior for control operations" on page 57

Securing directories		
Protect the SYMAPI directory and its contents so that only appropriate administrators have write access.	Protect the `<SYMAPI_HOME>/config` directory.	• "Running commands as a non-privileged user" on page 58 • "Securing Solutions Enabler configuration files" on page 58
Protect the `<SYMAPI_HOME>/db` directory to grant non-root users access.	Configure daemon_users to authorize non-root users to use daemons. Run SYMCLI commands as a non-root or non-Administrator user. Limit write access privileges to the `<SYMAPI_HOME>/db` directory to authorized users only.	
Prevent unauthorized access to the lockbox.	Change the lockbox password immediately after installation to best protect its contents.	"Managing the encrypted lockbox" on page 58

Table 2 Solutions Enabler security configuration checklist (page 3 of 3)

Purpose of activity	Task	Where to learn more
Limit which users have write privileges to the config directory.	Limit access to the `<SYMAPI_HOME>/config` directory to authorized users only. All other users should have limited access (read-only or no access, if possible) to this directory.	"Securing host directories" on page 62
Minimize injection attacks and other issues.	Use the daemon_options secure_directory_path to specify which output directories daemons may write to.	
Securing daemons		
Reduce system exposure by using non-root execution of daemons.	Use the `stordaemon setuser` command to establish a non-root user for daemons, and directory permissions.	"Daemon security settings" on page 61
Securing SRM operations		
Limit access to SRM functionality.	Limit permission to the SRM daemon. Edit the common daemon authorization file, `daemon_users`.	"Authorizing SRM daemon connections" on page 65
Limit security exposure by using a database account in SRM with minimal privileges.	Configure a minimally privileged account for SRM database access	
Protect directories and files.	Restrict access privileges for directories and files.	"Setting operating-system-level permissions for SRM" on page 66
Start up and shut down the database server manager instance.	Configure database startup options.	"Database start-up options" on page 67

Unisphere for VMAX checklist

Table 3 Unisphere for VMAX security configuration checklist

Purpose of activity	Task	Where to learn more
Access control		
Authenticate users with a user account stored on a LDAP-SSL server.	Set up LDAP-SSL authentication.	*Unisphere for VMAX Installation Guide* and online help.
User-based access control		
Restrict the management operations users can perform.	Assign users the minimum access they require.	• "User roles" on page 73, "About user authorization" on page 76 • "Assigning user authorization" on page 76
Certificate files		
Replace generated certificates with customer-supplied (trusted) certificates for secure communications.	Replace pre-generated SSL certificates.	"Replacing the Unisphere for VMAX server certificate" on page 79

vApp Manager checklist

Table 4 vApp Manager security configuration checklist

Purpose of activity	Task	Where to learn more
User-based access control		
Manage user accounts	Use the vApp Manager for Solutions Enabler online help to manage user authentication.	"User-based access control" on page 86
Log files and settings		
Manage log files	Use the vApp Manager for Solutions Enabler online help to download log files.	"Log files and settings" on page 87
Certificate files		
Replace generated certificates with customer-supplied (trusted) certificates for secure communications.	Use the vApp Manager for Solutions Enabler online help to replace pre-generated SSL certificates.	"Manage SSL certificates" on page 88
Other security settings		
Perform anti-virus scans, download scan logs, and edit the anti-virus configuration file.	Manage Clam anti-virus.	"Managing Clam anti-virus" on page 90

SMI-S checklist

Table 5 SMI-S security configuration checklist

Purpose of activity	Task	Where to learn more
User-based access control		
Restrict user access to specific functionality.	Configure user authentication, create cstadmin and cstuser accounts, and map users to roles.	• "Configure authentication" on page 94 "Create a cstadmin role" • "Create a cstadmin user" on page 95, "Create a role mapping" on page 96
Log files and settings		
Administer SMI-S log files.	Display SMI-S log files.	"Log files and settings" on page 97
Securely deploy SMI-S		
Enable authentication	Enable authentication for CIM and non-CIM requests.	"Securely deploying SMI-S" on page 99
Create the encrypted lockbox		
Create an encrypted lockbox to store and protect sensitive information.	Create the CST lockbox.	"Manage the encrypted lockbox" on page 99

CHAPTER 3
Solutions Enabler security configuration tasks

This chapter describes security tasks for Solutions Enabler 8.0, including:

- Access control 23
  - "Host-based access control" on page 23
  - "User-based access control" on page 28
- Log files and settings 30
- Port usage 34
- Solutions Enabler client/server security settings 36
- Managing certificate files 42
- Managing the Solutions Enabler server 52
- Data security settings 57
- Managing the encrypted lockbox 58
- Daemon security settings 61
- Securing SRM operations 65
- Maintenance: back up Solutions Enabler state 69

SYMAPI home and bin directory locations

The procedures in this chapter assume that the Solutions Enabler ‹*SYMAPI_HOME*› and ‹*SYMCLI_BIN*› directories are located as follows:

‹*SYMAPI_HOME*›

- Windows: `c:\Program Files\EMC\SYMAPI...`
- UNIX: `/var/symapi/...`
- z/OS: `/var/symapi/...`

Pathnames presented in this document use a UNIX-specific format: forward slashes (/) instead of the backslashes (\) typically used on Windows platforms.

‹*SYMCLI_BIN*›

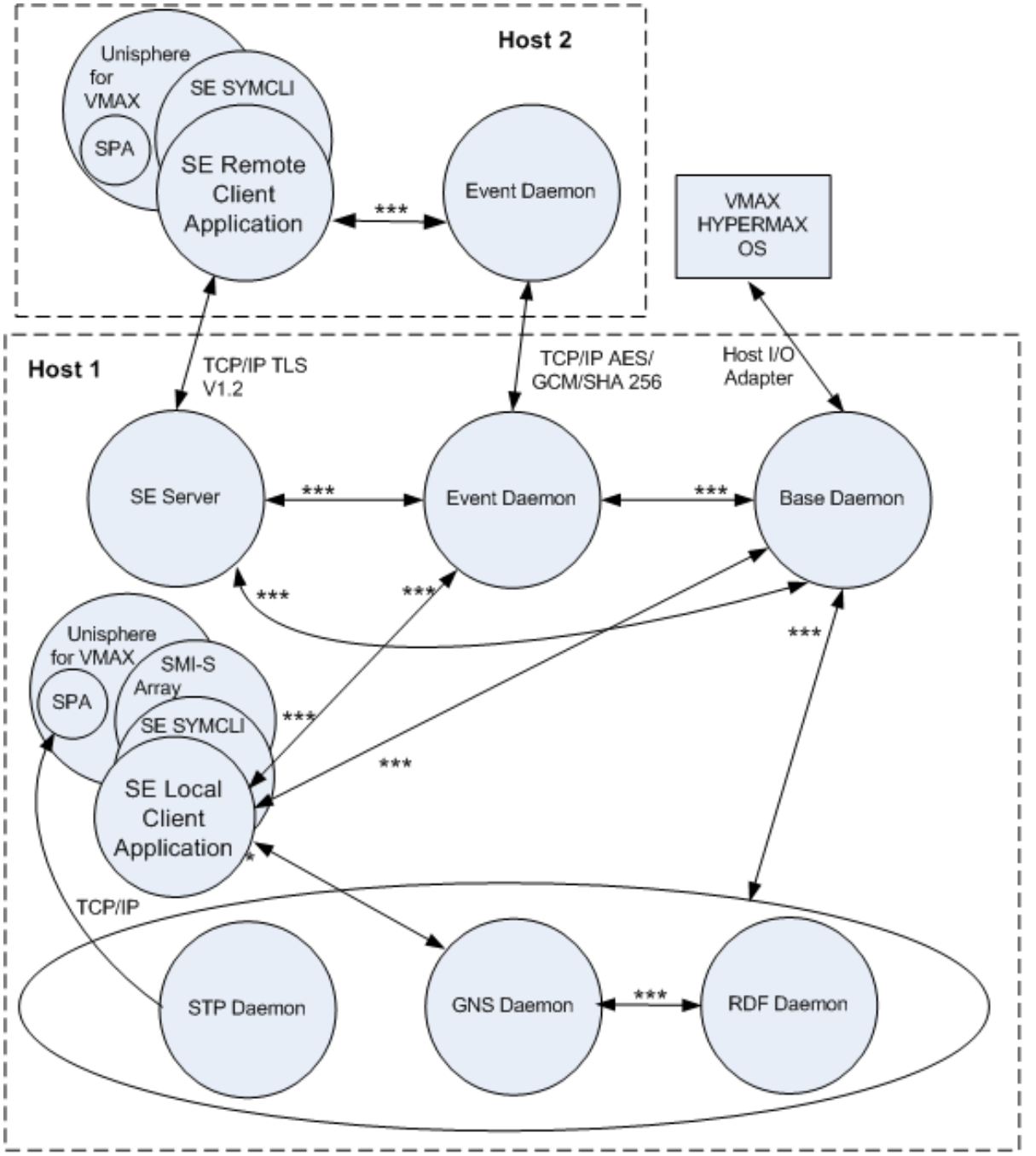
- Windows: `C:\Program Files\EMC\SYMCLI\bin...`
- UNIX: `/usr/storapi/bin...`

IMPORTANT

By default, the location of ‹*SYMAPI_HOME*› is the same for both z/OS and UNIX.

The *EMC Solutions Enabler Installation Guide* provides more information about:
- Changing the location for ‹*SYMAPI_HOME*› on z/OS systems during installation
- Open VMS file locations

Security controls map



*** = UNIX Domain Socket on UNIX systems, Anonymous IP with Named Pipe authentication on Windows systems.

(not pictured) All daemons rely on restart services provided by the Watchdog daemon in UNIX, and Service Control Manager in Windows.

Figure 1 Solutions Enabler managed objects

Access control

Solutions Enabler provides two mechanisms to control access to arrays: host-based access and user-based access.

- The `symacl` command provides host-based access control that can restrict host access to selected sets of devices across multiple arrays.

  `symacl` functionality is also referred to as Symmetrix Access Control.

- The `symauth` command provides user-based authorization that assigns a user or group to a role. Roles limit the management operations users can perform on an array.

Host-based access control

Host-based access control:

- Limits the management operations that a host can perform, and
- Provides highly granular control over management operations.

IMPORTANT

When configuring Symmetrix Access Control, it is important to:
- Give access rights only to authorized hosts,
- Assign only the privileges users require to perform their tasks,
- Grant ADMIN rights to a very limited number of users (for example, assign ADMIN rights to only known users and a select administrative group).

The *EMC Solutions Enabler Array Management CLI User Guide* provides:

- Detailed descriptions of the `symacl` and `symauth` commands.
- Steps to set up and perform host-based access control.

Host access IDs

Symmetrix Access Control identifies individual management hosts using an access ID. There are two different methods to generate these access IDs:

- **Alternate access ID**: The host's access ID can be generated at random or from a user-defined passphrase, and stored to a secure location on the local disk.

  Alternate access IDs are supported for all platforms.

  EMC strongly recommends alternate access IDs on platforms where the hardware-based access ID is derived from a network interface MAC address.

  "Alternate access IDs" on page 24 provides more information on this topic.

- **Hardware-based access ID** (default): The host's access ID is derived from hardware characteristics of that host:

  - On x86 (32-bit Intel), x86_64 (64-bit Intel/AMD), and IA 64 platforms, a network interface MAC address is used.
  - On other platforms, characteristics of the host, such as a processor identifier, are used.

  "Hardware-based access IDs" on page 26 provides more information on this topic.

IMPORTANT

When MAC addresses generate access IDs, the IDs may be unreliable or ineffective under some circumstances, including clustering environments, virtual environments, or following a hardware change.
For added security on x86 (32-bit Intel), x86_64 (64-bit), IA64, and BS2000 hardware platforms, EMC recommends that you use "Alternate access IDs" instead of hardware-based access IDs.

Alternate access IDs

Alternate access IDs are available for all platforms. When alternate access IDs are enabled, Solutions Enabler can:

- Randomly generate an access ID, as described in "Enabling alternate access IDs" on page 24, or
- Generate an access ID based on a user-chosen passphrase, where the passphrase is either:
  - Entered on the command line in an option,

  or

  - Entered in a file, whose name is specified in the command line.

  "Enabling alternate access IDs using a passphrase" on page 25 provides more information.

Solutions Enabler securely stores this alternate access ID on the local disk. The `symacl` man page provides more information on the `symacl -unique` command.

Enable the `SYMAPI_ALTERNATE_ACCESS_ID` option in the following file:

```
<SYMAPI_HOME>/config/options
```

When the `SYMAPI_ALTERNATE_ACCESS_ID` option is set to ENABLED and an alternate access ID is generated, copies of the ID, are securely stored on disk in the Solutions Enabler lockbox file.

Enabling alternate access IDs

1. Add the following option to the ‹*SYMAPI_HOME*›/config/options file:

   ```
   SYMAPI_ALTERNATE_ACCESS_ID = ENABLE
   ```

2. Run the `symacl -unique` command.

   Solutions Enabler:

   - Recognizes that the above option is set,
   - If one does not already exist for the host, generates an access ID,
   - Securely stores the access ID in the lockbox, and
   - Displays the access ID.

Note: If you run the `symacl -unique` command after enabling the `options` file setting, the new alternate access ID is different from the hardware-based access ID generated prior to enabling this option.
Any hardware-based access ID previously used to identify this host in an access group must be updated with the new alternate access ID using Solutions Enabler.

3. Use the `symaccess` command to add the access ID to the appropriate access groups.

   When an access ID is required on this host, the alternate access ID that was stored to disk is used.

Enabling alternate access IDs using a passphrase

1. Add the following option in the ‹*SYMAPI_HOME*›/config/options file:

   ```
   SYMAPI_ALTERNATE_ACCESS_ID = ENABLE
   ```

2. Run the `symacl -unique` command using the `-passphrase` option. The syntax when using the `-passphrase` option is as follows:

   ```
   symacl -unique [-passphrase [Passphrase|-file PassFile]]
   ```

   Note: Passphrases can be from 4 - 1000 characters in length.

   For example, to activate an alternate access ID using a passphrase:

   ```
   symacl -unique -passphrase Passphrase
   ```

   To activate an alternate access ID using a passphrase stored in a file on the local disk:

   ```
   symacl -unique -passphrase -file pathname
   ```

   Note: In client/server mode, *`pathname`* names the file on the client host.

   If no access ID already exists for the host, Solutions Enabler generates an access ID using the passphrase, securely stores it on the local disk, and displays it.

3. Use the `symaccess` command to add the access ID to the appropriate access group.

   When the access ID is required on this host, the alternate access ID that was stored to the disk is used.

Disabling an alternate access ID

There are two methods to disable `SYMAPI_ALTERNATE_ACCESS_ID` option in the options file:

1. Change the following setting in the `options` file to:

   ```
   SYMAPI_ALTERNATE_ACCESS_ID = DISABLE
   ```

   or:

   Remove the line from the `options` file.

2. Run the `symacl -unique` command.

This command recognizes that the option was reset, and disables the alternate access ID stored in the lockbox. The alternate access ID is retained in the lockbox in case you want to re-enable its use in the future.

Changing a host's alternate access ID

Note: Solution Enabler access control changes must be made from an administrative host with ADMIN rights to the array and rights to make `symacl` changes.

If you only have one such administrative host, and you change its alternate access ID, once that change is made, the host can no longer make access control changes because the new access ID is not yet in an access group.

EMC recommends that you enable a second administrative host prior to attempting to change a host's alternate access ID.

For example, to change the access ID for Host-1:

1. Log in to another administrative host, such as Host-2.
2. Remove any existing Host-1 definitions from the access group for all arrays to which Host-1 has access.
3. From Host-1, follow the steps outlined in "Enabling alternate access IDs" on page 24 or "Disabling an alternate access ID" on page 25 to enable or disable the alternate access ID mechanism and obtain a new access ID.
4. From Host-2, add Host-1 back into its access group using its new access ID to any arrays to which it requires access.

Hardware-based access IDs

Note: On IBM z/OS platforms, you must use job #14MSACL in the RIMLIB to generate and display the unique ID. #14MSACL takes the place of the `symacl -unique` command on this platform.

Enabling hardware-based access IDs

1. Confirm that the `SYMAPI_ALTERNATE_ACCESS_ID` option is disabled.

   In the ‹*SYMAPI_HOME*›/config/options file, verify that the option is set to DISABLE, as shown below:

   ```
   SYMAPI_ALTERNATE_ACCESS_ID = DISABLE
   ```

2. If the option is not set to `DISABLE`, do one of the following:
   - Edit the entry to set it to `DISABLE`.
   - Remove or comment out the statement.
3. Run the `symacl -unique` command to generate and display an access ID.
4. Use the `symaccess` command to add the access ID to the appropriate access groups.

Access control in client/server mode

Anyone with access to array management software can execute functions on any of the array's devices. Many applications can issue management commands to any device in a deployment.

Such shared systems may be vulnerable to a host accidentally or intentionally tampering with another's devices. To prevent this, use the `symacl` command to set up and restrict host access to defined sets of devices across the arrays.

The *EMC Solutions Enabler Array Management CLI User Guide* describes how to set up and perform host-based access control.

By default, client/server mode operations are executed on the server host using the access ID of the server. Access control checks are performed against the rules established for the server host, regardless of which client host initiated the operations.

You can use the access ID of the client host instead of the server host to perform this check. When this is enabled, access control rules must be established for, and checked against, the client hosts from which the operations are issued.

To use the access ID of the client host, you must make changes in the `options` file on the client and the server host, as explained in the following sections.

Server host options file settings

On the server host, the `SYMAPI_USE_ACCESS_ID` option controls the source of the access ID used for the client/server sessions:

```
SYMAPI_USE_ACCESS_ID = CLIENT | SERVER | ANY
```

The behavior of this option is as follows:

- `CLIENT` - The access ID supplied by the client host is used. If the client did not provide an access ID, operations fail. This can occur if the client is not configured to send its access ID.
- `SERVER` (default) - The server always uses its own access ID and ignores the access ID, if any, provided by the clients.
- `ANY` - The server uses an access ID provided by a singular client. If one is not provided, the server uses its own access ID.

Client host options file settings

On the client host, the `SYMAPI_ALTERNATE_ACCESS_ID` option must be enabled to use this alternate access IDs:

```
SYMAPI_ALTERNATE_ACCESS_ID = ENABLE
```

Additionally, you must set the following option to control whether the client can send its own access ID to the server:

```
SYMAPI_CLIENT_SIDE_ACCESS_ID = ENABLE | DISABLE
```

The behavior of this option is as follows:

- `ENABLE` - The client sends its access ID to the server in client/server mode.
- `DISABLE` (default) - The client does not send its access ID to the server in client/server mode.

IMPORTANT

After you enable the `SYMAPI_ALTERNATE_ACCESS_ID` and `SYMAPI_CLIENT_SIDE_ACCESS_ID` options, you must run the `symacl -unique` command on the client host to generate the access ID and store it in the lockbox on the client host. Client/server mode MUST be enabled to perform this task.

User-based access control

User authorization assigns individual users to roles. These user roles limit the management operations that users can perform. User-based controls are less granular than host-based controls.

Use the `symauth` command, SMC (Symmetrix Management Console), or Unisphere® for VMAX® 1.0 or higher, to assign users to management roles to restrict the types of operations they can perform.

Solutions Enabler does not support an explicit authentication mechanism for users. Solutions Enabler uses the credentials that users supply when logging onto the local system, as provided by the operating system.

SMC or Unisphere for VMAX 1.0 or higher pass the user's authenticated identity to Solutions Enabler.

EMC Solutions Enabler Array Management CLI User Guide provides more information about the `symauth` command.

EMC Unisphere for VMAX Installation Guide provides more information about managing Unisphere user accounts.

User identification

Internally, Solutions Enabler represents a user identity as a string assembled from the user's name and authentication source. The possible encodings are:

`H:HostName\UserName`	A user authenticated by the local operating system.
`D:DomainName\UserName`	A user authenticated by a specific domain on Windows.
`L:ServerName\UserName`	A user authenticated by an LDAP server. (SMC or Unisphere for VMAX 1.0 and higher.)
`C:HostName\UserName`	A user authenticated by the private SMC or Unisphere for VMAX 1.0 or higher authentication service on some host. (SMC or Unisphere for VMAX 1.0 and higher.)

Solutions Enabler uses these identities in a number of ways. A user name is included in records written to the array's secure Audit Log. This identifies the user that initiated the activity being logged. A user identity is the basis for optional user authorization rules that restrict management access to arrays.

Solutions Enabler 8.0 multiple authorization roles

A user or group can be assigned up to 4 authorization roles.

The `symauth` command has been enhanced to enable you to assign as many as 4 roles separated with a '+' character. For example:

```
StorageAdmin+Auditor+Monitor
```

Note: If any other role is combined with a role of None, the None role is ignored.

Output of the `symauth list` command has been enhanced to display authorization roles ordered from most powerful to least powerful. For example:

```
StorageAdmin+Auditor+PerfMonitor
```

Backward compatibility with Solutions Enabler 7.6 and earlier

Solutions Enabler versions 7.6 or earlier support only one role per user or group. To make your Solutions Enabler 8.0 compatible with Solutions Enabler versions 7.6 or earlier, create at least one authorization rule that corresponds to the 7.6 roles of Admin or SecurityAdmin.

This ensures that older Solutions Enabler versions can interpret at least one rule.

When a user has multiple roles defined on an array running Solutions Enabler 8.0, older versions of Solutions Enabler display only one (the highest assigned) role for that user.

Considerations when deleting or modifying rules

- Users on pre-8.0 systems can modify the rules on systems running Solutions Enabler 8.0, but the following cautions apply:
- Users on pre-8.0 systems can see only one (the highest) role of a rule on a system running Solutions Enabler 8.0, even if the 8.0 rule contains multiple roles.
- If a user on a pre-8.0 system deletes a rule on an 8.0 system that contains multiple roles, the operation deletes the entire multiple role rule.
- If a user on a pre-8.0 system modifies a a rule on an 8.0 system that contains multiple roles, the modification replaces the multiple roles in the rule with the single role specified by the pre-8.0 user.

For example:

- A rule on a system running Solutions Enabler 8.0 contains both StorageAdmin and Monitor roles.
- A user on a pre-8.0 system can see only the StorageAdmin role. The user modifies the rule to Auditor role.
- Both StorageAdmin and Monitor roles are removed even though the pre-8.0 system sees only the StorageAdmin role in the rule before the modification.

Support for all user groups

Solutions Enabler checks all groups to which a user belongs. During rights checking, each user group is examined for a role mapping and the “or” of all rights granted to each group.

The `symauth show -username` command displays all groups to which a user belongs.

Authorization rules can be configured for a array that map either a user or group name to a management role.

For both user and group authorization, the contained name can be fully qualified (such as `D:Corp\Jones` and `D:Corp\Sales`) or unqualified (such as Jones and Sales).

The rights that are called out for any of these entries matching the user's identity are granted to that user.

Authorization entries with an unqualified group name are only considered if there are no group entries with a fully qualified name matching the user.

The `symauth` man page provides more information on this topic.

Displaying user authorization

- To list user authorization policies:

  ```
  symauth -sid SID list
  ```

- To list the roles supported by the array:

  ```
  symauth list -roles
  ```

- To list mappings of roles to user and group names and their applicable components:

  ```
  symauth –sid SID list –users
  ```

- To list mappings of roles to user and group names and their applicable components, by user or group:

  ```
  symauth –sid SID list –users -by_user
  ```

Log files and settings

The secure audit log, SYMAPI, and the Solutions Enabler daemons maintain independent log files:

- **Secure audit log** - Records configuration changes, security alarms, service operations, and security-relevant actions on each array. The audit log is maintained on the storage array itself. Event contents in the audit log cannot be altered. User access is restricted to the auditor role that allows a user to view, but not modify, the log.

  Information from the audit log is retrieved using the `symaudit` SYMCLI command.

  Refer to *EMC Solutions Enabler Array Management CLI User Guide* for information about managing audit logs.

- **SYMAPI log files** - One log file is created per day, using the “dated” format to record SYMAPI errors and other significant conditions.

  Log files are stored at `<SYMAPI_HOME>/log/` and named `symapi_yyyymmdd.log`

  where `yyyymmdd` is the year, month, and day.

  A new log file is started every day on the first write after 12 a.m.

- **Solutions Enabler daemon log files** - Each daemon has two log files in “wrap” mode to record daemon errors and other significant conditions.

  Solutions Enabler daemon log files are stored at:

  ```
  <SYMAPI_HOME>/log/storXXXX.log0
  <SYMAPI_HOME>/log/storXXXX.log1
  ```

  Logging alternates between the two files, switching to the other file each time the maximum size specified by the daemon’s LOGFILE_SIZE parameter is reached.

Each daemon writes to the .log0 file until its size exceeds that specified in the LOGFILE_SIZE option, at which point it switches to the .log1 file. It switches back to .log0 under the same conditions.

and *storXXXX* is the name of the daemon, including:

- storsrvd (SYMAPI Server Daemon)
- storevntd(Event Daemon)
- storgnsd (GNS Daemon)
- storrdfd (RDF Daemon)
- storapid (Base Daemon)
- storstpd (STP Daemon)
- storwatchd (Watchdog Daemon, UNIX only)

By default, the daemon log files use “wrap” mode. You can use the LOGFILE_TYPE option in the daemon_options file to change this so that the specified daemon records its logs in “dated” mode. In dated mode, the daemon logs to a dated log file in the form *daemon_name-yyyymmdd*.log. A newly dated log file starts on the first write after 12 a.m.

The daemon_options file includes options that allow you to further customize logging for a particular daemon.

Table 6 shows the general logging configuration options you can use to customize the Solutions Enabler daemon log files. For details on the syntax and values, refer to the <*SYMAPI_HOME*>/config/daemon_options file.

Table 6 Options for managing daemon log files

Option	Description
LOGFILE_TYPE	Specifies the style of logging for the daemon. Possible values: **WRAP** (default) - Two log files are maintained: storxxxx.log0 and storxxxx.log1. Logging switches to the other file each time the maximum size specified by the LOGFILE_SIZE parameter is reached. **DATED** - A separate log file is used for each day: storxxxx-YYYYMMDD.log. There are no size limits on these files. Dated log files are retained for the number of days specified by the LOGFILE_RETENTION parameter.
LOGFILE_SIZE	Used for wrapping log files. Specifies the maximum number of KBs to write before switching to the other file of the pair. Default: 1000 (KB)
LOGFILE_RETENTION	Used for dated log files. How many days to retain old log files. Default: 3 (days) Valid values: A number of days greater than 0.
LOGFILE_PERM	Specifies the permissions on any newly created log files. Possible values: **rw** (default) - Anyone can read or write (UNIX mode of rwxrwxrwx). **r** - The owner (root) can read/write.

Table 7 summarizes information about SYMAPI, Solutions Enabler daemons, and secure audit log files.

Table 7 SYMAPI, Solutions Enabler daemons, and audit log file types and locations

Log type and location	Description
SYMAPI Log files `<SYMAPI_HOME>/log/symapi_yyyymmdd.log`	Solutions Enabler writes errors and other significant conditions to this log. • *yyyymmdd* is the numerical value for the year, month, and day. For example, the SYMAPI log for September 20, 2012 is `symapi_20120920.log` • By default, Solutions Enabler keeps these files forever. • Use the `SYMAPI_LOGFILE_RETENTION` option, as described in "Setting SYMAPI log file retention" on page 33, to configure when to automatically remove these files.

Daemon log files
`<SYMAPI_HOME>/log/storXXXX.log0`
`<SYMAPI_HOME>/log/storXXXX.log1`
	Each Solutions Enabler daemon maintains a pair of log files. The daemons alternate between these two files, switching from one to the other, when the size specified by LOGFILE_SIZE is reached.
	• *storXXXX* is the name of the daemon. For example, log file names include: `storapid.log0`, `storapid.log1`, `storgnsd.log0`, `storgnsd.log1`.
	• The default maximum size (LOGFILE_SIZE) is 1 MB.
	• Use the `LOGFILE_RETENTION` option, as described in "Setting daemon log file retention" on page 33, to configure when to automatically remove these files.

Audit Log (maintained on the array)	A secure audit log containing a record of configuration changes, security alarms, service operations, and security-relevant actions maintained on each array. Records are written to the audit log by: • Solutions Enabler, • Software running on the Service Processor, and • The Enginuity™ Operating Environment. Information from this log is retrieved using the `symaudit` SYMCLI command. You can configure the Solutions Enabler event daemon, `storevntd`, to automatically stream audit entries as they appear from this log to an external log service (EMC RSA® enVision®, syslog, Simple Network Management Protocol (SNMP), or the Windows Event Service). To learn more: • The *EMC Solutions Enabler Array Management CLI User Guide* provides more information about the audit log. • The *EMC Solutions Enabler Installation Guide* provides more information about configuring the Solutions Enabler event daemon.

Managing log file retention

During data center migrations and major configuration changes, you may want to increase how long log files are retained.

To conserve space, you may want to reduce log file retention to limit the disk space used by Solutions Enabler log files.

"Setting SYMAPI log file retention" on page 33 describes the steps to modify SYMAPI log retention.

"Setting daemon log file retention" on page 33 describes the steps to modify daemon log retention.

About log files

By default:

- The dated log files associated with SYMAPI are retained forever.
- If the log files associated with the Solutions Enabler daemons use dated mode, they are retained for 3 days.

Accumulated log files may consume considerable disk space.

EMC recommends that you configure a log file retention time for SYMAPI and the Solutions Enabler daemons to conserve disk space.

Log files are deleted after the specified retention time.

- Use the SYMAPI_LOGFILE_RETENTION option in the options file to set the retention time for the SYM API.
- Use the LOGFILE_RETENTION option in the daemon_options file to set the retention time for the Solutions Enabler daemons.

Setting SYMAPI log file retention

Use the SYMAPI_LOGFILE_RETENTION option in the options file to set the maximum number of days to retain SYMAPI log file, after which the log file is deleted.

The options file is located at: `<SYMAPI_HOME>/config/options`

The format for the option is: SYMAPI_LOGFILE_RETENTION = *NN*

where *NN* is the number of days to retain the SYMAPI log file.

Default value: 0 (retain forever)

Valid values: 5 (5 days) - 1825 (5 years)

Note: The log files might not be removed after the *NN* days are reached. This value indicates to the system when a given file can be removed by the logging logic during its normal operation.

The `README.options` file installed with Solutions Enabler has more information about the SYMAPI_LOGFILE_RETENTION option.

Setting daemon log file retention

By default, Solutions Enabler daemons log use wrap mode. If the format of a daemon's log file is changed to dated mode in the daemon_options file:

LOGFILE_TYPE =DATED

You can use the LOGFILE_RETENTION option in the daemon_options file to modify the number of days the daily log file is retained.

The format for the option is: LOGFILE_RETENTION = *NN*

where *NN* is the number of days to retain the daemon's daily log file.

Default value: 3 (days)

Valid values: A number of days greater than 0.

Assigning a custom audit log activity ID

By default, Solutions Enabler generates a random activity ID to identify each session. This ID appears in the audit log entries for that session. Since the default ID is random, filtering audit log entries based on the ID is difficult.

You can specify a custom activity ID, making it easier to filter audit log entries.

An optional argument `-actid <Activity ID>`, allows you to set a custom activity ID on all operations performed as part of that CLI command.

When you use the `-actid <Activity ID>` argument, entries in the audit log for that command are tagged with the specified activity ID prefixed with "U_".

User-defined activity IDs must meet the following requirements:

- Maximum of 14 characters (not including the automatic prefix)
- Include only alphanumeric characters

  Underscore (_), and hyphen (-) characters are allowed.

If you try to define an Activity ID with more than 14 characters, the operation fails, and an error is displayed.

All active SYMCLI commands, with the exception of `symaudit` command, accept the `-actid` argument. For example:

```
symqos -sid 237 -cp -name cptest -devs 410:411,1170 addall -actid
   CPTest1
```

Output of `symaudit` queries in verbose mode report the user-defined activity ID. For example:

```
symaudit list -sid 237 -v -activity_id U_CPTest1

              A U D I T   L O G   D A T A

Symmetrix ID            : 000190300237

  Record Number         :   711815
    Records in Seq      :        2
.
.
.
    Username            : H:dldv0181\root
    Activity ID         : U_CPTest1

  Record Number         :   711816
    Records in Seq      :        2
.
.
.
```

Port usage

This section describes:

- Ports used by the Solutions Enabler server and the event daemon.
- Options to modify the port settings

Server port usage

In client/server mode, the Solutions Enabler server (the `storsrvd` daemon) listens by default at TCP/IP port 2707 for client connections.

You can configure a port by adding an entry to `<SYMAPI_HOME>/config daemon_options` file as follows:

```
storsrvd:port = nnnn
```

At client hosts, the configuration file `<SYMAPI_HOME>/config/netcnfg` can be changed to reflect the use of this non-default port.

The port used by the `storsrvd` daemon cannot be changed while the server is running. If you want to use a different port, you must specify it in the `daemon_options` file, and restart the `storsrvd` daemon.

Event daemon port usage

When using the asynchronous events in client/server mode, the event daemon at the client host listens at a TCP/IP port for events being forwarded from the event daemon at the server. By default, the client event daemon asks the operating system to pick an unused port for it to use.

You can configure a specific port for use by adding an entry to the `<SYMAPI_HOME>/config /daemon_options` file on the client host as follows:

```
storevntd:event_listen_port = nnnn
```

Network port usage

If a firewall or network address translator is present, these ports must be open. Typically, this is a firewall between the Solutions Enabler client and the server hosts.

Table 8 lists the network ports used by Solutions Enabler.

Table 8 Network ports used by Solutions Enabler

Component	Protocol	Port	Description
Solutions Enabler	TCP/IP	2707	In client/server mode, the Solutions Enabler server daemon, `storsrvd`, listens on this port for connections from client hosts. Refer to "storsrvd:port = NNNN" on page 36 You can change the default port as described in "Server port usage" on page 35.
Event daemon	TCP/IP	Dynamically assigned	In client/server mode, the event daemon, `storevntd`, on a client host listens on this port for asynchronous events sent to it from a server host. By default, this is picked at random by the client host event daemon. Refer to "SvcName - TCPIP HostName - NNNN SECURE" on page 36 For information on setting a specific port value, refer to "Event daemon port usage" on page 35.
CLARiiON	TCP/IP	443 or 2163	A configuration file on CLARiiON storage arrays controls whether it listens for connections from management hosts over port 443 or 2163. When Solutions Enabler needs to communicate with an array, it attempts both values. Refer to "Network port usage" on page 35.

Options to modify port settings

Table 9 lists the options to modify the settings of ports used by Solutions Enabler.

Table 9 Options to modify port settings used by Solutions Enabler

Option location and name	Description
storsrvd:port = ***NNNN*** `<SYMAPI_HOME>/config/daemon_options`	On the server hosts, this directs the Solutions Enabler server, the `storsrvd` daemon, to listen for connections at this port instead of the default 2707. If the default value is changed for the server, you must edit this entry for this server in the `<SYMAPI_HOME>/config/netcnfg` file as explained in the next row.
SvcName - TCPIP ***HostName*** - ***NNNN*** SECURE `<SYMAPI_HOME>/config/netcnfg`	On client hosts, the `netcnfg` file maps service names (*SvcName*), used with the SYMCLI, to a host (*HostName*) and port (*NNNN*) on which the appropriate server is listening. If a non-default server port is configured, it also makes corresponding changes to the servers in this file necessary. For more information, refer to "Configuring the Solutions Enabler client host" on page 40.
storevntd:event_listen_port = ***NN NN*** `<SYMAPI_HOME>/config/daemon_options`	In client/server mode, the event daemon, `storevntd`, on a client host listens on this port for asynchronous events sent to it from a server host. By default, this is picked at random by the client-host event daemon. On client hosts, this setting directs the event daemon to listen at this specific port for events sent from the event daemon on the server host, instead of using a random port assigned by the local operating system. This setting is automatically transmitted to the event daemon on the server host as needed.

Solutions Enabler client/server security settings

In Solutions Enabler client/server mode, client host operations are automatically forwarded to the `storsrvd` daemon on a server host for execution.

By default, traffic transmitted between client and server hosts is encrypted using SSL.

This section describes the mechanisms to operate these connections in a secure manner.

Network encryption

On platforms where Solutions Enabler supports SSL, servers default to securing all connections using SSL.

Solutions Enabler uses OpenSSL 1.0.1h with the OpenSSL FIPS Object Module 2.0 (NIST certificate #1747). FIPS mode is supported on the following platforms:

- Linux x86 platforms
- Windows x86 64 bit platforms

Solutions Enabler V8.0 client and server use TLS V1.2 with Advanced Encryption Standard (AES) with 128-bit key, Galois Counter Mode (GCM), with Secure Hash Algorithm 1 (SHA-1).

If a client is running an earlier version of Solutions Enabler, SSLv3 with AES-128 + SHA-1 is used.

Note: FIPS 140-2 mode is enabled by default.

Securing remote connections using SSL

The default/initial configuration for SYMAPI client and server communications, (on platforms that support it) is to negotiate only SECURE sessions. You can modify the security level at which the client and server are operating.

Before you begin

Before modifying the security level, you should:

- Understand that the security level specifies the capability of the local side and the local side's expectation of the remote side.
- Know whether the host is SSL-capable or SSL-incapable.

The possible security levels are:

- **Level 3 (SECURE)** — (Default) Indicates that only secure sessions will be negotiated between the client and server. This is the highest level of security, and it should only be used when there is no chance of an SSL-incapable client attempting to connect with the server, or an SSL-capable client connecting to an SSL-incapable server.
- **Level 2 (ANY)** — Indicates that either secure or non-secure sessions will be negotiated between the client and server on SSL-capable platforms.
- **Level 1 (NONSECURE)** — Indicates that only non-secure sessions will be negotiated between the client and server. This level is intended as a last resort in situations where SSL cannot be used for some reason or is undesirable. In addition, this level can also be useful in matters of performance and availability.

Note: The default security level is SECURE on platforms that support secure communications and NONSECURE on platforms that do not support secure communications.

The following messages may be issued by the server if SSL-related problems occur:

- ANR0141E through ANR0145E
- ANR0147E
- ANR0148E
- ANR0150E through ANR0153E
- ANR0155E

The *EMC Solutions Enabler Installation Guide* provides details about SYMAPI server daemon messages.

Session negotiation behavior

Table 10 details the type of session negotiated if a client and server are at the same or different security levels (implied or configured).

Table 10 **session negotiation behavior**

Client security level	Server security level	Negotiated session type
SECURE	SECURE	SECURE
	ANY	SECURE
	NONSECURE	Rejected
NONSECURE	NONSECURE	NONSECURE
	ANY	NONSECURE
	SECURE	Rejected
ANY	ANY	SECURE
	SECURE	SECURE
	NONSECURE	NONSECURE

Configuring the Solutions Enabler server host

Two options specify whether the Solutions Enabler server accepts only secure sessions from clients and whether FIPS 140-2 cryptographic algorithms are used for client/server communication:

- **SYMAPI_SECURITY_LEVEL ‹SECURE |ANY |NONSECURE ›**

  This option specifies whether the Solutions Enabler server accepts only secure sessions from clients.

  The default value for SYMAPI_SECURITY_LEVEL is SECURE. That is, the Solutions Enabler server accepts only secure sessions from clients.

- **SYMAPI_FIPS ‹ ENABLE|DISABLE›**

  When SYMAPI_SECURITY_LEVEL is set to SECURE, this option enables/disables FIPS 140-2 compliant encryption of Solutions Enabler server/client sessions (on Linux and Windows platforms).

  The default value for the SYMAPI_FIPS option is ENABLE.

On Linux and Windows platforms; when the SYMAPI_SECURITY_LEVEL option is set to SECURE, enabling the SYMAPI_FIPS option enables FIPS 140-2 compliant encryption for client/server communications.

On other platforms, when SYMAPI_SECURITY_LEVEL option is set to SECURE, the standard Solutions Enabler encryption algorithms are used for client/server communication.

Backward compatibility to pre-8.0 configuration files

Solutions Enabler 8.0 provides backward compatibility to 7.5 and earlier versions using the following logic to select the security level:

- Look for SYMAPI_SECURITY_LEVEL in the ‹*SYMAPI_HOME*›/config/options file.

- If SYMAPI_SECURITY_LEVEL is specified in the ‹*SYMAPI_HOME*›/config/options file, use it.
- If the SYMAPI_SECURITY_LEVEL security level is not specified in the ‹*SYMAPI_HOME*›/config/options file, the server looks for storsrvd:security_level in the ‹*SYMAPI_HOME*›/config/daemon_options file.
  - If the storsrvd:security_level is *not* specified on the server, look for SYMAPI_SERVER_SECURITY_LEVEL.
    - If the SYMAPI_SERVER_SECURITY_LEVEL is *not* specified, use the default for the platform: SECURE everywhere except OVMS, BS2000, or AS400 which use NONSECURE.
    - If the SYMAPI_SERVER_SECURITY_LEVEL *is* specified, use the specified value and post a message saying it was used instead of the storsrvd:security_level.
  - If the storsrvd:security_level is specified, use it.

Allow non-secure client sessions

NOTICE

EMC does not recommend using NONSECURE sessions.

You can allow non-secure sessions from clients that cannot or are not configured to negotiate secure sessions by modifying the SYMAPI_SECURITY_LEVEL in the ‹*SYMAPI_HOME*›/config/options file.

To permit non-secure sessions from clients, do one of the following:

- To accept both secure and non-secure sessions, change the setting to ANY:

  ```
  SYMAPI_SECURITY_LEVEL = ANY
  ```

- To accept only non-secure sessions, change the setting to NONSECURE:

  ```
  SYMAPI_SECURITY_LEVEL = NONSECURE
  ```

Note: Regardless of the value of the SYMAPI_SECURITY_LEVEL option, the cryptographic algorithms used for non client/server communications on Linux and Windows are FIPS 140-2 compliant.

security_clt_secure_lvl

By default, a server requires from and verifies the client's subject certificate, if the client is able to provide one. You can modify this configuration as follows:

- To configure the server to accept only connections for which the client can be verified, add the following line to the `<SYMAPI_HOME>/config/daemon_options` file at that host:

  ```
  storsrvd:security_clt_secure_lvl = MUSTVERIFY
  ```

- To configure a server to bypass the validation of a client certificate, set the `security_clt_secure_lvl` statement to `NOVERIFY` in the `<SYMAPI_HOME>/config/daemon_options` file:

  ```
  storsrvd:security_clt_secure_lvl = NOVERIFY
  ```

- To enable a server to validate client certificates, set the `security_clt_secure_lvl` statement to `VERIFY` (the default value) in the `<SYMAPI_HOME>/config/daemon_options` file:

  ```
  storsrvd:security_clt_secure_lvl = VERIFY
  ```

Table 12 on page 42 provides a summary of the values of the security_clt_secure_lvl statement.

Configuring the Solutions Enabler client host

NOTICE

The following section includes a description of the steps to disable secure communications. EMC does not recommend this activity.

By default, the Solutions Enabler client attempts to negotiate a secure session with the server when both are capable of doing so.

To allow non-secure sessions with a server that cannot negotiate a secure session, do one of the following:

- To allow a mix of secure and non-secure sessions to servers, depending on the capability of the server, change the following setting to `ANY` in the `<SYMAPI_HOME>/config/options` file:

  ```
  SYMAPI_SECURITY_LEVEL = ANY
  ```

- To require a client to negotiate non-secure sessions to all servers, change the following setting to `NONSECURE` in the `<SYMAPI_HOME>/config/options` file:

  ```
  SYMAPI_SECURITY_LEVEL = NONSECURE
  ```

To configure the session security for specific server hosts, specify `NONSECURE` or `ANY` in the `<SYMAPI_HOME>/config/netcnfg` file for the server in question. This file maps service names to server hostnames (or IP addresses) and port numbers for Solutions Enabler SYMCLI commands.

The format of records in the `netcnfg` file is as follows:

`ServiceName - PairingMethod - TCPIP HostName IP-Address Port SecurityLevel`

Where:

- *`ServiceName`* is the name by which the server is known. This is the same value used by the `SYMCLI_CONNECT` environment variable for SYMCLI commands.
- *`PairingMethod`* indicates whether the entry is a Single entry or one of a Balanced or Ordered pair of entries.
  - `Single` (legacy method) a single service name.
  - `Balanced` SYMAPI randomly selects server entry for the client/server session. If selection fails, SYMAPI tries the other entry.
  - `Ordered` SYMAPI selects first server entry for the client/server session. If selection fails, SYMAPI tries the other entry.

- *HostName* is the name of the host on which the server resides. Specify either *HostName* or *IP-Address*.
- *IP-Address* is the IP address of the server. Specify either *HostName* or *IP-Address*.
- *Port* is the port number (default 2707) on which the server is listening.
- *SecurityLevel* is one of three security levels:
  - SECURE negotiates secure sessions:
  - NONSECURE negotiates non-secure sessions
  - ANY negotiates both secure and non-secure sessions, depending on the server configuration.

  If you do not specify a security level, SECURE is used for secure-capable platforms, and NONSECURE is used for secure-incapable platforms, depending on the configuration of the server.

IMPORTANT

The security level specified in the <*SYMAPI_HOME*>/config/netcnfg file takes precedence over the one in the options file.

The *EMC Solutions Enabler CLI Command Reference* provides more information on this topic.

Secure session configuration summary

Table 11 lists the host operating systems that support SSL.

Table 11 Host operating systems that support SSL

Operating systems that support SSL
AIX (64-bit)
HP-UX (64-bit) HP-UX Itanium (64-bit)
Linux Itanium (64-bit) Linux AMD (64-bit)
Solaris (64-bit)
Windows AMD (64-bit)
z/OS

Note: Solutions Enabler does not support SSL on iSeries, BS2000, or OpenVMS.

Table 12 provides a summary of the secure session settings.

Table 12 Secure sessions summary

Option name, possible values, and location	Description
storsrvd:security_clt_secure_lvl =MUSTVERIFY |VERIFY |NOVERIFY `<SYMAPI_HOME>/config/daemon_options`	On server hosts, controls how the server validates client certificates. **Note:** This option is not supported on z/OS hosts, where it defaults to NOVERIFY. **MUSTVERIFY**: The server requires clients to send a valid certificate. **VERIFY** (default): The server verifies a client's certificate, if one is sent. **NOVERIFY**: The server does not verify client certificates. "security_clt_secure_lvl" on page 39 provides more information.
storsrvd:security_level =SECURE | NONSECURE |ANY `<SYMAPI_HOME>/config/deamon_options`	On server hosts, controls whether servers establish a secure session. **SECURE** (default): Secure sessions are always used. All other connection types are refused. **NONSECURE**: Non-secure sessions are used; secure sessions are not used. **ANY**: A secure session is established when supported by the client; otherwise a non-secure session is used.
SYMAPI_SECURITY_LEVEL = SECURE | ANY | NONSECURE `<SYMAPI_HOME>/config/options`	Specifies whether the Solutions Enabler server accepts only secure sessions from clients. Applies to both server and client. **SECURE** (default): Secure sessions are always used. All other connection types are refused. **NONSECURE**: Non-secure sessions are used; secure sessions are not used. **ANY**: A secure session is established when supported by the client; otherwise a non-secure session is used. "Configuring the Solutions Enabler server host" on page 38 provides more information.

Managing certificate files

Solutions Enables uses OpenSSL to generate certificates for secure client-server communication. The client and server verify each other's identity based on the information contained in the certificates.

During installation, the user has the option to install the certificate component. If the user chooses to install the certificate component, a default set of certificates is generated. These certificates are signed by a self-signed root certificate.

Solutions Enabler uses a root certificate and key to generate subject certificates that identify client and server hosts. The root certificate is installed on the host. The installation process automatically generates a subject certificate for the host on which the install is executed.

The generated certificates can be replaced with certificates that you generate or that are issued to you by a commercial certificate authority (CA). See "Replacing SYMAPI-generated certificates:" on page 48.

Subject certificates are generated for both client and server hosts. The subject certificates represent the identity of the host without respect to whether the host acts as a client or a server. Thus, a single set of certificates can be used in both the client and server.

If desired, the client and server can be configured separately to use other sets of certificates. By default, both the client and the server validate the certificate of the peer during secure session negotiation. The client always validates the server's certificate, and you cannot disable this validation when a secure session is negotiated.

The `cert` directory is located at:

- Windows: `<SYMAPI_HOME>\config\cert`
- UNIX and z/OS: `<SYMAPI_HOME>/config/cert`

Note: By default, the location of cert directory is the same for z/OS as UNIX. The location for z/OS systems can be changed during installation.

The following certificate files enable a client to verify a server's identity and a server to verify a client's identity:

- `symapisrv_cert_v8.0.pem` is the default version 8.0 subject certificate file. It is created specifically for its particular host during installation. It is signed by the EMC Enterprise Storage Automation root certificate symapisrv_trust_v8.0.pem. This file must be in the `cert` directory on the SYMAPI client and server for client/server security to work.
- `symapisrv_trust_v8.0.pem` is the EMC Enterprise Storage Automation Root certificate. This file must be in the `cert` directory on every client and server.
- `symapisrv_key_v8.0.pem` is the key file associated with the subject certificate. It is created specifically for its particular host during installation. It is generated during the certificate creation process. This file must be in the `cert` directory on the SYMAPI client and server for client/server security to work.

For backward compatibility with pre-V8.0 versions the following certificate files are also created in the cert directory:

- `symapisrv_cert.pem` is the pre-V8.0 subject certificate file. It is created specifically for its particular host during installation. It is signed by the EMC SPEA pre-V8.0 Root certificate. This file must be in the cert directory on the SYMAPI client and server for pre-V8.0 client/server security to work.
- `symapisrv_trust.pem` is the EMC SPEA pre-V8.0 Root certificate used to sign the SYMAPI certificate file. This file must be in the cert directory on every client and server for pre-V8.0 client/server security to work.
- `symapisrv_key.pem` is the pre-V8.0 key file associated with the subject certificate. It is created specifically for its particular host during installation. It is generated during the certificate creation process. This file must be in the cert directory on the SYMAPI client and server for pre-V8.0 client/server security to work.

About wildcards in DNS names

There are several use-cases where the host may have multiple network identities:

- The host has multiple NICs (and thus multiple IP addresses).

- The host is known in multiple domains.
- The host is part of a cluster where a failover causes a different hostname to be in effect at the time the host is issuing the handshake request.

In Solutions Enabler 7.5 and earlier, the Subject identifier of a certificate contains the host information. Specifically, the Common Name (CN) part of the certificate contains the host identity. The CN had to match the Fully Qualified Domain Name (FQDN) of the host being authenticated. Solutions Enabler 7.5 and earlier allowed wildcards (*) in the CN to facilitate this matching.

The **-san** argument of the `manage_server_cert create` command allows multiple individual domain names and IP addresses to be specified in a single certificate, eliminating the need for wildcards in the CN.

Wildcards are used is as follows:

- Wildcards are allowed in the CN and in arguments for the **–san** option.
- To support backward compatibility, a new `storsrvd` option in the daemon_options file; `security_cert_allow_wildcards` allows you to control whether or not wildcards are supported when authenticating certificates from pre-7.6 clients.
- New keywords extend the `manage_server_cert create` command to accommodate the changes.

manager_server_cert commands syntax

In Solutions Enabler 8.0, the manage_server_cert.sh and manage_server_cert.bat scripts are replaced with the manager_server_cert executable. Options previously used with the scripts can be used with the executable.

The manager_server_cert executable has two additional options: create_root and export.

The manager_server_cert create option has two additional options: -pass and -mode options.

IMPORTANT

The format for wildcards used by manager_server_cert for certificate creation varies depending on the platform.
On Unix platforms, **-san** arguments MUST be in quotes.
On Windows, **–san** are NOT in quotes.

On Unix:

```
<SYMCLI_BIN> manage_server_cert.sh create "host*" -san "* *.lss.emc.com"
```

On Windows:

```
<SYMCLI_BIN> manage_server_cert.bat create host* -san * *.lss.emc.com
```

The location for `<SYMCLI_BIN>` is described at “‹SYMCLI_BIN›” on page 21.

```
manage_server_cert create
   [common_name]
   –pass <LockBoxPassword>
   [-mode [V76|V80]
   [-san <san_list>]
   [-o <organization_name>]
   [-ou <organization_unit>]

manage_server_cert create_root -pass <LockBoxPassword> [-mode V76]

manage_server_cert export [-mode <V76|V80>]

manage_server_cert update

manage_server_cert list <Certfile>

manage_server_cert secure
```

- **create -** Creates the subject certificate and key files.
- **common name** - Can be at most 55 characters long and can contain wildcards. If the common name (CN) is not specified, the script guesses the host name on which the script is being run and uses that in the CN field of the Subject property of the certificate.
- **-san** (optional) - The Subject Alternative Name (**-san**) option allows you to specify multiple hosts, including wildcards.

  If you do not use the **-san** option (the default), you can enter only one hostname as the CN.

  There is no limit on the number of hosts you can specify using the **-san** option.

  Enter a space-separated list of a of DNS names and IP addresses. The IP addresses can be IPv4 and IPv6 addresses. See "Using the manage_server_cert create -san option (7.5 and earlier/7.6 and later)" on page 46
- **create_root** - Creates the root certificate file in the current directory, and stores the root key file in the lockbox.
- **export** - Creates the root certificate file in the current directory.
- **list** - Shows all names recorded in a certificate (Common Name and Subject Alternative Name if present). The Certfile default is `symapisrv_cert_v8.0.pem`.
- **secure** - Removes any root certificates and key files (symapisrv_trust.pem and symapisrv_trustkey.pem) created using Solutions Enabler 7.6 or earlier.
- **update** - Create or update certificate verification files used during session negotiation.
- **-mode V76|V80** - Specifies the version of the certificate to be created. If no mode is specified, the default (V80) is used.
  - **V76** - Creates Solutions Enabler 7.6 version of the certificate.

    When used with the create_root option, adds the version 7.6 root key to the lockbox.
  - **V80** (default) - Creates Solutions Enabler 8.0 version of the certificate.
- **-pass** ‹*LockBoxPassword*› - Specifies the password for the lockbox.

Table 13 lists examples of the manage_server_cert create script in Solutions Enabler Version 7.5 and earlier and how to use the **-san** option in Solutions Enabler Version 7.6 and later.

Table 13 Using the manage_server_cert create -san option (7.5 and earlier/7.6 and later)

Solutions Enabler 7.5 and earlier	Solutions Enabler 7.6 and later
Specify a single hostname: manage_server_cert.sh create aaa.bbb.com	No change.
Specify a hostname with a wildcard: manage_server_cert.sh create aaa.bbb.com ccc.bbb.com *.acme.com	Use the **-san** option to allow wildcards: `manage_server_cert.sh create host_name-san aaa.bbb.com ccc.bbb.com *.acme.com`
Specify an IP address with a wildcard: manage_server_cert.sh create 10.244.245.153 10.245.*	Wildcards are not allowed for IP addresses. Use the **-san** option and specify the individual IP addresses: `manage_server_cert.sh create 10.244.245.153 -san 10.245.150.110 10.245.150.111 10.245.150.112`
Use a wildcard for the entire hostname: manage_server_cert.sh create *	Use the **-san** option to allow the wildcard: `manage_server_cert.sh create -san "*"`
Specify a hostname with the wildcard in the anything other than the leftmost label: manage_server_cert.sh create aaa.bbb.com aaa.*.com	Wildcards are allowed only in the leftmost label of the FQDN. Use the **-san** option and specify the individual labels and hosts: `manage_server_cert.sh create aaa.bbb.com -san aaa.ccc.com aaa.ddd.com aaa.eee.com`
Specify a DNS name using a wildcard: manage_server_cert.sh create *.com	Wildcards are not allowed in without the **-san** option, and must comply with "Rules for wildcards in DNS names". Use the **-san** option and specify the individual DNS names: `manage_server_cert.sh create -san aaa.abc.com bbb.abc.com ccc.abc.com`

Rules for wildcards in DNS names

The following are rules for wildcards in DNS names with **-san** extensions.

Note: The following wildcard rules do not apply to wildcards in the CN.

- Wildcards are allowed only in the leftmost label in a DNS name. DNS names in which the wildcard is other than the leftmost label are ignored. For example:

  host0100.*.acme.com - Ignored. Wildcard is not the leftmost label.

  *.bbb.acme.com - Is matched.

- If the wildcard is the only character in the leftmost label of the DNS name, only the leftmost label of the host FQDN will be matched. For example:

  host aaa.bbb.acme.com matches host *.bbb.acme.com

  host aaa.bbb.acme.com does not match *.acme.com

- If a DNS name includes a label with a wildcard plus other characters, the wildcard is matched based on regular rules. For example:

  host0100.bbb.acme.com matches dldv*.bbb.acme.com

  host0100.bbb.acme.com also matches *01*.bbb.acme.com.

Managing backward compatibility of certificates

Solutions Enabler 8.0 is backward compatible with certificates generated by earlier versions, back to 7.4. For example:

- A Solutions Enabler 8.0 server can verify a certificate generated by an older version.
- A Solutions Enabler 7.6 client can verify a server certificate generated with **-san** and **-mode V76** options.
- An older client (Solutions Enabler 7.5 or earlier), can verify a certificate generated by a Solutions Enabler 8.0 server if the certificate's CN contains:
  - A Fully Qualified Domain Name (FQDN) - if the server host name can be resolved to a FQDN, or
  - An IP address corresponding to the server - if the server host name cannot be resolved to a FQDN.

  In cluster configurations, if the Solutions Enabler 8.0 server's certificate does not contain wildcards in the CN, the Solutions Enabler 7.5 client will not verify the server if the server fails over and presents a different host ID than that present in the CN.

  If a Solutions Enabler 8.0 server is running in a clustered environment, Solutions Enabler 7.5 and older clients must have certificates for each host node of the server cluster.

⚠CAUTION

When generating certificates on Solutions Enabler 8.0 servers, be careful not to add non-DNS host names in the CN if Solutions Enabler 7.5 and older clients will connect to the server.

Enabling/disabling support for wildcards in the CN

`storsrvd` allows you to control whether wildcards are accepted in the Common Name (CN) field in client certificates. The syntax is:

```
storsrvd:security_cert_allow_wildcards [enable|disable]
```

- The `enable` setting allows a Solutions Enabler 8.0 server that receives an older certificate (Solutions Enabler 7.5 or earlier) from a client to authenticate the client based on wildcards in the CN.
- The `disable` setting prevents a Solutions Enabler 8.0 server that receives an older certificate (Solutions Enabler 7.5 or earlier) from a client from authenticating the client based on wildcards in the CN. This is the default setting.

Use the `stordaemon setvar` command to temporarily enable or disable the `security_cert_allow_wildcards` option. For example:

```
stordaemon setvar storsrvd -name security_cert_allow_wildcards=enable
  storsrvd                    Variable was set
```

Use the `stordaemon getvar` command to display the setting:

```
stordaemon getvar storsrvd -name security_cert_allow_wildcards
  storsrvd                    security_cert_allow_wildcards=enable
```

Managing certificate files

The following sections describe how to use the `manage_server_cert` to manage certificate files, including:

- "Replacing SYMAPI-generated certificates:" on page 48
- "Remove unneeded files (optional)" on page 49
- "Changing a host's name" on page 49
- "Working with a host in multiple domains" on page 50
- "Working with a Windows cluster" on page 50
- "Adding virtual server names to a certificate" on page 51
- "Working with a multi-homed host" on page 52
- "Listing the hostnames in the certificate" on page 52

Note: The *EMC Solutions Enabler Installation Guide* provides more information about installing certificates.

Replacing SYMAPI-generated certificates:

During installation, the installer may choose to install the certificate component.

If the installer installs the certificate component, a default set of certificates is generated. These SYMAPI-generated certificates are signed by a self-signed root certificate.

This section describes the steps to replace the self-signed SYMAPI-generated certificate created at installation with a CA-signed certificate.

You can replace a SYMAPI-generated certificate with one generated by your certificate authority or an external certificate authority (for example, Verisign).

When creating a replacement certificate, you must adhere to the following rules in order for the certificate to work with the client/server:

- Restrictions about wildcards as described in Table 13 on page 46.
- The certificate must be created in Privacy Enhanced Mail (.pem) format.

Once you have created the certificate, do the following on the host:

1. Move the certificate file and the associated key file to the `cert` directory.
2. Move the trusted certificate files that signed the created certificate to the same `cert` directory.
3. Run the `manage_server_cert update` command in the `cert` directory:

   ```
   <SYMCLI_BIN> manage_server_cert update
   ```

   "manager_server_cert commands syntax" on page 44 describes the command format for your platform.
4. Edit the following options in the `config` directory:
   - If this is a client certificate, edit the following in the `options` file.

  - Change the SYMAPI_SECURITY_ALT_CERT_FILE option to specify the name of the new certificate file.
  - Change the SYMAPI_SECURITY_ALT_KEY_FILE option to specify the name of the new key file.
- If this is a server certificate, edit the following in the `daemon_options` file.
  - Change the `storsrvd:security_alt_cert_file` option to specify the name of the new certificate file.
  - Change the `storsrvd:security_alt_key_file` option to specify the name of the new key file.

Remove unneeded files (optional)

When a server no longer needs to communicate with 7.6 or earlier clients, delete the certificate and key files for that communication to increase security.

Note: For client-only installations, delete these files after installation.

To remove these files, run the `manage_server_cert secure` command in the `cert` directory:

```
<SYMCLI_BIN>manage_server_cert secure
```

"manager_server_cert commands syntax" on page 44 describes the command format for your platform.

Changing a host's name

If you change the name of the host on which the client or server is running, you must also change its name in its certificate. To do this, you must run the `manage_server_cert.sh create` command in the host's `cert` directory. This command reads the hostname from the environment and recreates the certificate:

```
<SYMCLI_BIN>manage_server_cert create -pass <LockBoxPassword>
```

"manager_server_cert commands syntax" on page 44 describes the command format for your platform.

The following example illustrates the `manage_server_cert create` command:

```
/usr/storapi/bin/manage_server_cert create -pass <LockBoxPassword>
Generating a 1024 bit RSA private key
.............++++++
.....................................++++++
writing new private key to 'symapisrv_key_v8.0.pem'
-----
Signature ok
subject=/CN=storsrvd
   aaa.bbb.com/ST=Massachusetts/C=US/L=Hopkinton/emailAddress=support@emc.com/O=EM
   C Corporation/OU=EMC Enterprise Storage Automation
Getting CA Private Key
The files symapisrv_cert_v8.0.pem and symapisrv_key_v8.0.pem were created in the
   directory /var/symapi/config/cert.
```

Working with a host in multiple domains

When client/server is running on a host that is in multiple domains (for example, `host001.acme.com` and `host001.example.com`), a client or server may not be able to verify the certificate being sent by the other host. This occurs because only one fully qualified name is written to the certificate during installation.

For small numbers of short names (such as those above), you can explicitly spell them out, without using the wildcard.

If the names are long, or if there are many of them, use the **-san** option to add multiple names to a certificate.

To create a certificate, run the following command from the `cert` directory:

```
<SYMCLI_BIN> manage_server_cert create host_name -pass
<LockBoxPassword> -san host host host_wildcard ...
```

"manager_server_cert commands syntax" on page 44 describes the command format for your platform.

For example, running the following command in a UNIX environment:

```
/usr/storapi/bin/manage_server_cert.bat create lab1 -pass
<LockBoxPassword> -san 10.244.245.153 *.bbb.acme.com
lqam*.bbb.acme.com
```

produces output similar to the following:

```
Generating a 1024 bit RSA private key
.............++++++
.....................................++++++
writing new private key to 'symapisrv_key_v8.0.pem'
-----
Signature ok
subject=/CN=storsrvd
   lab1/ST=Massachusetts/C=US/L=Hopkinton/emailAddress=support@emc.com/O=EMC
   Corporation/OU=EMC Enterprise Storage Automation
Getting CA Private Key
The files symapisrv_cert_v8.0.pem and symapisrv_key_v8.0.pem were created in the
   directory /var/symapi/config/cert.
```

Working with a Windows cluster

This section describes procedures to perform when working with Windows clusters.

Creating a certificate that includes both the hostname and cluster name

During client/server operations, if either the client or server is in a Windows cluster, the hostname sent to the other system may be a cluster name and not a hostname. When the host tries to verify the certificate, it will not find the cluster name since it is not included during installation on the server.

To correct this problem, you can create a certificate with the hostname and the cluster name in it by running the following command from the `cert` directory:

```
<SYMCLI_BIN>\manage_server_cert.bat create
fully_qualified_host_name -pass <LockBoxPassword> -san
fully_qualified_cluster_name
```

For example, running the following command:

```
C:\Program Files\EMC\SYMAPI\config\cert> "\
Program Files\EMC\SYMCLI\bin\
manage_server_cert.bat" create host001.acme.com -pass
<LockBoxPassword> -san host001cluster.acme.com
```

produces output similar to the following:

```
Generating a 1024 bit RSA private key
.............++++++
.....................................++++++
writing new private key to 'symapisrv_key_v8.0.pem'
-----
Signature ok
subject=/CN=storsrvd
   host--1.emc.com/ST=Massachusetts/C=US/L=Hopkinton/emailAddress=support@emc.com/
   O=EMC Corporation/OU=EMC Enterprise Storage Automation
Getting CA Private Key
The files symapisrv_cert_v8.0.pem and symapisrv_key_v8.0.pem were created in the
   directory /var/symapi/config/cert.
```

Adding virtual server names to a certificate

If virtual server names are defined in the Windows cluster, you should also add these names to the certificate by running the following command from the `cert` directory:

```
<SYMCLI_BIN>\manage_server_cert.bat create clustername -pass
<LockBoxPassword> -san servername1 servername2 servername3
servername4 servername5 servername6 servername7 ...
```

Note: You can specify any number of arguments in the manage_server_cert.bat script.

For example, running the following command from the `cert` directory:

```
C:\Program Files\EMC\SYMAPI\config\cert> "\Program
Files\EMC\SYMCLI\bin\
manage_server_cert.bat" create cluster -pass <LockBoxPassword> -san
svr1 svr2 svr3 svr4 svr5 svr6 svr7
```

produces the following output:

```
Generating a 1024 bit RSA private key
.............++++++
.....................................++++++
writing new private key to 'symapisrv_key_v8.0.pem'
-----
Signature ok
subject=/CN=storsrvd
   cluster/ST=Massachusetts/C=US/L=Hopkinton/emailAddress=support@emc.com/O=EMC
   Corporation/OU=EMC Enterprise Storage Automation
Getting CA Private Key
The files symapisrv_cert_v8.0.pem and symapisrv_key_v8.0.pem were created in the
   directory /var/symapi/config/cert.
```

You can also use the following command to perform the same operation:

```
C:\Program Files\EMC\SYMAPI\config\cert> "\Program
Files\EMC\SYMCLI\bin\manage_server_cert.bat" create cluster -pass
<LockBoxPassword> -san svr*
```

Working with a multi-homed host

When the client or server is running on a multi-homed host (that is, a host with multiple hostnames), a client or server may not be able to verify the certificate being sent by the other host. This occurs because only one fully qualified name, which is obtained from the hostname command, is written to the certificate during installation.

To correct this problem, you can create a certificate for the multi-homed host containing all of its hostnames by running the following command from the `cert` directory:

```
<SYMCLI_BIN>/usr/storapi/bin/manage_server_cert.sh create -pass
<LockBoxPassword> -san multi-homed-name1 multi-homed-name2 [...]
```

"manager_server_cert commands syntax" on page 44 describes the command format for your platform.

For example, running the following command on host 'host000' in a UNIX environment:

```
/usr/storapi/bin/manage_server_cert.sh create
-pass <LockBoxPassword> -san host001.acme.com host002.acme.com
host003.acme.com
```

produces output similar to the following:

```
Generating a 1024 bit RSA private key
.............++++++
.......................................++++++
writing new private key to 'symapisrv_key_v8.0.pem'
-----
Signature ok
subject=/CN=storsrvd
   host000.bbb.com/ST=Massachusetts/C=US/L=Hopkinton/emailAddress=support@emc.com/
   O=EMC Corporation/OU=EMC Enterprise Storage Automation
Getting CA Private Key
The files symapisrv_cert_v8.0.pem and symapisrv_key_v8.0.pem were created in the
   directory /var/symapi/config/cert.
```

Listing the hostnames in the certificate

Use the following command to list the hostnames contained in the certificate:

```
<SYMCLI_BIN>/manage_server_cert.sh list
```

"manager_server_cert commands syntax" on page 44 describes the command format for your platform.

For example, running the following command in a Windows environment:

```
/usr/storapi/bin/manage_server_cert.bat list
```

produces output similar to the following:

```
The host names in this machine's certificate:
lab1
10.244.245.153
*.bbb.acme.com
lqam*.bbb.acme.com
```

Managing the Solutions Enabler server

This section describes activities to manage the Solutions Enabler server, including:

- "Starting the Solutions Enabler server"

- "Restricting access to the Solutions Enabler server " on page 53
- "Restricting the number of concurrent connections" on page 55
- "Restricting functionality in the Solutions Enabler server" on page 56
- "IBM z/OS-specific behavior for control operations" on page 57

Starting the Solutions Enabler server

The `storsrvd` daemon does not run by default. You must explicitly start it before it can accept connections from remote clients. Run the following command to start the `storsrvd` daemon:

```
stordaemon start storsrvd
```

You can configure the `storsrvd` daemon to start automatically whenever a server host starts by running the following command:

```
stordaemon install storsrvd -autostart
```

Daemons are started differently on z/OS platforms. The *EMC Solutions Enabler Installation Guide* provides detailed instructions on starting the Solutions Enabler server.

Restricting access to the Solutions Enabler server

Use the `<SYMAPI_HOME>/config/nethost` file on a server host to restrict the hosts and users from which the `storsrvd` daemon accepts connections. If the `nethost` file is not present, connections are accepted from all client hosts.

Each line of the `nethost` file identifies authorized hosts with an optional comma-separated list of user names. If a host's user list is omitted or is specified as an asterisk (*), all users connecting from that host are accepted.

When the `nethost` file exists, only the nodes/users listed in this file are allowed to connect to the server to execute remote SYMAPI functions. The trusted host file uses the following format:

```
node                    user-1 [, …, user-n]
address                 user-1 [, …, user-n]
*                       user-1 [, …, user-n]
node                    *
address                 *
*                       *
```

Note: `*` denotes a wildcard for any host or any user, and that no spaces are permitted between user names (such as `joe,sally`). For example:

```
# From Client host host001, all users may connect.
host001        *
# From Client host host002, only users joe and sally may connect.
host002       joe,sally
# An IP address can be used instead of a hostname.
180.100.90.75 *
```

Connections from hosts or users not in the `nethost` file are refused. When a connection is refused, an error message containing the requesting client's user and hostname is written to the `storsrvd` log file on the server.

The `nethost` file is reprocessed every time a new session starts. Any updates made to the file while the server is running will be applied to all future sessions.

Note: The server considers the contents of this file before deciding whether it will negotiate a SYMAPI session with the client. If the client host and user are not defined in the `nethost` file, a session will not be negotiated, regardless of the security level. "Securing remote connections using SSL" on page 37 provides more information on the SSL security settings.

Considerations for specifying node and address

The identity of a client host may vary from the perspective of the server, since the server can accept connections from IPv4 and IPv6 clients.

Thus, the network address of the client could be an IPv4 or IPv6 address.

If you specify the network address in the `nethost` file instead of the node name, then the exact syntax of the address is important. If you incorrectly specify an address, connections from some clients may be denied.

EMC recommends that you specify the node name (or the FQDN) since proper DNS configuration usually ensures that the name of the client host is consistent, regardless of the network address.

If you must specify the address, keep these factors in mind:

- The rules for specifying an IPv4 address are simple: Specify the complete address in its dotted-decimal form, without leading zeros in each octet. For example:

  ```
  172.23.191.20          user1
  10.243.142.82          user1
  ```

- If you want to specify an IPv6 address, follow these shorthand rules (part of the IPv6 standard):
  - Leading zeros in each quartet can be omitted.
  - Contiguous sets of zeros can be replaced by two adjacent colons, but only once in an address. If there are multiple non-adjacent sets of contiguous sets of zeros, only one set of double colons can be used. The other set of zeros must be specified. For example:

    ```
    3FFE:80C0:22C:18:250:88FF:FEAD:F92F
    ```

    If you are uncertain about the address syntax, ask your network administrator to determine the exact syntax. For most UNIX and Linux hosts, the `ifconfig -a` command can be used to display the IPv6 address of a machine. In a Microsoft Windows environment, use the `ipconfig /all` command to display the IPv6 address.

- If you have IPv4 client hosts that connect to IPv6-capable servers on AIX or Linux, the client network address appears as IPv4-mapped addresses. The server host file validation logic takes this into account and treats IPv4-mapped addresses as though they are native IPv4 addresses. Thus you can specify the regular IPv4 address as described in the first point above.

- You may have to experiment to find the right address.

Restricting the number of concurrent connections

The maximum number of concurrent connections from client hosts is controlled by the `storsrvd:max_sessions` daemon option. When a new session arrives that exceeds the threshold, it is refused.

The default and maximum value is 100.

Concurrent sessions may be limited based on the source hostname or username of the client:

- **Limiting by source host** is based on the IP address of the host where the client session originates. User name is not considered when counting concurrent connections from hosts.
- **Limiting by source user** is based on the user identity format described in the "User identification" on page 28. Only two types of user identity formats are counted:
  - The H: format identifies that the client user has been authenticated by the local operating system. This format is used when the client comes from any UNIX or Linux type of host, or from a Windows host where the user has logged into the local system (not a Windows domain). In the host authentication case, the user is considered the same only when logging in from the same host with the same user name.
  - The D: format is used when the client user has logged into a Windows domain. In this case, a user can log into the same domain from different host computers. Such a user identity is considered the same, without respect to the source host that initiates the session.

Two configuration statements for `storsrvd` control session refusal from specific sources:

- `storsrvd:max_sessions_per_host=value` – This option specifies the maximum number of concurrent sessions from any specific host. If a new session from the source host exceeds the threshold for that host, the session is refused.
- `storsrvd:max_sessions_per_user=value` – This option specifies the maximum number of concurrent sessions from any specific user. If a new session from the same user exceeds the threshold for that user, the session is refused.

Table 14 on page 56 lists the `storsrvd` session control options and values.

Note: These options and values are only used by the `storsrvd` daemon and apply to SYMAPI remote sessions. There is no impact on the use of the `stordaemon` control CLI or any other Solutions Enabler daemon.

Best practices for setting the `storsrvd` session control options:

- Set `max_sessions_per_host` and `max_sessions_per_user` to a value less than `max_sessions`. Specifically:
  - Set `max_sessions` to the highest number of concurrent sessions you will tolerate without respect to the source host or user of the session.
  - Set `max_sessions_per_host` and `max_sessions_per_user` to lower values, reflecting the maximum number of concurrent sessions from specific sources you will tolerate.

- Both `max_sessions_per_host` and `max_sessions_per_user` can be used concurrently to count sessions.
- It is possible to set either `max_sessions_per_host` and `max_sessions_per_user` to 0, but doing so refuses all new connections. EMC recommends that if you want to refuse all sessions temporarily, set `max_sessions` to 0. When you wish to resume accepting new sessions, change `max_sessions` to a non-zero value.

Table 14 storsrvd daemon session control options and values

Option name	Values	Default	Notes
max_sessions	0 – All new sessions are refused. 1 – 100 – Maximum (host and user) sessions allowed.	100	Default of 100 is compatible with previous releases.
max_sessions_per_host	0 – All new sessions are refused. 1 – 100 – Maximum number of sessions allowed from a specific host. NOLIMIT -Disables counting of sessions from a specific host.	NOLIMIT	NOLIMIT value provides backward compatibility. NOLIMIT is case-insensitive: NOLIMIT = nolimit
max_sessions_per_user	0 – All new sessions are refused. 1 – 100 – Maximum number of sessions allowed from a specific user. NOLIMIT – Disables counting of sessions from a specific user.	NOLIMIT	

Restricting functionality in the Solutions Enabler server

Settings in the `<SYMAPI_HOME>/config/options` file on a server host can be used to restrict the functionality that the `storsrvd` daemon is allowed to perform on behalf of remote client hosts.

Check to make sure all references to the options file have a path name of `<SYMAPI_HOME>/config/options`. These options can be changed by editing the `options` file while the server is running. The running server uses the new settings for all future sessions.

Since these are not specified in the `<SYMAPI_HOME>/daemon_options` file, they cannot be changed using the `stordaemon setvar` command.

Table 15 lists the options to restrict the `storsrvd` daemon:

Table 15 Options that restrict storsrvd functionality (page 1 of 2)

Option name (in ‹*SYMAPI_HOME*›/config/options)	Description
SYMAPI_ACC_ADMIN_VIA_SERVER	Enable/disable Symmetrix Access Control changes. Default is ENABLE.

Table 15 Options that restrict storsrvd functionality (page 2 of 2)

Option name (in <*SYMAPI_HOME*>/config/options)	Description
SYMAPI_ACC_DISPLAY_VIA_SERVER	Enable/disable Symmetrix Access Control information displays. Default is ENABLE.*
SYMAPI_ALLOW_SCRIPTS_VIA_SERVER	Enable/disable TimeFinder® pre-action and post-action scripts. Default is DISABLE.
SYMAPI_CTRL_VIA_SERVER	Enable/disable array control operations in general. Default is DISABLE.*

*When set to DISABLE, this class of functionality is not available through the server.

IBM z/OS-specific behavior for control operations

By default, a Solutions Enabler server running on any z/OS host allows configuration changes when requested by a remote client. The *EMC Solutions Enabler Installation Guide* provides additional information.

NOTICE

If control operations are left enabled by default, remote Open Systems users (client/server mode) can make changes to the array configuration on your mainframe system.

Data security settings

Solutions Enabler maintains important configuration data in a number of files. It is important that you back up and protect these files at all times. If lost, functionality that depends on the data in these files may be impacted.

"Maintenance: back up Solutions Enabler state" on page 69 provides information on the complete set of directories to back up regularly.

Table 16 Important Configuration Files and Locations

File location	Description
`<SYMAPI_HOME>/config/emcpwddb.dat`	This file stores connectivity information (including user names and passwords) used to interact with CLARiiON storage arrays and VMware/Hyper-V Virtual Infrastructure Services. It is managed using the `symcfg authorization` SYMCLI command. The file is encrypted to protect its contents and prevent tampering.
`<SYMAPI_HOME>/db/symapi_db.bin`	The Solutions Enabler database file contains array topology information; arrays, devices, directors, and other information.
`<SYMAPI_HOME>/config/lockboxp2`	This file contains sensitive configuration information. The file is encrypted to protect its contents to prevent tampering.
`<SYMAPI_HOME>/gns/storgnsd.db`	The Solutions Enabler groups database file contains information about CG's, DG's and their contents.

Securing Solutions Enabler configuration files

Solutions Enabler stores its configuration files in the following directory:

```
<SYMAPI_HOME>/config
```

Protect the files in the `config` directory by making sure only authorized Solutions Enabler administrators have write access.

All other users should have {no access | read-only access}.

Running commands as a non-privileged user

Following an initial installation of Solutions Enabler, most SYMCLI commands can only be run as a root user on UNIX systems and by an administrator on Windows systems. To allow other users to execute these commands (for example `symcfg discover`), you must grant them write access to the following directories and their contents:

```
<SYMAPI_HOME>/config
<SYMAPI_HOME>/db
```

In addition, non-root users on UNIX and non-administrators on Windows must be authorized (using the `stordaemon` command) to manage daemons, and to use daemons in the process of running SYMCLI commands. To authorize these users, add an entry for a specific user in the file `<SYMAPI_HOME>/config/daemon_users`. For example:

```
# Allow user 'jones' to make use of the storapid daemon:
jones       storapid

# A '*' character at the end of a name can be used
# as a simple wildcard. The following allows user 'jones'
# to make use of any of the Solutions Enabler daemons:
jones       stor*
```

The `<SYMAPI_HOME>/config/README.daemon_users` file installed with Solutions Enabler provides additional information on this topic.

Managing the encrypted lockbox

Solutions Enabler uses an encrypted lockbox to store and protect sensitive information. The lockbox is associated with a particular host. This association prevents the lockbox from being copied to a second host and used to obtain access.

The lockbox is created at installation. During installation, the installer is prompted to provide a password for the lockbox. If no password is provided at installation, a default password: host_name@SELockbox1 is generated and stored in the lockbox along with Stable System values (SSVs, a fingerprint that uniquely identifies the host system). The host_name is the same value as returned by the hostname command.

The SSV values validate access to the lockbox. When data is written to or retrieved from the lockbox, the SSVs in the lockbox are compared against the SSVs generated from the host. If the SSVs match, the operation is permitted. If the SSVs do not match, the operation fails.

When Solutions Enabler is upgraded, product information in the existing lockbox is automatically copied into the lockbox when the lockbox is first accessed.

When the host is upgraded, or when the lockbox file is moved to another host, the host fingerprint may no longer match and the values inside of the lockbox must be reset, as described in "Changing the lockbox password/SSVs" on page 60.

The lockbox is used on the following platforms:

- HP-UX 11.23 and 11.31
- IBM AIX 6.1 and AIX 7.1
- Microsoft Windows XP Professional SP2, Vista Enterprise, and 7 Enterprise
- Microsoft Windows Server 2003 SP2, 2008, and 2008 R2
- Novell SUSE Linux Enterprise Server 10.0 SP1 to SP4, 11.0 SP1, and SP2
- Oracle Solaris 10 and 11
- Red Hat Enterprise Linux AS 5.0 U1 to U8, AS 6.0 U1, and U2
- OVMS
- z/OS

For other Solutions Enabler platforms, lockbox functions do not change.

About lockbox passwords

EMC recommendation

If you chose to create the lockbox using the default password (during installation), change the password immediately after installation to best protect the contents in the lockbox.

For maximum security, select a password that is hard to guess. It is very important to remember the password.

⚠WARNING

Loss of this password can lead to situations where the data stored in the lockbox is unrecoverable.

Passwords must meet the following requirements:

- 8 - 256 characters in length
- Include at least one numeric character
- Include at least one uppercase and one lowercase character
- Include at least one of the following non-alphanumeric characters: ! @ # % &

  Lockbox passwords may include any character that can be typed in from US standard keyboard.
- The new password must not be the same as the previous password.

The default lockbox password

When you install Solutions Enabler, you are asked whether to you want to use the default password for the lockbox. If you choose to use the default, the installation process establishes the default lockbox password in the following format:

nodename@SELockbox1

where: *nodename* is the hostname of the computer on which you are installing. Operating systems have different methods of determining the nodename:

Unix: The installation program uses the `hostname` command to determine the node name. Normally, the node name is set in the /etc/hosts file

Windows: TBD.

z/OS: The `gethostname()` function is used to get the node name of the machine.

If the value of the *nodename* is stored in upper case letters, it is converted to lower case for the default password.

IMPORTANT

If you allow the installation program to use the default password, you must make a note of it for future use. You will need the password if you need to reset the lockbox Stable System Values or generate certificates for client/server operations.

Changing the lockbox password/SSVs

SSVs are platform-dependent, thus changes to hardware or software on a host could require a reset of the SSVs stored in the lockbox.

Solutions Enabler supports administrative interactions with the lockbox including:

- Changing the password used to protect the lockbox.
- Resetting the saved SSVs in the lockbox after attributes on the host change, making the lockbox inaccessible to user-initiated SYMAPI and SYMCLI calls.

Two new `symcfg` commands allow administrative interactions with the lockbox:

```
symcfg -lockbox [-password <Password>]
   reset -ssv
   setpw [-new_password <NewPassword>]
```

Note: Both commands require the existing password.

Changing the lockbox password

Use the following steps to change the password on the lockbox:

1. Type the following command:

   ```
   symcfg -lockbox setpw
   ```

For example:

```
[root@host0100 api]# ../cli/symcfg64 -lockbox setpw
```

A prompt to enter the current lockbox password appears:

```
password:
```

Note: If the lockbox is not present, this command will fail with an error. The lockbox file needs to be created with the symcfg -lockbox reset -ssv command.

2. Type the current password* and press ENTER. A second prompt appears:

```
New password:
```

3. Type the new password* and press ENTER. The following message appears:

```
Confirm new password:
```

4. Type the new password* and press ENTER. The following message appears:

```
Lockbox password has been successfully changed.
```

* The password and the new password are not displayed on the screen.

You can also enter the old password and new password in a single command line:

```
[root@DLDV0130 api]# ../cli/symcfg64 -lockbox -password SELockbox#1
setpw -new_password SELockbox#2

[root@DLDV0130 api]#
```

⚠CAUTION

Do not forget the new password. If you change the default password, and then forget it, there is no way to recover it.

Changing the SSVs

Use the following syntax to change the SSVs stored in the lockbox:

```
symcfg -lockbox reset -ssv
```

For example:

1. Type the following command:

```
symcfg -sid 123 -lockbox reset -ssv
```

A prompt to enter the lockbox password appears:

```
password:
```

2. Type the password* and press ENTER. The following message appears:

```
Lockbox Stable System Values have been successfully reset.
```

* The password is not displayed on the screen.

Daemon security settings

Solutions Enabler uses a number of helper daemon processes:

- storapid
- storevntd
- storgnsd
- storrdfd
- storsrmd
- storsrvd
- storwatchd

Daemon identity on UNIX

On UNIX, daemons run as a root user by default.

Some daemons can be configured to run as an identity other than a root user. The daemons that may run as non-root user are:

- storevntd
- storgnsd
- storrdfd
- storsrvd
- storstpd
- storwatchd (Unix only)

Note: The storapid (base) daemon must run as root.

You can configure daemon user identity:

- During Solutions Enabler installation in either the interactive or silent install process. Refer to the *Solutions Enabler Installation Guide* for the details on how to choose non-root daemon execution during install.
- Post-installation using the `stordaemon` command. For information on which daemons are affected by this option, refer to the `stordaemon` man page.

The following considerations apply to running daemons as a non-root user:

- When configured to run as a non-root user, all daemons must run as the same user.
- `stordaemon setuser` sets the UNIX setuid bit on the daemon executables to the named user.
- `stordaemon setuser` alters permission s of directories and files under /var/symapi such that the named user can create and delete, read, write the files it needs during normal operation

To configure all daemons to run under the bin user account:

```
stordaemon setuser all -user bin
```

Authorized users are allowed to control daemons using the `stordaemon` command line utility. For example, to start the SRM daemon:

```
stordaemon start storsrmd
```

Non-root and non-administrative users must be defined in the `daemon_users` file to obtain authorization for using daemons and other daemon services.

For additional information, refer to:

- The `stordaemon` man page.
- `<SYMAPI_HOME>/config/README.daemon_users` file installed with Solutions Enabler.

Securing host directories

The Solutions Enabler daemons can run with root privileges for UNIX systems and system account file privileges for Windows systems.

These privileges are typically greater than the privileges granted to users making use of the daemon processes. This can present security vulnerabilities in situations where a user through a CLI or some other application provides a pathname on which a daemon can operate, such as a backup file to be written to or read from.

To prevent these security vulnerabilities for the `storsrvd` daemon running as a root user, you can specify a list of secure directories in which the `storsrvd` daemon can read, write, and execute files. Existing mechanisms protect the Solutions Enabler database and log file locations. Specify a list of secure directories for the `storsrvd` daemon to protect other operations, such as backups and restores.

Note: When daemons are running as non-root user, the secure_directory_path option is ignored. In this case, the privileges of the non-root user are used when attempting to write output files in specific directories.

Specifying a secure directory path

Review the following before specifying a `secure_directory_path` for the `storsrvd` daemon running as a root user:

- The supplied pathname directories must exist when the daemon is started or the `daemon_options` file is reloaded.

  Nonexistent paths are ignored.
  All subdirectories below the specified directories are also treated as being secure.

- A total of 32 secure directory locations can be maintained.
- Once the `storsrvd` daemon has read the `security_directory_path` statement, directories specified cannot be removed without changing the value in the `daemon_options` file and restarting the daemon.
- New directories can be added while the `storsrvd` daemon is running by editing the `daemon_options` file and reloading it using the following command:

  `stordaemon action storsrvd -cmd reload`

- If the `secure_directory_path` option is not present, no security checks are performed).
- The `secure_directory_path` option does not apply to the following pathnames:
  - Pathnames provided in the `options` or `daemon_options` files.

    These files are assumed to be protected by an administrator.

    An exception is the path named in the storstpd:dmn_root_location option:

    If storstpd is running as root, and was started by a non-root user using the stordaemon command, storstpd validates that the path in the dmn_root_location option is also specified in the secure_directory_path option.

  - Pathnames accessed (read or written) by the SYMCLI itself.

    In client/server mode, these occur under the identity of the user and are subject to standard access control checks against the user identity.

  - Pathnames accessed by an API on the client host in client/server mode because these occur under the identity of the user and are not a security risk.

Windows platforms

On Windows platforms, the secure directory path is a list of directories separated by a semicolon (;). Use the backward slash (\) when specifying each directory name.

To apply the secure_directory_path to the `storsrvd` daemon:

```
storsrvd:secure_directory_path = c:\Temp\dir1;c:\Users\SE
```

UNIX platforms

On UNIX platforms, the secure directory path is a list of directories separated by a semicolon (;) or a colon (:). Use the forward slash (/) when specifying each directory name.

To apply the secure_directory_path to the `storsrvd` daemon:

```
storsrvd:secure_directory_path = /tmp/dir1;/opt/dir2;/users/se
```

Listing secure directories

To display a list of secure directories in effect for the `storsrvd` daemon:

```
stordaemon getvar storsrvd -name secure_directory_path
```

Authorizing daemon connections

By default, daemons only accept connection requests from users running with root or administrator privileges.

For non-root users to use this feature, create a `<SYMAPI_HOME>/config/daemon_users` file (initially installed as `README.daemon_users`) with a list of allowed usernames.

Using a text editor, a system administrator can add entries to this file using the following formats:

smith storapid	Local user smith is authorized to use the `storapid` daemon.
ENG/smith storapid	Windows local user smith in the ENG domain is authorized to use the `storapid` daemon.
smith storora*	Local user smith is authorized to use any daemon whose name begins with `storora`. For example, the SRM Oracle DB daemons. (The `*` is a wildcard.)
smith stororad freeze,...	Local user smith is authorized to perform freeze and thaw operations using the `stororad` daemon. The third column consists of a comma separated list of operations that the user is authorized to perform. Valid values are: • freeze: The user is authorized to perform DB freeze and thaw operations. • startup_instance: The user is authorized to start a DB instance. • shutdown_instance: The user is authorized to shutdown a DB instance.

Note: Privileged users are automatically authorized, and do not need to be added to this file. Solutions Enabler daemons make connections between one another. Daemon-to-daemon connections are automatically authenticated and authorized.

Note: For more information, refer to the `daemon_users` file.

Securing SRM operations

This section describes activities pertaining to configuring security for EMC's Storage Resource Management (SRM).

Authorizing SRM daemon connections

Access to SRM functionality is controlled by limiting permission to the SRM daemon. This access is controlled using the common daemon authorization file, `<SYMAPI_HOME>/config/daemon_users`.

Note: It is important to protect this file so that only privileged administrators can modify it.

Users meeting any of the following criteria are permitted to control and use the SRM daemon:

- Authorized users: UNIX users with root access, and Windows users that are a members of the Administrators group
- Users listed in the `daemon_users` file located on each host from which they require access

For example, the following lines in the `daemon_users` file would permit users named `smith` and `jones` to use the SRM daemon:

```
smith     storsrmd
jones     storsrmd
```

Various SRM control operations for authorized local users can be defined by adding the appropriate control operation keyword to the `daemon_users` file command line in the third column, as shown in the following example:

```
smith     storsrmd      file_allocate, file_extend
jones     storsrmd      file_allocate, file_extend
```

Note: Multiple control operations can be added to the line, separated by a comma.

Table 17 lists the available SRM control operations by keyword that can be added for a user. The keyword must be added to the `daemon_users` file to authorize the user to perform the specified SYMCLI control operations.

Table 17 SRM control operations (page 1 of 2)

Keyword	Control operation	SYMCLI command
file_allocate	Allocate a file	Not available
file_extend	Extend a file	Not available
file_trim	Trim a file	Not available
fs_flush	Flush a file system	Not available

Table 17 SRM control operations (page 2 of 2)

Keyword	Control operation	SYMCLI command
fs_freeze	Freeze a file system	Not available
fs_thaw	Thaw a file system	Not available
lv_create	Create a logical volume	symlv create
lv_delete	Delete a logical volume	symlv delete
lv_resize	Resize a logical volume	symlv extend symlv reduce
lv_mirror_add	Add a logical volume mirror	symlv add
lv_mirror_remove	Remove a logical volume mirror	symlv remove
vg_create	Create a volume group	symvg create
vg_delete	Delete a volume group	symvg destroy
vg_device_add	Add a device to a volume group	symvg adddev
vg_device_remove	Remove a device from a volume group	symvg rmdev
vg_recover	Recover a volume group	symvg recover

Note: For any directories and files being accessed for SRM control and mapping operations, operating-system-level permission is required. "Setting operating-system-level permissions for SRM" provides more information on this topic.

Setting operating-system-level permissions for SRM

The operating-system-level permissions for any directories and files being accessed for the control and mapping operation must be set for the user. The following examples show various administrator settings for directories and files to allow read (r), write (w), and execute (x) privileges:

Permits root user access:

```
-rwx--------  root  other  /usr/vxfs/root.bin
```

Permits user smith and root access:

```
-rwx-------  smith  symapi  /usr/vxfs/smithroot.bin
```

Permits all users access:

```
-rwxrwxrwx  root  other  /usr/vxfs/allusers.bin
```

Connecting to the SRM database

A connection must be established between the SRM database and the database commands to allow access to the database. To connect to the database, set `SYMCLI_RDB_CONNECT` to your username and password. When working with one type of database, use `SYMCLI_RDB_TYPE` to save keystrokes with a set of commands.

Note: For a non-root user on Solaris, the Sybase database daemon must be manually started from the root user before calling any Sybase database functions.

If the connection is remote, a network service name must be supplied with the password.

For SYMCLI mapping access to an Oracle database, the user must have one of the following:

- Select any table privilege
- DBA role
- SYSDBA role

To invoke control access of an Oracle database, the user must have administrator privileges.

Database start-up options

The database control commands start up and shut down of the specified database server manager instance.

Database manager instance start up or shut down can be done on the client side. This removes the limitation of most databases that only allows start-up and shutdown of their database manager instance on the database server side.

Use the `symrdb startup -type DbType` CLI command to start up the specified database, including: Sybase, Oracle, SQL Server, and DB2/UDB databases.

Note: Database start-up and shutdown options are not available for Informix databases.

Sybase

The following options are available for Sybase databases:

```
symrdb startup
      -type Sybase
      -f runserver_file
      -m
      -t delay_time
```

where:

- *runserver_file* — Specifies the absolute pathname of a runserver file used as a reference each time a Sybase server is restarted.
- **-m** — Starts the database in single user mode.
- *delay_time* — Specifies the estimated time, in seconds, to start up the Sybase server.

SQLServer

The following start-up options are available for SQLServer databases:

```
symrdb startup -type SqlServer -s instance [-c] [-f] [-m] [-n] [-x]
      -p master_file_path
      -e error_log_path
      -l master_log_path
      -g virtual_addr_space
      -t trace_number
```

where:

- *instance* — Instance name to be started.
- *master_file_path* — Master database file.
- *error_log_path* — Error log file.
- *master_log_path* — Master database log file.
- *virtual_addr_space* — Amount of virtual address space, in megabytes.
- *trace_number* — Trace number.

DB2/UDB

The following start-up options are available for DB2/UDB databases:

```
symrdb startup -type IBMUDB [-c computer]
      [-n node [ADDNODE -u hostname -p port
      [-nt netname] [NODE | CATALOG -tsn tablespace_node]] |
      [RESTART [-u hostname] [-p port] [-nt netname]]|[STANDALONE]]
```

where:

- **ADDNODE** — Issues the ADD NODE command.
- **RESTART** — Issues the RESTART DATABASE command.
- **STANDALONE** — Start the node in STANDALONE mode.
- **NODE** — Specifies that the containers for the temporary tablespaces should be the same as those for the specified node.
- **CATALOG** — Specifies that the containers for the temporary tablespaces should be the same as those for the catalog node of each database.
- *profile* — Specifies the name of the profile.
- *node* — Specifies the node number.
- *hostname* — Specifies the system name.
- *port* — Specifies the port number.
- *netname* — Specifies the net name.
- *tablespace_node* — Specifies the node number from which the temporary tablespace definitions should be obtained.
- *computer* — Specifies the computer name.

Oracle

The following start-up options are available for Oracle databases:

```
symrdb startup -type Oracle [[FORCE][RESTRICT][PFILE=FileName][QUIET]
   [MOUNT [-db DbName] |
   [[OPEN | OPEN_READ_ONLY | OPEN_READ_WRITE | OPEN_READ_WRITE_RECOVER
   | RECOVER | OPEN_RECOVER]
   [-db DbName] ] | NOMOUNT]] |
   [ [PFILE=FileName] MIGRATE [QUIET]]
```

where:

- *FileName* — Specifies the file to be used while starting up the instance.
- *DbName* — Specifies the database name to mount or open. Refer to the Oracle document for the definition.

- FORCE — Shuts down the current Oracle instance (if it is running) with the shutdown option ABORT before restarting it.
- RESTRICT — Allows only Oracle users with the RESTRICTED SESSION system privilege to connect to the database.
- QUIET — Suppresses the display of the System Global Area information for the starting instance.
- MOUNT — Mounts the database but does not open it.
- OPEN — Mounts and opens the database.
- NOMOUNT — Causes the database not to be mounted upon instance start-up.
- MIGRATE — Starts the database in OPEN MIGRATE mode and sets system initialization parameters to specific values required to enable the database upgrade or downgrade scripts to run.
- OPEN_RECOVER — Opens the database and performs media recovery, if necessary, before starting the instance.
- OPEN_READ_ONLY — Specifies READ ONLY to restrict users to read-only transaction, preventing them from generating redo logs.
- OPEN_READ_WRITE — Specifies READ WRITE to open the database in read/write mode, allowing users to generate redo logs. This is the default.
- OPEN_READ_WRITE_RECOVER — Specifies READ WRITE to open the database in read/write mode and specifies that media recovery should be performed, if necessary, before starting the instance.

Maintenance: back up Solutions Enabler state

Back up the following directories and their contents to preserve the Solutions Enabler configuration on a host:

```
<SYMAPI_HOME>/config
<SYMAPI_HOME>/db
<SYMAPI_HOME>/gns
```

If you want to retain the logs for audit purposes, include the ‹*SYMAPI_HOME*›/log directory in your backups.

The other directories under ‹*SYMAPI_HOME*› contain less critical data that is recreated by Solutions Enabler as needed.

CHAPTER 4
Unisphere for VMAX security configuration tasks

This chapter describes security settings for Unisphere for VMAX, including:

- Unisphere access control 72
- User-based access control..... 73
- Using the encrypted lockbox 78
- Port usage..... 82
- Replacing the Unisphere for VMAX server certificate 79
- Other security settings 81

Security controls map

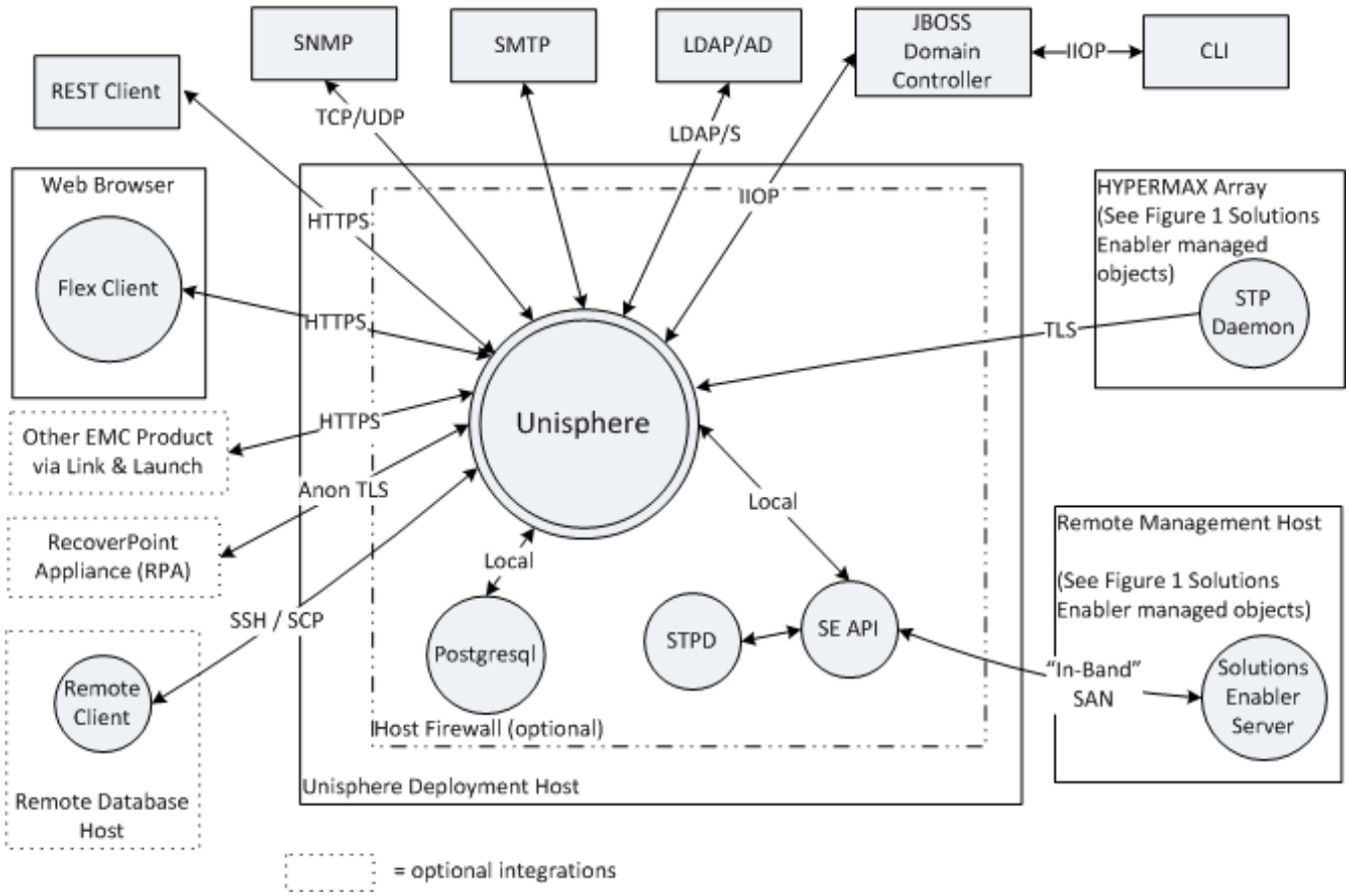


Figure 2 Unisphere components

Unisphere access control

Unisphere supports the following types of user authentication:

- **Windows** (local and domain-based): Users have a Windows account on the SMAS server.

  Users login with Windows domain\username and password.

- **LDAP**: User accounts are stored on an LDAP server, which may be accessible over LDAPS (LDAP with SSL).

  To use this method, a Unisphere Administrator or SecurityAdmin must set up LDAP-SSL authentication in Unisphere. *Configuring authentication* in the *Unisphere for VMAX Installation Guide* and online help includes instructions for completing this task.

IMPORTANT

EMC strongly recommends using VPN solutions if the customer's LDAP servers are outside the DMZ, and in the cases where the customer's Unisphere deployment is vulnerable to man-in-the-middle attack (due to malicious insiders).

- **Local Unisphere users**: Users can have local Unisphere accounts.

  Users login with their Unisphere username and password.

  Local user accounts are stored locally on the SMAS server host and work in much the same way as the other methods to validate user credentials.

  To use this method, a Unisphere Initial Setup User, Administrator, or SecurityAdmin must create a local Unisphere user account.

Unisphere for VMAX Installation Guide and online help includes instructions for completing this task.

Trust in Unisphere is established using the sequence described in "Port usage" on page 82.

User-based access control

Unisphere uses "roles" and groups to restrict which management operations a user can perform on an array.

The steps to create and manage Unisphere user accounts, including user authorization are described in *EMC Unisphere for VMAX Installation Guide* and *EMC Unisphere for VMAX* online help.

Default user account

The Initial Setup User is created during installation.

The Initial Setup User is a temporary local user created by the Unisphere installer software. The Initial Setup User has an Administrator role, and is used to install and set up Unisphere. Once an Administrator or SecurityAdmin is assigned to an array, the Initial Setup User can no longer access or view the array from the Unisphere console.

EMC recommends that you delete this user as soon as the array is configured.

The steps to create the Initial Setup User are described in *EMC Unisphere for VMAX Installation Guide* and *EMC Unisphere for VMAX* online help.

User roles

Unisphere includes the following user roles:

- **None** - Provides no permissions.
- **Monitor** - Performs read-only (passive) operations on an array excluding the ability to read the audit log or access control definitions.
- **StorageAdmin** - Performs all management (active or control) operations on an array in addition to all Monitor operations. This role does not allow users to perform security operations.

- **Administrator** - Performs all operations on an array, including security operations in addition to all StorageAdmin and Monitor operations.
- **SecurityAdmin** - Performs security operations on an array in addition to all Monitor operations.
- **Auditor** - Grants the ability to view, but not modify, security settings for an array (including reading the audit log, symacl list, and symauth) in addition to all Monitor operations. This is the minimum role required to view the audit log.
- **Perf Monitor** - Performs the same operations as a monitor, with the addition of being able to set performance alerts and thresholds.
- **Initial Setup User** - Defined during installation, this temporary role provides administrator-like permissions for the purpose of adding local users and roles to Unisphere. For more information on the Initial Setup User, see the online help.

Individual and group roles

Users access an array or component directly through a role assignment and/or indirectly through membership in a user group that has a role assignment.

User groups enable administrators to assign roles to multiple users simultaneously. User groups are created on the SMAS server according to its operating system and assigned roles with Unisphere.

If a user has two different role assignments (one as an individual and one as a member of a group), the permissions assigned to the user will be combined.

For example, if a user is assigned a Monitor role and a StorageAdmin role through a group, the user will be granted Monitor and StorageAdmin rights.

User IDs

The following section describes the SYMAPI format to create users and roles.

Note: This format displays in the footer bar of the Unisphere GUI, but not in the User/Role list view or creation wizard.

Users and user groups are mapped to their respective roles by IDs. These IDs consist of a three-part string in the form:

```
Type:Domain\Name
```

In the event that a user is matched by more than one mapping, the user authorization mechanism uses the more specific mapping:

- If an exact match (e.g., D:sales\putman) is found, that is used.
- If a partial match (e.g., D:*\putman) is found, that is used.
- If an unqualified match (e.g., putman) is found, that is used.
- Otherwise, the user is assigned a role of None.

Valid values for `Type`, `Domain`, and `Name` are as follows:

`Type`

Type of security authority used to authenticate the user or group.

Possible types are:

`L`

A user or group authenticated by LDAP. In this case, *`Domain`* specifies the fully qualified name of the domain controller on the LDAP server.

For example:

`L:danube.com\Finance`

indicates that user group Finance will log in through domain controller danube.com.

Once configured, individual LDAP users and groups can log in to Unisphere using a simple username, or simple group name, respectively.

For example, Finance.

`C`

A user or group authenticated by the SMAS server.

For example:

`C:Boston\Legal`

indicates that user group Legal will log in through Unisphere sever Boston.

`H`

A user or group authenticated by logging into a local account on a Windows host. In this case, `Domain` specifies the hostname.

For example:

`H:jupiter\mason`

indicates that user mason will log in on host jupiter.

`D`

A user or group authenticated by a Windows domain. In this case, `Domain` specifies either the simple domain name (for individual users) or the fully qualified domain name (for groups).

For example:

`D:sales\putman`

indicates user putman will log in through Windows domain sales.

Once configured, individual Windows domain users can log in to Unisphere using a simple username.

For example, putman.

Group Windows domain users can log in to Unisphere using either a simple domain name\group name or a fully qualified domain name\group name.

`V`

A user or group authenticated by a virtualization domain. In this case, `Domain` specifies the virtualization domain name.

`Domain`

Within role definitions, IDs can be either fully qualified (as above), partially qualified, or unqualified.

When the Domain portion of the ID string is an asterisk (*), the asterisk is treated as a wildcard, meaning any host or domain.

Note: When configuring group access, the `Domain` portion of the ID must be fully qualified.

For example:

`D:ENG\jones`	Fully qualified path with a domain and username (for individual domain users).
`D:ENG.xyz.com\ExampleGroup`	Fully qualified domain name and group name (for domain groups).

	`D:*\jones`	Partially qualified that matches username jones with any domain.
	`H:HOST\jones`	Fully qualified path with a hostname and username.
	`H:*\jones`	Partially qualified that matches username jones within any host.
	`jones`	Unqualified username that matches any jones in any domain on any host.
`Name`	Specifies the username relative to that authority. It cannot be longer than 32 characters and spaces are allowed if delimited with quotes. Usernames can be for individual users or user groups.	

About user authorization

User authorization restricts the management operations users can perform on an array.

By default, authorization is enforced within Unisphere against the respective authorization rules database of a given array. This enforcement is done regardless of the authorization control setting (Enabled/Disabled) for that array. SYMCLI uses this authorization control state to determine enforcement of rules. Unisphere always behaves as if symauth is enabled (exception is the Unisphere Initial Setup User).

An Administrator or SecurityAdmin user can map individual users or groups of users to specific user roles which determine the operations the users can perform.

The authorizations on an array determine the privileges the Initial Setup User has on the array. The following section describes the relationship between the Initial Setup User and authorizations:

- If authorization is enabled, authorization rules are always enforced. The Initial Setup User could be locked out if no authorization rule exists for the user.
- If authorization is disabled and there are no authorization rules on the array, the Initial Setup User is granted Admin privileges.
- If authorization is disabled and there are no Admin or Security authorization rules on the array, the Initial Setup User is granted Admin privileges. All other rules are enforced as defined.
- When authorization is disabled and Admin or Security Admin authorization rules are defined on the array, if the Initial Setup User does NOT have an auth rule explicitly defined, the initial setup user will have NO permissions. All other rules are enforced as defined.

Assigning user authorization

Before you can use the Unisphere REST API, you must assign user authorization for each VMAX array the user is permitted to access. Use the following procedure to assign user authorization for arrays:

1. Log into Unisphere.
2. At the bottom of the Common Tasks panel click Administration.
3. Click Users and Roles to open the Users and Roles list view.

4. Create a user login profile for each array to be accessed by the user, and assign them to any of the following roles:
   - Monitor
   - StorageAdmin
   - Administrator
   - SecurityAdmin

Note: These user roles are valid for the currently available REST resource methods (GET, POST, and DELETE). When they become available, only Admin and Storage Admin roles will be able to initiate PUT methods.

Unisphere 1.6 multiple authorization roles

Starting in Unisphere for VMAX 1.6, a user or group can be assigned up to 4 authorization roles.

To add a user or group with multiple roles:

1. Navigate to the Add Authorization page:

   All -> Home -> Authorized Users & Groups

2. In the General tab, specify user or group name and type (and, optionally, authority and/or domain).
3. Click Roles tab.
4. Select an ID or DB Classify application.
5. Select up to 4 entries in the Roles list:
   - Admin
   - SecurityAdmin
   - StorageAdmin
   - Auditor
   - PerfMonitor
   - Monitor
   - None

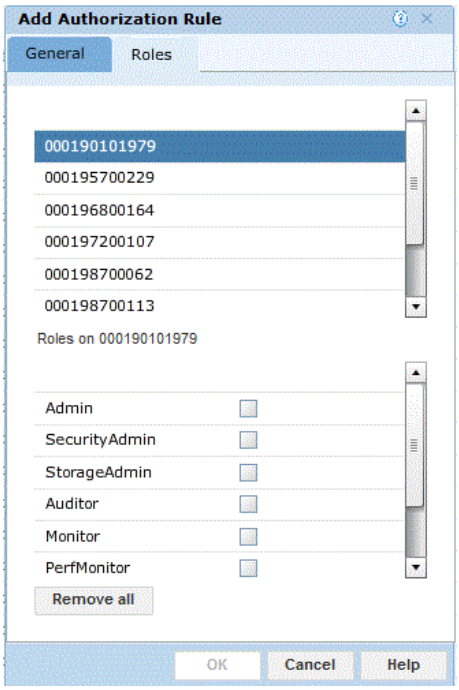


Figure 3 Unisphere for VMAX - Add Authorization Rule

When at least the first role is selected for one object, the OK button activates.

6. Optionally, select another object and specify roles for the second object.
7. Click OK.

Backward compatibility to Unisphere 1.5

Unisphere 1.5 or earlier supports only one role per user or group. To make your Unisphere compatible with Unisphere version 1.5 or earlier, create at least one authorization rule that corresponds to the 1.5 roles of Admin or SecurityAdmin.

This ensures that older Unisphere versions can interpret at least one rule.

Using the encrypted lockbox

Unisphere uses the Common Security Toolkit Standalone Lockbox (lockbox) to store and protect sensitive information.

The lockbox is first created during installation. During installation, you can use either the default password, or a password you define.

⚠WARNING

Loss of this password can lead to situations where the data stored in the lockbox is unrecoverable.

The default password is generated and stored in the lockbox with the Stable System Values (SSVs). The SSVs uniquely identify the host. These values are used to validate access to the lockbox from Unisphere authentication and local user management calls.

When the Unisphere for VMAX is upgraded, product information in the existing lockbox is automatically copied into the new lockbox when the lockbox is first accessed.

SSVs are platform-dependent, thus changes to hardware or software on a host may require a reset of the SSVs stored in the lockbox. You must update the SSVs in the lockbox whenever the host SSVs no longer match the values in the lockbox, including when:

- The host is upgraded,
- The lockbox file is moved to another host.

The lockbox includes a CLI utility to reset the host system SSVs.

Resetting the host system SSVs

This section describes the steps to reset the host system SSVs using the CLI utility.

To reset the lockbox used by Unisphere for VMAX:

1. Start the SMAS service.

   The steps to start and stop the server are described in *EMC Unisphere for VMAX Installation Guide*.

2. Find the CST_PASSPHRASE used on install.
3. Change directory location to:

   Windows: install_location\jboss\bin

   Linux: install_location/jboss/bin

4. Type the following command:

   Windows: service.bat updatessv CST_PASSPHRASE

   Linux: ./initcst.sh updatessv CST_PASSPHRASE

5. Restart SMAS service.

Replacing the Unisphere for VMAX server certificate

At installation, the installer generates and installs the self-signed server certificate used for HTTPS transport-level security.

This section describes the steps to replace this certificate with the one issued by a trusted third-party.

Before you begin

You will need the keystore password to complete the following procedure. The keystore password is generated during installation. It is stored in the following file:

‹SMAS installation›/jboss/domain/configuration/domain.xml.init

where ‹SMAS installation› is the directory where SMAS is installed.

Open the file and search for "ssl key-alias="tomcat" password=".

Customers must generate new JKS key/trust store file with the server certificate alias "tomcat" and key/store password as described in above. The key/trust store must contain all CA certificates needed for full certificate trust chain verification.

Step 1: Generate a certificate request.

a. Type the following commands where `<SMAS installation>` is the directory where SMAS is installed:

   On **Windows** systems:

```
cd <SMAS installation>\jboss\standalone\configuration

<SMAS installation>\jre\bin\keytool -certreq -alias tomcat -file
tomcatcert.csr -keystore keystore
```

   On **Linux** systems:

```
cd <SMAS installation>/jboss/standalone/configuration

<SMAS installation>/jre/bin/keytool -certreq -alias tomcat -file
tomcatcert.csr -keystore keystore
```

   A prompt to enter the keystore password appears. This is the password described in "Before you begin".

b. Type the password and press ENTER.

   A file named tomcatcert.csr is generated. This file is a certificate request.

   The next step varies depending on whether the following error message appears:

```
"Failed to establish chain from reply"
```

   – If the error message appears, proceed to Step c.

   – If the error message does not appear, skip to Step d.

c. The error appeared because your CA is not in the keystore's default trust chain (the keystore comes with a default set of trusted CAs). You must import a trusted certificate into your keystore to serve as the root for the trust chain.

   To import a trusted certificate into your keystore, type the following commands where `<SMAS installation>` is the directory where SMAS is installed and `<Trusted CA cert file>` is the signed certificate you received from your CA:

   ⚠CAUTION

   Be very careful about importing a new trusted certificate.

   On **Windows** systems:

```
cd <SMAS installation>\jboss\standalone\configuration

<SMAS installation>\jre\bin\keytool -import -alias root -file
<Trusted CA cert file> -keystore keystore -trustcacerts
```

   On **Linux** systems:

```
cd <SMAS installation>/jboss/standalone/configuration

<SMAS installation>/jre/bin/keytool -import -alias root -file
<Trusted CA cert file> -keystore keystore -trustcacerts
```

Skip to "Step 3: Start the SMAS server".

d. Send the certificate request to your Certificate Authority (CA).

The CA will validate the request and provide you with a signed certificate.

Step 2: Import the CA-signed certificate into the keystore.

a. Stop the SMAS server.

b. Type the following commands where `<SMAS installation>` is the directory where SMAS is installed and `<signed certificate file>` is the signed certificate you received from your CA:

On **Windows** systems:

```
cd <SMAS installation>\jboss\standalone\configuration

<SMAS installation>\jre\bin\keytool -import -alias tomcat -file
<signed certificate file> -keystore keystore -trustcacerts
```

On **Linux** systems:

```
cd <SMAS installation>/jboss/standalone/configuration

<SMAS installation>/jre/bin/keytool -import -alias tomcat -file
<<signed certificate file>> -keystore keystore -trustcacerts
```

A prompt to enter the keystore password appears. This is the password described in "Before you begin".

c. Type the password and press ENTER.

Step 3: Start the SMAS server

The steps to start and stop the server are described in *EMC Unisphere for VMAX Installation Guide*.

Other security settings

This section describes other security-related topics applicable to Unisphere for VMAX, including:

- "Port usage" on page 82
- "Link-and-launch security" on page 82
- "Unisphere data security" on page 83
- "Security alert system" on page 83
- "Session timeout" on page 83
- "Root access requirements" on page 83

Port usage

Unisphere components use the following ports:

Table 18 Unisphere port usage

Component	Port
https	8443
vApp Manager	5480
CLI	9999 (not available on network)
Remoting	4447
postgresql	3324

Link-and-launch security

Link-and-launch clients connect to Unisphere only using HTTPS. The client and Unisphere are required to establish mutual trust. That is, the client side trusts that the server is authentic.

The Link-and-launch client (acting as SSL client) must establish trust either by:

- Explicitly importing Unisphere self-signed certificate into the client's trust store, or
- Implicitly, if the Unisphere self-signed certificate (generated during installation) is replaced with a certificate issued by a mutually-trusted CA (a CA trusted by both Unisphere and the Link-and-Launch client).

Unisphere's trust with the client's launching application is established by explicit registration (by Admin/SecurityAdmin) of the Link-and-Launch client's ID.

The client must provide a valid username of the Unisphere user in whose context the Link-and-Launch is performed. Once trust is established, a one time password (token) is issued to trusted Link and Launch clients. The tokens are then exchanged as a means to single sign on into Unisphere.

Username format is documented in "User IDs" on page 74.

Note: Unisphere supports Link-and-Launch ONLY in the context of the users with Admin, StorageAdmin, or Monitor roles.

When the transport is fully secured (by mutual trust establishment), and the user is validated (during initial registration connection), Unisphere issues the client a one-time password (OTP).

In the following request, the client exchanges the OTP for a launch token. The exchange must take place within OTP's time-to-live of 10 minutes, otherwise the process (of OTP acquisition and OTP-to-token exchange) must be started anew.

The token is valid only for a single launch-and-link until Unisphere server reboots.

Unisphere data security

You can export and import some Unisphere configuration settings. This feature allows you to configure multiple Unisphere installations more easily.

Exported settings are protected with a customer-defined one-time password.

The password must be communicated out-of-band by means the customer deems necessary.

Security alert system

Administrator or StorageAdmin users can configure Unisphere to deliver alert notifications for SNMP, e-mail, and Syslog.

The steps to configure alerts, manage alert thresholds, and view alert-related information are described in *EMC Unisphere for VMAX Installation Guide* and *EMC Unisphere for VMAX* online help.

Session timeout

Unisphere sessions timeout after 8 hours of user inactivity.

The timeout interval is not configurable.

When timeouts occur, the user is logged out, but the user account is not locked.

Root access requirements

Unisphere requires Root/Administrator access privileges for installation, deployment, and operations.

CHAPTER 5
vApp Manager security configuration tasks

EMC's Virtual Appliance Manager (vApp Manager) for Solutions Enabler is a web-based array management application deployed on a virtual machine. Once configured, vApp Manager discovers attached arrays, runs some system operations, and monitors arrays using log, data, and debug files.

This chapter describes security tasks related to vApp Manager, including:

- Secure deployment settings 86
- User-based access control 86
- Component access control 87
- Log files and settings 87
- Port usage 88
- Manage SSL certificates 88
- Secure serviceability 89
- Alerts 89
- Managing Clam anti-virus 90
- Maintenance 91

Security controls map

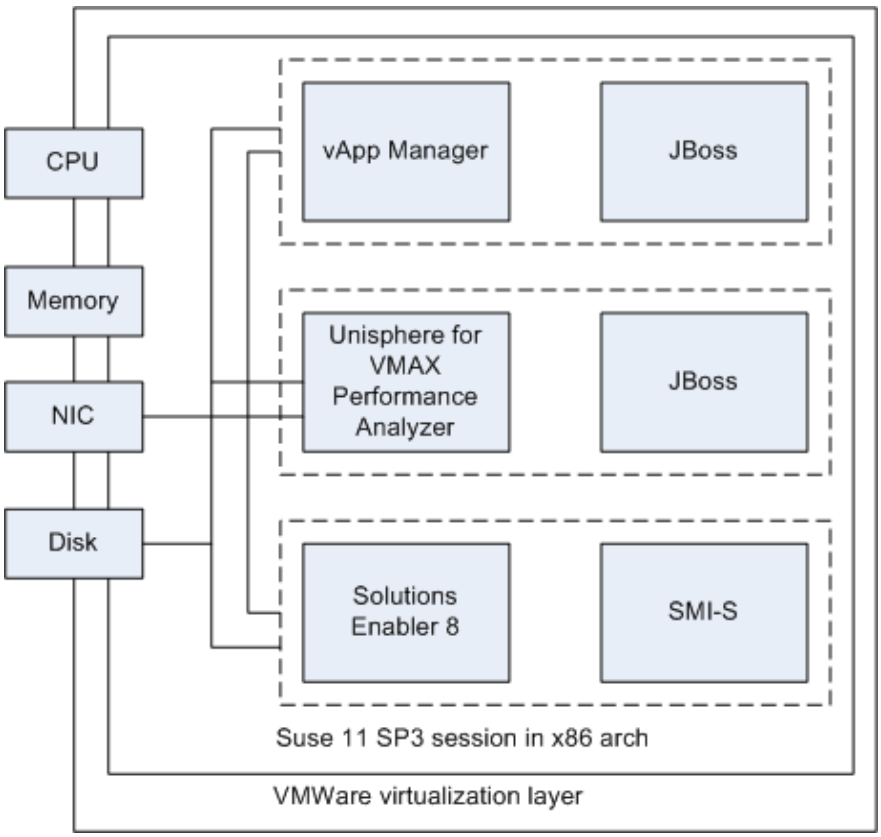


Figure 4 vApp Manager managed objects

Secure deployment settings

vApp is deployed as a single OVA in a standard ESX appliance. vApp Manager is a web-based application accessed via secure https layer.

vApp can only be accessed via vApp Manager. For example:

https://hostname:5480

No additional security deployment settings are required.

User-based access control

This section describes user accounts, and user authentication and authorization.

User authentication

vApp Manager provides two types of user authentication:

- Local directory authentication (username and password) using the Common Security Toolkit (CST).
- Lightweight Directory Access Protocol (LDAP) authentication.

vApp Manager for Solutions Enabler online help describes the steps to manage user authentication, including:

- Configure LDAP
- Change the LDAP configuration
- Import certificates
- Add user accounts
- Remove user accounts
- Change user passwords

Default accounts

vApp Manager has one or two default accounts.

- The first account is created at installation with username/password seconfig/seconfig.

  You are prompted to change the password for this default account at first login.

  You can change the password for this default account at any time.
- The second account is created when SSH is enabled using vApp Manager's online help with username/password cseadmin/cseadmin.

  Use this account to access vApp using SSH.

You can add new local users or map existing LDAP users.

All new users, whether added directly to vApp Manager or mapped using LDAP have admin role and privileges that allows access to all screens and options in the vApp Manager GUI.

User actions without authentication

VM console

You can access the VM console via the ESX server. Only the following activities are supported using ESX server access:

- Network configuration
- Upgrade
- Setting timezones

SSH

You can enable/disable the appliance SSH port in the vApp Manager.

Enable the SSH port for an SSH session to allow troubleshooting the appliance or storage system. The default state of the SSH port is disabled.

⚠CAUTION

Troubleshooting the appliance or storage system should only be done under the direction of EMC Customer Support.

User authorization

vApp Manager authorizes users in an LDAP group with an admin role.

LDAP admin users can be either a "user" or "group" type. All users belonging to an LDAP group can perform all vApp operations.

Component access control

vApp is a tightly architected with access only through vApp Manager.

No components can be individually managed.

Log files and settings

You can use vApp Manager to download the following log files:

- daemon log files, including:
  - storapid
  - storgnsd
  - storrdfd
  - storevntd
  - storsrmd
  - storwatchd
  - storstpd
  - storsrvd

- ecom
- univmaxpa

◆ appliance (vApp Manager) log files

vApp Manager for Solutions Enabler online help describes the steps to download these log files.

Log file management

Logging levels, log file retention, and synchronization between the log files and the ESX timer are not configurable.

Log file entries cannot be streamed to an external log service (syslog).

If the disk space utilized by log files reaches 80% capacity, an alert is generated. This threshold is not configurable.

Port usage

vApp Manager uses the ports listed in Table 19. All other ports are blocked.

Table 19 Network ports used in vApp

Component	Protocol	Port	Description
vApp Manager	TCP	5480	Port where the vApp JBoss web server listens for vApp manager requests.
Unisphere for VMAX	TCP	8443	Standard EMC Unisphere for VMAX listening port.
Postgres Database	TCP	3324	Used by Unisphere.
SSH	TCP	22	SSH port. This port can be enabled/disabled using vApp Manager. Default: disabled.
Solutions enabler as client server	TCP	2707	Standard EMC SE server port.
SMI	TCP	5988, 5989	Standard EMC SMI port.
vApp Manager	TCP	8080	Listening port for uploading certificates and licenses to Unisphere for VMAX over HTTP.
vApp Manager	TCP	7070	Standard JBoss interface for management of the vApp.

Manage SSL certificates

vApp Manager allows an alternate (custom) SSL certificate to be imported and used for the storsrvd daemon.

The certificate is used when stordaemon command requests are made from a remote client. Certificates can be self-signed or CA-signed.

To import an alternate certificate for the storsrvd daemon requires the following files:

- Private key file
- Replacement certificate file
- Trust certificate file

These files must be in a .pem format. For example:

customer_key.pem.

The common name (CN) of the certificate must include storsrvd followed by a space, and the fully qualified name of the host where the certificate will be installed. For example:

storsrvd my.host.com.

SSL certificates for vApp Manager can not be modified.

vApp Manager for Solutions Enabler online help describes the steps to create and update SSL certificates.

Data security settings

vApp Manager persistent data files include the following appliance configuration files:

- Daemon Option file
- Option file
- Network configuration file
- symapi.db file
- daemon specific files.

You can download these persistent files using vApp manager.

Downloaded data files are saved to a .zip file, (containing a .gpg file). This data is fully encrypted.

The encryption key is not configurable and cannot be modified.

Secure serviceability

There is no special login to vApp Manager for service personnel.

Service personnel can use the root password (not shared with customers) to access the system for troubleshooting via SSH console session.

Security patches and other updates are applied using a wholesale ISO upgrade. A new ISO image is mounted and the upgrade is launched from the VM console.

Alerts

vApp Manager has two alerts:

- virus update alert - issued when an update for ClamAV (an anti-virus package that detects viruses, trojans, malware, and other malicious threats) is available.

- log file usage alert - issued when a log file reaches 80% of available capacity.

Managing Clam anti-virus

vApp Manager includes Clam Anti-Virus (AV). ClamAV provides anti-virus protection designed to detect viruses, trojans, malware, and other malicious threats on the appliance virtual machine.

ClamAV supports on-demand scanning, anti-virus updates, scan log files, and editing the ClamAV configuration file.

On-demand scanning

You can run Clam AV scans on demand.

Note: A pre-configured nightly scan runs between 12am and 1am local time. The nightly scan cannot be canceled and the run time cannot be changed.

To start an on-demand virus scan:

1. Select Clam Anti-virus.
2. In the Operations panel, click Scan Now.

   Scan progress displays in the Output panel.

To stop an on-demand virus scan:

1. Select Clam Anti-virus.
2. In the Operations panel, click Cancel Scan.
3. In theScan Canceled dialog, click Close.

   The scan stops and "Scan Complete" displays in the Output panel.

Download scan log files

Clam AV log files are saved on the appliance in a zip file. You can download the zip file to a local machine. The zip file contains:

- freshclam.log — The Clam Anti-virus definition update log.
- clamscan.log — The virus scan report.

To download the log files:

1. Select Clam Anti-virus.
2. In the Operations panel, click Download logs.
3. In the Confirm Download dialog, click Yes to download the zipped log files.
4. From the file browser screen, navigate to desired location to save the .zip file and click Save.

Edit the ClamAV configuration file

The freshclam.conf file contains parameters for updating the database virus definitions, and configure the freshclam.log file output. The configuration parameters can be changed.

To edit the freshclam.conf file:

1. Select Clam Anti-virus.
2. In the Operations panel, click Edit freshclam.conf.

   The Edit freshclam.conf file dialog is displayed.
3. Make changes to the file, and then click Save.

Updating the Clam Anti-virus

To update Clam Anti-virus:

1. Select Clam Anti-virus.
2. In the Operations panel, click Update Clam Anti-Virus.

   The appliance Clam Anti-virus database is checked against the latest database from the Clam AV web site.

   If the appliance database is out of date, the update begins. Update progress is displayed in the Output panel.

Maintenance

Updates to vApp Manager are installed using a full ISO upgrade.

Patching is not supported.

CHAPTER 6
SMI-S security configuration tasks

SMI-S uses the EMC Common Object Manager (ECOM) Toolkit to implement security at a variety of levels. ECOM uses SSL 3.0 and TLS 1.0 protocols to secure and protect network requests, responses, and indication deliveries. Refer to Refer to *EMC Common Object Manager (ECOM) Toolkit Deployment and Configuration Guide* for information about:

- ECOM port security
- Securing ECOM communication

This chapter describes other SMI-S security tasks, including:

- User-based access control 94
- Component access control 97
- Log files and settings 97
- Port usage 97
- Network encryption 97
- VMAX3, SMI-S Group Replication and Solutions Enabler GNS Global Mode 98
- Securely deploying SMI-S 99
- Manage the encrypted lockbox 99
- Other security settings 100

Security controls map

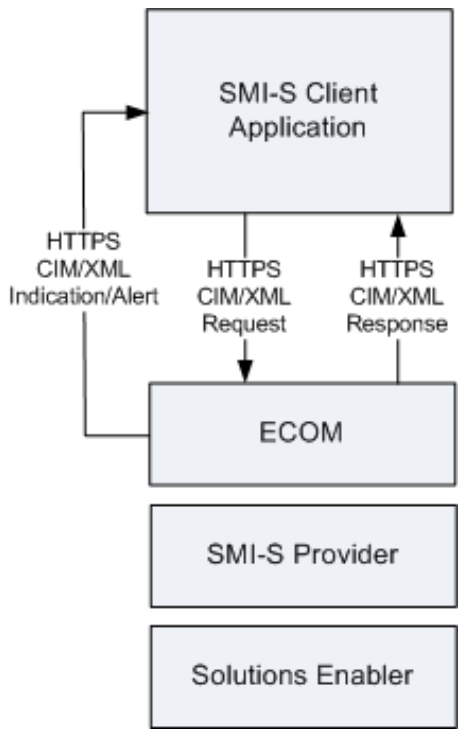


Figure 5 SMI-S managed objects

User-based access control

This section describes the following topics:

- "User authorization"
- "User authentication"
- "Administrator user account"

User authorization

User access control to the SMI provider is provided by ECOM authorization and security toolkit.

User authentication

ECOM supports three types of authorities: LocalDirectory (default), LDAP, and OSLogin. These authorities grant the user access.

To authenticate, ECOM requires user information following one of these two formats along with the user password:

```
user information := [ authority '/' ] [ domain '\' ] < username >
```

or

```
user information := [ domain '\' ] < username > [ '@' authority ]
```

If the authority recognizes the user, the authentication succeeds and ECOM returns a valid security token.

Configure authentication

The default authority is LocalDirectory. LocalDirectory is if the authority information is not informed by the user.

You can specify the Local Directory Authority as any substring from the Local Directory name as defined in Config.xml configuration file (default is LocalDirectoryTest). For example:

```
admin

LocalDir/admin
LocalDirectory/admin
LocalDirectoryTest/admin

admin@LocalDir
admin@LocalDirectory
admin@LocalDirectoryTest
```

LDAP servers can also be used as the authority to authenticate a user. For example:

```
PSO-AD-Authority/admin
PSO-SunOneAuthority/lennon

admin@PSO-AD-Authority
lennon@PSO-SunOneAuthority
```

Windows users can also be authenticated by the OSLogin authority.

The string "OSLogin" is used as the authority name in order to authenticate OS users.

Both local and domain users can be authenticated:

- If no domain is specified, the user is treated as a "local user" (default).
- If the domain is explicitly specified, the user is treated as a "domain user".

Both the fully-qualified domain name (FQDN) and the domain name can be used during authentication. The user-supplied domain entry will be converted into the FQDN.

For example:

```
OSLogin/Administrator
Administrator@OSLogin

OSLogin/CORP\mccartney
CORP\mccartney@OSLogin

OSLogin/corp.localdomain\ringo
corp.localdomain\ringo@OSLogin
```

Administrator user account

ECOM requires a user account under LocalDirectory authority named administrator.

This section describes the commands to create the administrator role, create a user, and assign the user to the role.

Create a cstadmin role

Use the `cstadmin create-role` command to create a new role.

The syntax for the `cstadmin create-role` command:

```
cstadmin create-role <role>
     -app=<app>
     -cstdir=<directory>
     -description description
     -passphrase=<passphrase>
```

- *role* (mandatory) - Name of the role to create.
- **-app=**‹*App*› (optional) - Name of the application bootstrap file.
- **-cstdir=**‹*directory*› (optional) - Path to the CST configuration directory.
- **-description** *description* (optional) - Description for the role.
- **-threshold** (optional) - Sets the lockbox SSV threshold.
- **-passphrase=**‹*passphrase*› (optional) - Passphrase for the lockbox.

For example:

```
$ cstadmin create-role administrator -cstdir=.
Enter lockbox passphrase:
Confirm passphrase:
cstadmin: Role administrator created in role database RoleManagement.
```

Create a cstadmin user

Use the `cstadmin create-user` command to create a local directory user account.

The syntax for the `cstadmin create-user` command:

```
cstadmin create-user <account>
     -app=<app>
     -cstdir=<directory>
     -description description
     -passphrase=<passphrase>
     -password=<Initial password>
```

- *account* (mandatory) - Name of the local directory account to create.
- **-app=**‹*App*› (optional) - Name of the application bootstrap file.
- **--cstdir=**‹*directory*› (optional) - Path to the CST configuration directory.
- **-description** *description* (optional) - Description for the user.
- **-passphrase=**‹*passphrase*› (optional) - Passphrase for the lockbox.
- **-password=***Initial password*› (optional) - Initial password for the account.

For example:

```
$ cstadmin create-user lennon -cstdir=c:/cst/lockbox
Enter new user's password:
Confirm passphrase:
Enter lockbox passphrase
cstadmin: User lennon created with account manager LocalDirectoryTest.
```

Create a role mapping

Use the `cstadmin add-rolemember` command to add an identity to a role.

The syntax for the `cstadmin add-rolemember` command:

```
cstadmin add-rolemember <authority type>
     <authority type>
     <authority name>
     <account name>
     <role name>
     -app=<app>
     -cstdir=<directory>
     -group
     -passphrase=<passphrase>
```

- *authority type* - Type of authority.
- *authority name* - Name of authority.
- *account name* - The account name to add.
- *role name* - Role name to add.
- **-app=**‹*App*› (optional) - Name of the application bootstrap file.
- **-cstdir=**‹*directory*› (optional) - Path to the CST configuration directory.
- **-passphrase=**‹*passphrase*› (optional) - Passphrase for the lockbox.

For example:

```
$ cstadmin add-rolemember LocalDirectory LocalDirectoryTest lennon
   administrator -cstdir=c:/cst/lockbox
Enter lockbox passphrase
cstadmin: Role administrator added to lennon from account manager
   LocalDirectoryTest.
```

Component access control

Access control for SMI-provider components is provided by EMC Common Object Manager (ECOM).

EMC Common Object Manager (ECOM) Toolkit Deployment and Configuration Guide describes the steps to complete this task.

Log files and settings

if `SecurityLoggingEnabled` is set to true in the Security_settings.xml configuration file (located at ‹ECOM_install_dir›/conf/), ECOM logs security-related information to the file securitylog.txt.

Whether security logging is enabled or not, security-related information is always logged to the file cimomlog.txt.

cimomlog.txt and securitylog.txt are located at:

‹ECOM_install_dir›/log/

Displaying log files

Use the ECOM web server to administer logs and security. The server can be accessed from:

https://‹ManagementIPAddress›:‹port›/ecomconfig

where ‹port› is a secure port as defined in Port_settings.xml.

EMC Common Object Manager (ECOM) Toolkit Deployment and Configuration Guide describes the steps to complete this task.

Port usage

Table 20 Ports used by SMI-S

Component	Service	Protocol	Port	Description
CIMXMLAdapter	ECOM	CIM/XML	5989	Secure HTTPS CIM/XML
WSManProtocolAdapte	ECOM	WS-MAN	5986	Secure HTTPS WS-MAN
EDAAAdapter	ECOM	Rest	5989	Secure HTTPS EDAA Rest

Network encryption

BSAFE library is included in all ECOM distributions to support SSL.

ECOM's secure communication capabilities are configured in the file Security_settings.xml located at ‹ECOM_install_dir›/conf/).

The relevant parameter settings in the file are:

- CertificatesDirectory - The relative path to ECOM SSL certificates directory from ‹ECOM_install_dir›.

  Default: conf/ssl

- SSLCertFile - SSL certificate file name in CertificatesDirectory.

  Default: ecomtls.crt

- SSLKeyFile - SSL private key file name in CertificatesDirectory.

  Default: ecomtls.pk

- SSLCAFile - CA file name in CertificatesDirectory, needed if SSLClientAuthentication is enabled.

  Default: ecomtls.ca

- SSLClientAuthentication - Option that controls if the client SSL certificate should be verified or not.
- SSLProtocol - Option that controls the method functions used to specify the various protocols supported by TLS and SSL connections for both the client and the server.
- SSLCipherSuite - Option that controls the supported cipher suites of the SSL connection.

VMAX3, SMI-S Group Replication and Solutions Enabler GNS Global Mode

The EMC SMI-S Provider supports the SNIA SMI-S Replication Service profile. The Replication Services profile offers client applications the ability to manage replication using groups, which is also known as Group Replication. The Solutions Enabler global name service (GNS) can be started in Global Mode which will store the replication group information into the VMAX3 system. The advantage to storing replication group information into the VMAX3 system is that it will centralize the group data and make it accessible to different hosts/servers accessing the same VMAX3 system.

The default installation of Solutions Enabler with SMI-S will have the default GNS in Local Mode which stores the replication group information onto the host which is running the Solutions Enabler SMI-S service. To enable Global Mode, the following steps are required. These steps must be completed before any replication group operations are initiated.

1. Shut down ECOM service.
2. Shut down Solutions Enabler daemons.
3. In the `SYMAPI/config/options` file add/enable this setting:
   `SYMAPI_USE_GNS = ENABLE`
4. Start ECOM service. ECOM service will automatically start the Solutions Enabler daemons.

Securely deploying SMI-S

To enable authentication for:

- CIM requests - set the configuration parameter CIMRequest_AuthenticationEnabled to true
- non CIM requests - set NonCIMRequest_AuthenticationEnabled.

Manage the encrypted lockbox

SMI-S uses an encrypted lockbox to store and protect sensitive information.

The lockbox must be initialized with a user account created and mapped to the administrator role.

The lockbox must be located at ECOM_install_dir›/conf/cst/

Create the CST lockbox

Use the `cstadmin initialize` command to create the lockbox in the specified directory.

The command creates a new lockbox in the specified directory used to store keys, signed configuration files and signatures.

The syntax for the `cstadmin initialize` command:

```
cstadmin initialize <directory>
     -attended
     -overwrite
     -set-lockbox-policy
     -threshold
     -two-factor
```

- *directory* (mandatory) - Path to CST configuration directory. Contains CST configuration files. The lockbox will be created in this directory.
- **-attended** (optional) - Attended lockbox.
- **-overwrite** (optional) - Overwrites existing lockbox.
- **-set-lockbox-policy** (optional) - Sets lockbox passphrase policy.
- **-threshold** (optional) - Sets the lockbox SSV threshold.
- **-two-factor** (optional) - Two factor lockbox.

For example:

```
$ cstadmin initialize c:/cst/lockbox
Enter lockbox passphrase:
Confirm passphrase:
cstadmin: Lockbox c:\cst\lockbox\csp.clb initialized.
```

Other security settings

Security alerts

SMI Provider manages alerts as follows:

- SMI Provider registers to receive all Solutions Enabler storage-related events from Solutions Enabler.
- SMI Provider converts the storage-related events to indication objects.
- The indication objects are sent to ECOM indication handler, which then
- Delivers the objects to listening client applications.

CHAPTER 7
Embedded NAS

Embedded NAS (eNAS) uses the lightweight hypervisor provided in HYPERMAX OS to create and run a set of virtual machines on VMAX3 controllers. These virtual machines host two major elements of eNAS: software data movers and control stations. These virtual machines are distributed based on the mirrored pair architecture of VMAX3 to evenly consume VMAX3 resources for both performance and capacity. All VMAX3 block and file resources are managed through the intuitive, easy to use Unisphere management interface.

eNAS extends the value of VMAX3 to file storage by enabling customers to leverage vital enterprise features including SLO-based provisioning, Host I/O Limits, and FAST technologies for both block and file storage.

The eNAS guest runs in a virtual environment created by a “container”. Containers identify the resources (memory, ports, and LUNs) used by their guest. When a guest is created, HYPERMAX OS assigns an internal IP address that is not exposed to the customer network. MAC Address filtering prevents unauthorized access between guests on the array's internal network.

Security controls map

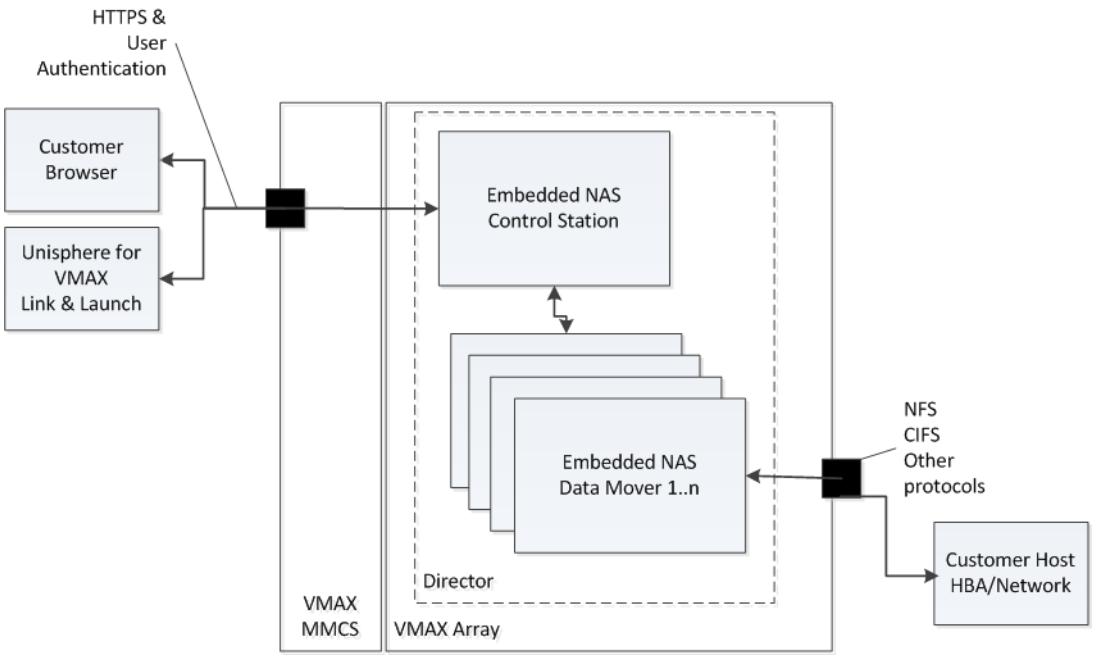


Figure 6 Embedded NAS managed objects

The security features and tasks the eNAS guest running on the VMAX array are the same as those for the VNX series.

- *EMC VNX Series Security Guide for VNX* provides information on the following security-related topics:

- Access control
- Logging
- Communication security
- Data security settings
- Security maintenance
- Advanced management

◆ *EMC VNX Series Command Line Interface Reference for File* provides information the CLI commands to manage access control, certificates, LDAP configuration, and other security-related activities.

Note: Customers are responsible for securing their eNAS/VNX deployment. Pre-configured settings may not be sufficiently secure for their needs.