

**EMC Solutions Enabler
Symmetrix Device Masking CLI**
Version 6.0

PRODUCT GUIDE
P/N 300-000-875
REV A06

EMC Corporation
Corporate Headquarters:
Hopkinton, MA 01748-9103
1-508-435-1000
www.emc.com

Copyright © 2002, 2003, 2004, 2005 EMC Corporation. All Rights Reserved.

Printed January, 2005

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, replication, or distribution of any EMC software described in this publication requires an applicable software license.

Trademark Information

EMC², EMC, Symmetrix, Celerra, CLARiiON, CLARAlert, Documentum, HighRoad, Legato, Navisphere, PowerPath, ResourcePak, SnapView/IP, SRDF, TimeFinder, VisualSAN, and where information lives are registered trademarks and EMC Automated Networked Storage, EMC ControlCenter, EMC Developers Program, EMC OnCourse, EMC Proven, EMC Snap, Access Logix, AutoAdvice, Automated Resource Manager, AutoSwap, AVALONidm, C-Clip, Celerra Replicator, Centera, CentraStar, CLARevent, Connectrix, CopyCross, CopyPoint, DatabaseXtender, Direct Matrix, Direct Matrix Architecture, EDM, E-Lab, Enginuity, FarPoint, FLARE, GeoSpan, InfoMover, MirrorView, NetWin, OnAlert, OpenScale, Powerlink, PowerVolume, RepliCare, SafeLine, SAN Architect, SAN Copy, SAN Manager, SDMS, SnapSure, SnapView, StorageScope, SupportMate, SymmAPI, SymmEnabler, Symmetrix DMX, Universal Data Tone, and VisualSRM are trademarks of EMC Corporation. All other trademarks used herein are the property of their respective owners.

Preface	ix
----------------------	----

Chapter 1 Introduction

Device Masking Overview	1-2
How Symmetrix Device Masking Works	1-2
Host Access Example	1-3
Managing Access for Unsupported Host Platforms.....	1-4
Supported Topologies	1-5
Fibre Channel Topology.....	1-5
Native iSCSI Topology	1-6
Device Masking VCMDB Security Enhancement	1-7
Using Enginuity Syscalls	1-8
Device Masking Commands	1-9
Database Device Locking	1-9
Command Summary	1-10
Volume Logix Conversion.....	1-12

Chapter 2 iSCSI Setup

iSCSI CHAP Authentication: Enginuity Version 56xx	2-2
Requirements.....	2-2
Setting iSCSI Authentication via the SYMCLI	2-2
Showing Authentication Information.....	2-3
Restoring Authentication Data and Updating the iSCSI Driver.....	2-3
iSCSI Software Driver Configuration	2-4
Requirements.....	2-5
Installing the iSCSI Software Initiator	2-5
Configuring iSCSI with CHAP Authentication	2-6

Configuring iSCSI without CHAP Authentication	2-14
---	------

Chapter 3 **Device Access Management**

Initial Device Masking Setup	3-2
Access Control Environment Setup	3-2
Device Masking Configuration.....	3-3
Identify Configuration Components	3-3
Initialize and Update the Database.....	3-4
Enable Authentication	3-5
Recommendations for Activating the Configuration.....	3-5
Discovering Host HBAs.....	3-6
Using Alias Names.....	3-6
How to Add and Remove Masked Devices.....	3-8
Adding Devices	3-8
Removing Devices.....	3-9
Device Masking VCMDB Maintenance.....	3-10
Initializing the Database	3-10
Activating Configuration Changes	3-10
Viewing the Login History Table	3-11
Refreshing Director Profile Tables.....	3-11
Viewing the Database	3-11
Viewing Device Capacity	3-14
Managing a Backup VCMDB File	3-16
VCMDB Database Types	3-17
Converting a VCMDB Type	3-18
Restoring a Backup VCMDB.....	3-18
Restore a Backup and Convert its Type.....	3-18
Blocking Direct Writes to the VCMDB	3-19
HBA Initiator Management.....	3-20
Deleting HBA Associations.....	3-20
Fibre Channel-to-Host Interface Management.....	3-21
Locking Down a Fibre Channel ID	3-21
Setting Device LUN Visibility.....	3-24
Setting the LUN Base/Offset Skip Adjustment	3-25
Setting the Heterogeneous Host Configuration.....	3-26
 Index.....	 i-1

Figures

1-1	Device Masking Solution with WWN Initiators	1-3
1-2	Point-to-Point and Multi-Initiator Topologies	1-5
1-3	Native iSCSI Topology	1-6
1-4	Device Masking Syscalls	1-8
3-1	Device Masking Components	3-3

Tables

1-1	symmask Command Summary	1-10
1-2	symmaskdb Command Summary	1-11
1-3	Volume Logix to SYMCLI Conversion	1-12
3-1	Identifying Your Configuration	3-4
3-2	Initializing and Updating the Database	3-4
3-3	LUN Base/Offset Scenarios for Multiple Hosts with Skip Holes	3-26
3-4	Host Platforms and Interface Configuration Flags	3-27

As part of its effort to continuously improve and enhance the performance and capabilities of the EMC product line, EMC periodically releases new versions of both the EMC Enginuity Operating Environment and Solutions Enabler. Therefore, some functions described in this guide may not be supported by all versions of Enginuity or Solutions Enabler currently in use. For the most up-to-date information on product features, see your product release notes.

If a Solutions Enabler feature does not function properly or does not function as described in this guide, please contact the EMC Customer Support Center for assistance.

Audience This manual is intended for command-line users and script programmers interested in details about using the Device Masking SYMCLI commands.

Organization This manual describes how to assign and mask access privileges of hosts and adapters to Symmetrix directors and devices using the Device Masking SYMCLI commands of the EMC Solutions Enabler software. The following defines the structure of this manual:

Chapter 1, *Introduction*, highlights the major Symmetrix features and provides an overview of device masking.

Chapter 2, *iSCSI Setup*, describes how configure the iSCSI software driver and set CHAP authentication.

Chapter 3, *Device Access Management*, explains how to use the device masking commands to allow host access to Symmetrix devices.

Note: Detailed man page descriptions of all SYMCLI commands, environment variables, option file parameters, and error codes can now be found in the companion *EMC Solutions Enabler Symmetrix CLI Command Reference*.

Related Documentation

Other Symmetrix publications of related interest are:

- ◆ *EMC Solutions Enabler Symmetrix CLI Command Reference*, EMC Corporation
- ◆ *EMC Solutions Enabler Support Matrix, V6.0*, EMC Corporation
- ◆ *EMC Solutions Enabler Installation Guide*, EMC Corporation
- ◆ *EMC Solutions Enabler Symmetrix Base Management CLI Product Guide*, EMC Corporation
- ◆ *EMC Solutions Enabler Symmetrix Access Control CLI Product Guide*, EMC Corporation
- ◆ EMC Host Connectivity Guides

Conventions Used in this Manual

The following conventions are used in this manual:

In this manual, every use of the word SYMCLI means EMC Symmetrix command line interface.

Every occurrence of the word MVS in text or in symbolic syntax means OS/390 and z/OS.

Every occurrence of the word OSF1 in text or in symbolic syntax means Tru64 UNIX.

Note: A note calls attention to any item of information that may be of special importance to the reader.



CAUTION

A caution contains information essential to avoid damage or degraded integrity to storage of your data. The caution might also apply to protection of your software or hardware.

Typographical Conventions

This manual uses the following type style conventions in this guide:

bold text	Boldface text provides extra emphasis and emphasizes warnings, and specifies window names and menu items in text.
<i>italic text</i>	<i>Italic text and characters emphasizes new terms, identifies variables in a software syntax (non-literal notation), identifies unique word usage, and applies emphasis in examples and in references to book titles and sections.</i>
<code>fixed space courier font</code>	A fixed space font identifies files and path names, and is used in command line entries, displayed text, or program listings.

Where to Get Help

EMC software products are supported directly by the EMC Customer Support Center.

Obtain technical support by calling the EMC Customer Support Center at one of the following numbers:

- United States:** (800) 782-4362 (SVC-4EMC)
- Canada:** (800) 543-4782 (543-4SVC)
- Worldwide:** (508) 497-7901

Language services are available upon request.

Sales and Customer Service Contacts

For the list of EMC sales locations, please access the EMC home page at:

<http://www.emc.com/contact/>

For additional information on the EMC products and services available to customers and partners, refer to the EMC Powerlink website at:

<http://powerlink.emc.com>

Your Comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please e-mail us at **techpub_comments@emc.com** to let us know about your opinion or any errors concerning this manual.

This chapter provides an overview of the device masking architecture. The chapter covers the following topics:

- ◆ Device Masking Overview1-2
- ◆ Supported Topologies.....1-5
- ◆ Device Masking VCMDDB Security Enhancement1-7
- ◆ Device Masking Commands1-9

Device Masking Overview

SYMCLI device masking provides the ability to assign and mask access privileges of host bus adapters (HBAs) to Symmetrix® directors and devices by associating one or more devices with an HBA-to-FA connection (known as a *masked channel*) that you define in the Symmetrix-based device masking database, known as the VCMDB. The VCMDB maintains all access records for an array and monitors host access to resolve any conflicts that might arise from multiple hosts having visibility to the same devices.

The device masking commands can also be used to configure heterogeneous hosts with shared access to the same FA port, which is useful in an environment with different host types. However, you can also use Fibre Channel ID lockdown security to protect an HBA from predatory WWN spoofing.

Note: For a detailed introduction to Solutions Enabler, SYMCLI, and the Symmetrix array, refer to the *EMC Solutions Enabler Symmetrix Base Management CLI Product Guide*.

How Symmetrix Device Masking Works

If you define masked channels that allow multiple hosts to connect to a single Symmetrix director, potential conflicts may arise as multiple hosts have access to discover and use the same set of devices. Device Masking allows you to control host access to a set of devices by maintaining a set of entries in the VCMDB on the array that defines the relationship between masked connections and devices.

Each entry includes a host's HBA identity (the HBA port WWN), its associated FA port, and a range of devices mapped to the FA port that should be visible only to the corresponding HBA. Once you make this VCMDB entry and activate the configuration, the Symmetrix makes visible to a host those devices that the VCMDB indicates are available to that host's initiator WWN through that FA port.

The VCMDB on each Symmetrix array specifies the devices that a particular host can access through a specific director. Each director can control access to as many as 64 unique WWNs or 128 iSCSIs (beginning with Engenuity Version 5670). As many as 128 fiber director ports, and 64 multi-protocol (iSCSI) ports (depending on the Symmetrix model) can be configured within the device masking VCMDB.

You can initialize, back up, and restore this database. In addition, you can list, add, and remove database entries, clear the database, and manage WWN and iSCSI names.

Host Access Example

When a host attempts to access a Symmetrix storage device, as shown in In Figure 1-1, the host HBA initiator name (supplied when the host logs in to the fabric or arbitrated loop) is passed to the Symmetrix director port.

The Symmetrix records the connection, stores the initiator name in a *login history table* in its memory, and thereafter grants access to only the devices that are available to that initiator through that director port (as specified in the device masking VCMDB). However, if CHAP authentication is enabled in a native iSCSI topology, the VCMDB will first check the credential and secret before granting access.

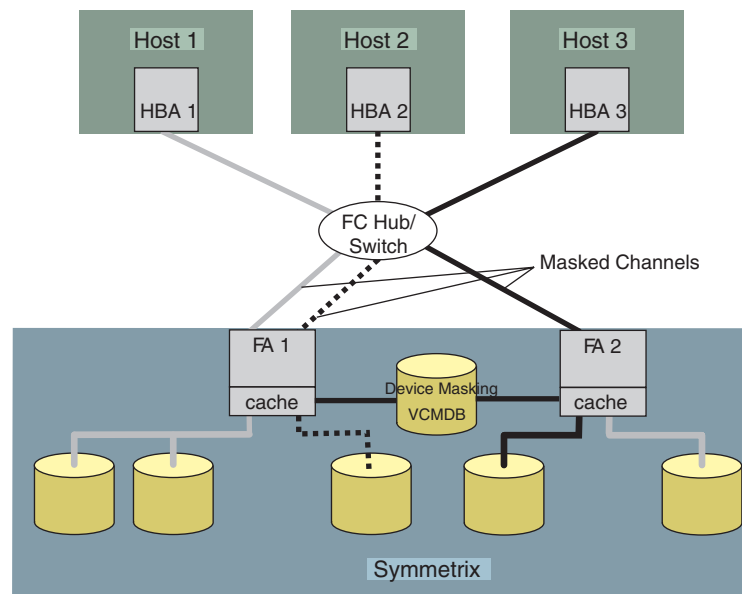


Figure 1-1 Device Masking Solution with WWN Initiators

The host HBA port then sends I/O requests directed at particular Symmetrix devices to the director port. Each request includes the identity of the requesting HBA (from which its WWN or iSCSI can be determined) and the identity of the requested device, with its director and logical unit number (LUN).

The software that runs on a Symmetrix system processes each I/O request to verify that the HBA is allowed to access that device. Any request for a device that an HBA does not have access to, returns an error to the host.

In Figure 1-1 on page 1-3, device masking grants Host 1 access to two of the three devices available through FA1, and grants Host 2 access to a third device. Similarly, Host 3 is granted access to only one of the two devices available through FA2, reserving the second device for use as a spare.

Managing Access for Unsupported Host Platforms

Device masking can also manage access for host platforms that are not supported by this release. If a host can log on to the Symmetrix arrays using a Fibre Channel interface, its access can be controlled.

However, device masking cannot automatically determine the configuration of hosts on unsupported platforms. Instead, you must manually set up a record in the database for these hosts.

Note: Because hosts on unsupported platforms cannot run device masking commands used for verifying host initiator name bindings, you must manage and update names without SYMCLI. Contact EMC Customer Support for help with hosts on unsupported platforms.

Supported Topologies

Device masking supports Fibre Channel (point-to-point and multi-initiator) and native iSCSI topologies.

Fibre Channel Topology

Figure 1-2 illustrates two different Fibre Channel network configurations that Device Masking supports:

- ◆ Point-to-Point — Network A (left) is configured with a direct connections from one HBA on each host to one FA on the array, providing each host with access to a different set of devices.
- ◆ Multi-Initiator — Network B (right) is configured with multiple hosts accessing the same Symmetrix devices via a common fabric.

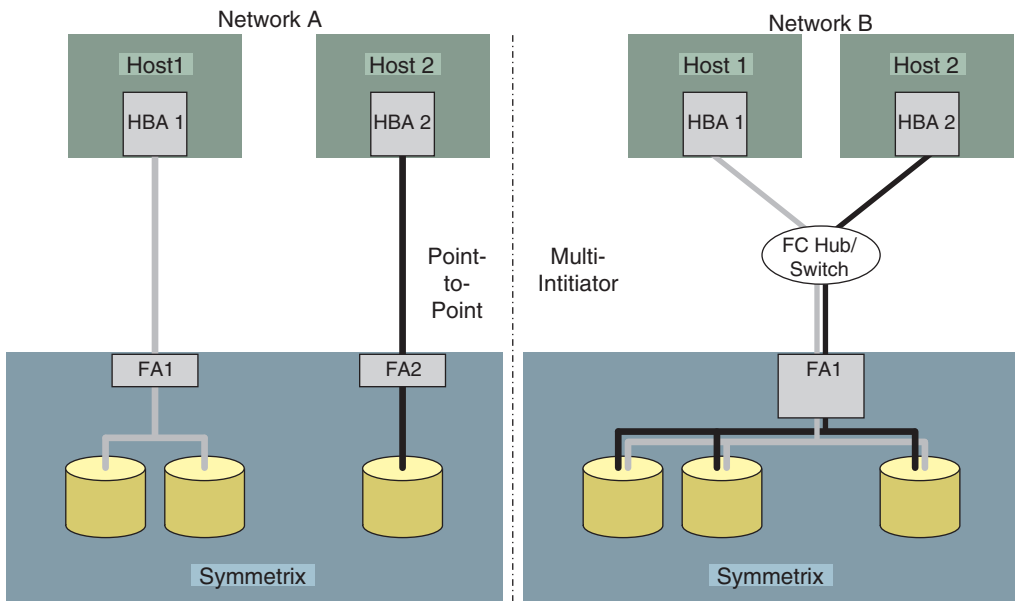


Figure 1-2 Point-to-Point and Multi-Initiator Topologies

Native iSCSI Topology

In contrast to the Fibre Channel topology, in a native iSCSI environment, hosts are connected to a Symmetrix DMX™ array through an Ethernet switch, as shown in Figure 1-3.

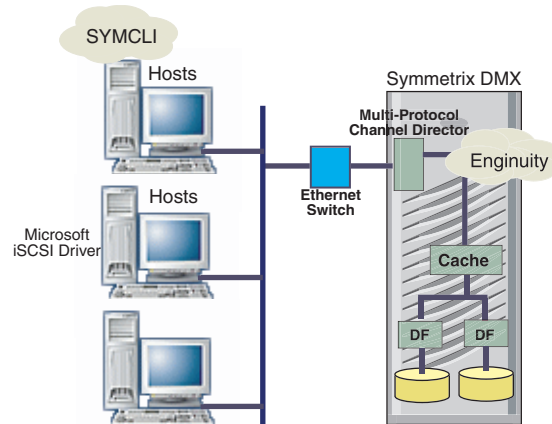


Figure 1-3 Native iSCSI Topology

CHAP

Native iSCSI support standards require that a security protocol be available. Enginuity™ Version 5670 provides the Challenge Handshake Authentication Protocol (CHAP), which can be enabled or disabled by the user. Refer to *iSCSI Software Driver Configuration* on page 2-4 for more information about CHAP authentication.

HBA Initiator Support

Both HBA and Symmetrix director ports in the topology are uniquely identified by a name (WWN or iSCSI). For ease of use, you can associate an ASCII nickname (AWWN and AISCsi).

SYMCLI device masking supports the following HBA initiators:

- ◆ World Wide Name (*wwn*) and alias for World Wide Name (*awwn*)
- ◆ Native iSCSI over TCP/IP (*iscsi*) and alias for iSCSI over TCP/IP (*aiscsi*)
- ◆ iSCSI over TCP/IP on fibre (*iscsi*) and alias for iSCSI over TCP/IP on fibre (*aiscsi*)

Refer to *Discovering Host HBAs* on page 3-6 for more information about WWN and iSCSI initiators.

Device Masking VCMDB Security Enhancement

By default, the device masking VCMDB is accessible to all HBAs that log into the director port where the database is configured. Thus, any host with access privileges can effectively modify the contents of the database if it has device masking installed.

However, to prevent an unauthorized host from changing the database, an enhancement to the Symmetrix operating system (Enginuity Versions 5265 and higher) allows you to control a host's access to the database device through the contents of the database records. This enhancement allows only HBAs with valid records in the database to access to database. This enhancement works with all versions of device masking.

Beginning with Enginuity Version 5670, the VCMDB can be unmapped from any director that is not being used for masking control.

Note: If you have PowerPath installed, you should keep the VCMDB mapped.

Using Enginuity Syscalls

The Solutions Enabler SYMCLI Version 5.3 includes some changes to the management of the VCMDB. In prior versions of SYMCLI, the host system wrote directly to the VCMDB in the Symmetrix array, which was then read by the Enginuity software (see Figure 1-4). Any host with access to the VCMDB could update the database.

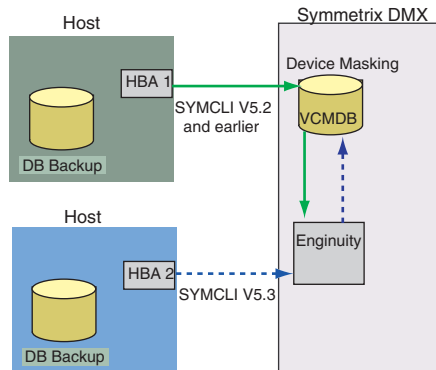


Figure 1-4 Device Masking Syscalls

Since SYMCLI Version 5.3, and Enginuity Version 5670, the host communicates with the Enginuity software, which then communicates via syscalls to the VCMDB.

Device Masking Commands

SymCLI commands `symmask` and `symmaskdb` specifically support the device masking control and monitor operations. With these commands, you can define and query the Symmetrix devices that each host's HBA ports are permitted to access.

The `symmask discover` command can be run on both the control station and the managed hosts. The `symmask discover` action locates paths to the device masking database (VCMDB) and assigns alias names (AWWN/AISCSI) to the HBAs residing on the host on which the command is run if they are NULL. You can optionally use the `rename` action to generate aliases to be assigned.

Database Device Locking

During the execution of the `symmask` or `symmaskdb` commands, the SymCLI sets a Symmetrix External Lock (SEL) on the Symmetrix where the device masking database (VCMDB) resides. This lock ensures that only one host can make changes to the database at any one point in time.

If during the processing of a `symmask` or `symmaskdb` command, the host fails, or a Ctrl/C is performed in the middle of the command, the lock might not release and could lock out further needed changes or control actions. If a device masking command is interrupted and the lock is not released, future invocations of a device masking command will display the following error message:

```
The operation failed because another process has an
exclusive lock on the local Symmetrix.
```

To further examine the presence of this lock, use the following form:

```
symcfg -sid SymmID list -lock -lockn ALL
```

The command will list Symmetrix external locks being held. For this case, it will show a number 14 device masking lock and the length of time it has been on.

To release this lock, use the following form:

```
symcfg -sid SymmID -lockn 14 release
```

Command Summary

Table 1-1 and Table 1-2 on page 1-11 summarizes the device masking actions. The `symmask` and `symmaskdb` actions are described in detail in the *EMC Solutions Enabler Symmetrix CLI Command Reference*.

Table 1-1 symmask Command Summary

Command	Action	Description
symmask	add devs	Adds a device to the list of devices that a WWN can access in the database.
	remove devs	Removes a device from the list of devices that a WWN can access in the database.
	delete	Deletes all access rights for a WWN in the database (specified either by WWN or AWWN).
	enable authentication	Enables the use of authentication by the Symmetrix array for the host HBA.
	disable authentication	Disables the use of authentication by the Symmetrix array for the host HBA.
	show authentication	Shows the current authentication data for the specified iSCSI host HBA.
	replace	Allows one HBA to replace another.
	set authentication	Allows authentication data to be established for iSCSI connections.
	set lockdown	Sets or clears the Fibre Channel ID lockdown.
	set visibility	Sets or clears device visibility for noncontiguous LUNs.
	set lunoffset	Sets or clears a LUN base/offset skip for noncontiguous LUNs.
	set heterogeneous	Sets or clears heterogeneous host information with distinctive attributes.
	rename	Changes the AWWN for the specified WWN in the database and the login history table.
	refresh	Causes the Symmetrix system to refresh its WWN-related memory tables with the contents of the database.
	discover hba	Discovers the HBAs on the host and assigns AWWNs to the login history table entries for those WWNs that are not set.
	list logins	Lists, for each fibre director, which hosts and HBAs are logged in to a Symmetrix system (login history table contents).
	list HBA	Lists the WWNs of the fibre HBAs on this host.

Table 1-2 symmaskdb Command Summary

Command	Action	Description
symmaskdb	init	Creates and initializes a device masking database. On completion, the database device cannot be written to by the operating system. Caution: This action removes all information from an existing database.
	backup	Backs up a database to a specified file.
	restore	Restores a database from a specified file.
	remove	Removes the specified meta member device(s).
	convert	Converts the database from a Type 3 to a Type 4 or Type 5 database and a Type 4 to a Type 5 database.
	set	Allows you to block or allow direct IO reads from the host to the VC MDB.
	list database	Lists, for each Symmetrix fibre director, which devices in a Symmetrix system a WWN can access (device masking database contents). Lists the contents of a backup file.
	list devs	Lists all devices accessible to an HBA on a specified Symmetrix system or a backup file, and all directors that can access each device.
	list assignment	Lists the HBA assignments to devices.
	list capacity	Lists the capacity of devices assigned to a particular host.

Volume Logix Conversion

If you have been using EMC's Volume Logix and need to convert to the SYMCLI device masking command set, Table 1-3 lists equivalent SYMCLI commands to replace the Volume Logix commands.

Table 1-3 Volume Logix to SYMCLI Conversion

VCM Command	SYMCLI Command
vcmfind	symmask discover hbas
fpath lshbawwn	symmask list hbas
fpath lshosts -d	symmask -sid list logins
fpath adddev -d [-w -u] -f -r	symmask -sid [-wwn -awwn] -dir -p add devs <r>
fpath rmdev -d [-w -u] -f -r	symmask -sid [-wwn -awwn] -dir -p remove devs <r>
fpath chgname -d -w -n	symmask -sid -wwn rename <awwn>
fpath clrrwn -d [-w -u]	symmask -sid [-wwn -awwn] delete
fpath swaphba -d [-w -u] -n	symmask -sid [-wwn -awwn] replace <wwn>
fpath chgattr -d -h	symmask -sid [-wwn -awwn] -dir -p set visibility <on off>
fpath chgattr -d -s -v	symmask -sid [-wwn -awwn] -dir -p set lockdown <on <fcid> off>
fpath chgattr -d -l -o -b	symmask -sid [-wwn -awwn] -dir -p set lunoffset <on <offset><base> off>
fpath chgattr -d -m -c	symmask -sid [-wwn -awwn] -dir -p set heterogeneous <on <host> off>
fpath refresh -d	symmask -sid refresh
fpath lsdb -d	symmaskdb -sid list database
fpath lsbackup -o	symmaskdb -file list database
fpath lshbavols [-d -o] [-w -u]	symmaskdb -sid [-wwn -awwn] list devs
fpath initdb -d	symmaskdb -sid -file init
fpath backupdb -d	symmaskdb -sid -file backup
fpath restoredb -d	symmaskdb -sid -file restore
fpath lshostdev	sympd list -sid

Table 1-3 Volume Logix to SYMCLI Conversion (continued)

VCM Command	SYMCLI Command
<code>fpath lssymmdev -d</code>	<code>symcfg list -sid -FA all -address</code>
<code>fpath lssymmfas -d</code>	<code>symcfg list -sid -FA all</code>
<code>fpath lsstatus -d</code>	<code>symcfg list -sid -v</code>

Prior to using the device masking SYMCLI commands with iSCSI, you must configure your iSCSI driver software and authentication information. The chapter covers the following topics:

- ◆ iSCSI CHAP Authentication: Engenuity Version 56xx.....2-2
- ◆ iSCSI Software Driver Configuration.....2-4

iSCSI CHAP Authentication: Enginuity Version 56xx

The iSCSI authentication is negotiated during the HBA login phase and can be implemented using CHAP (Challenge Handshake Authentication Protocol). CHAP allows you to manage a credential name and a CHAP secret, which are similar to a username and a password, though more secure than the standard Password Authentication Procedure (PAP).

Requirements

Setting iSCSI authentication requires:

- ◆ Symmetrix DMX running Enginuity version 5670 (or higher)
- ◆ Fig-E board that manages the front-end connections in the Symmetrix array
- ◆ Gig-E-configured port
- ◆ host systems that provide driver support for iSCSI
- ◆ An initialized device masking database (VCMDB)

Before an iSCSI host can log in and see any devices, the iSCSI name of the host must have a valid VCMDB database entry specifying the director and port from which it is connecting. For details on configuring your iSCSI drivers, refer to *iSCSI Software Driver Configuration* on page 2-4.

Setting iSCSI Authentication via the SYMCLI

Once you have configured your iSCSI driver software, you can set the credential name and CHAP secret required for iSCSI authentication. The following command sets the authentication for the iSCSI initiator, `iqn.2002-06.com.microsoft.host210`, using the authentication type of CHAP. The `-credential` option and `-secret` option specify the required authentication information.

```
symmask -sid 6208
        -iscsi iqn.2002-06.com.microsoft.host210
        set authentication -type CHAP
        -credential MyCredentials -secret MySecret
```

Showing Authentication Information

The `symmask show` command returns the authentication information for a specified iSCSI initiator on a specific Symmetrix array. Note that the CHAP secret is never displayed. For example:

```
symmask -sid 6208
-iscsi ign.2002-06.com.microsoft.host210
show authentication
```

You can also display authentication data using the `symmaskdb list database -v` command.

When you set authentication using the `symmask` command, authentication is automatically enabled. If you decide to disable authentication, the authentication values are retained in the VC MDB, which allows you to enable them at a later time using the `enable` action. The following command disables authentication.

```
symmask -sid 6208
-iscsi ign.2002-06.com.microsoft.host210
disable authentication
```

Restoring Authentication Data and Updating the iSCSI Driver

When you restore a database, authentication data is restored to the Symmetrix array from the backup file. Keep in mind that the same authentication data also needs to be set in the host's iSCSI driver software if authentication had been changed since the backup file was generated.

If you had changed your authentication data after the backup file was created, the restored authentication data will be out of sync with the authentication data stored in the iSCSI driver software. To rectify this discrepancy, you must update the iSCSI driver software with the same information contained in the restored authentication data. For more information, refer to *iSCSI Software Driver Configuration* on page 2-4.

To avoid restoring obsolete authentication data, use the `-skip_authentication` option. For example:

```
symmaskdb -sid 814 restore
-file MyDevMaskBackup -skip_authentication
```

iSCSI Software Driver Configuration

This section provides the requirements and configuration steps for preparing a host system with a native iSCSI initiator and the VCMDB (residing in a Symmetrix DMX) to communicate via the Microsoft iSCSI software driver and the EMC Multi-Protocol Channel Director.

The following is an overview of the configuration process:

1. Collect information about the host computer and the Symmetrix DMX Multi-Protocol Channel director:
 - Get the iSCSI name and IP address of the Symmetrix director from the Symmetrix array.
 - Get the iSCSI name of the initiator from the host computer.
2. Configure information in the VCMDB of the Symmetrix array that will allow the host computer to access the Symmetrix devices desired:
 - Add access to the Symmetrix devices from the host initiator by the iSCSI name to the VCMDB.
 - Add the iSCSI authentication information (if any) about the host initiator.
 - Refresh the database.
3. Update the iSCSI Initiator with the Symmetrix information:
 - Establish a target connection via iSCSI between the host computer and the designated Symmetrix director port with/without authentication.
 - Have the host computer logon to the Symmetrix via iSCSI and establish target devices on the host computer that will persist through a reboot.
4. Perform the following disk administration on the devices on the Symmetrix array, if needed:
 - Format
 - Write signatures
 - Assign drive letters

Configuration of the iSCSI driver can be completed with CHAP authentication as described in *Configuring iSCSI with CHAP Authentication* on page 2-6, or without authentication as described in *Configuring iSCSI without CHAP Authentication* on page 2-14. Refer to

the procedure that meets your environment's authentication requirements.

Requirements

For a list the supported hosts, network, and array requirements for native iSCSI refer to the *EMC Solutions Enabler Support Matrix, V6.0*.

Note: Your systems must be installed and connected to the network before beginning the configuration.

Installing the iSCSI Software Initiator

From the Microsoft download site, install the Microsoft iSCSI Software Initiator Version 1.0.

The setup installs an icon on your desktop.

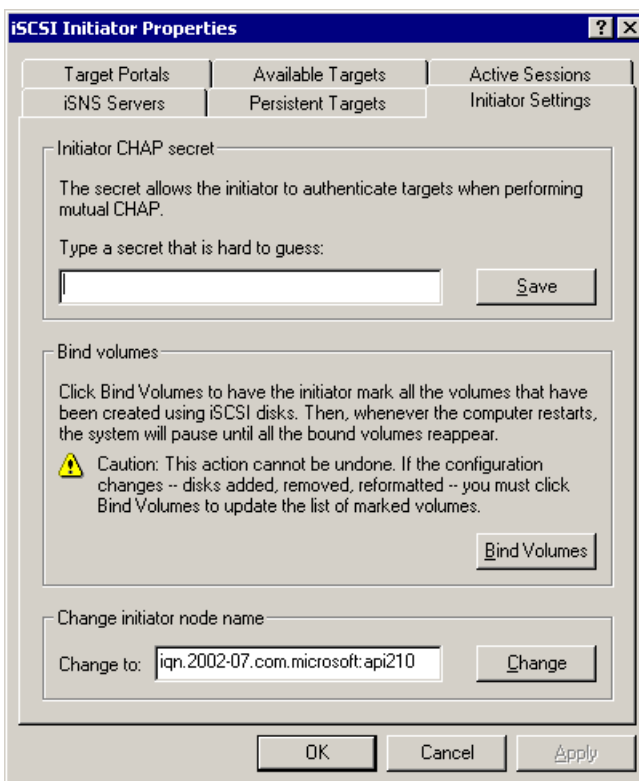
Configuring iSCSI with CHAP Authentication

To complete this configuration, you must obtain the iSCSI name of the host, and the iSCSI ID of the multi-protocol director.

Note: This procedure contains steps that require the use of the iSCSI Initiator window and the DOS command window, as follows.

Collect Information about the Host Computer and Symmetrix Director

1. Execute the iSCSI Initiator control panel on the host system.
2. Click the **Initiator Settings** tab.



3. Copy the iSCSI ID of your host from the **Change to** field at the bottom of the window.

Important: Do not enter any data in this window.

4. From the command line, display and copy the IP address of the Symmetrix multi-protocol director, as shown in this example:

```
symcfg -sid 6208 -dir 3a list -v
```

The last two lines of the display contain the iSCSI name and IP address. For example:

```
Symmetrix ID: 000000006208

Product Model           : DMX2000P
Symmetrix ID            : 000000006208
Microcode Version (Number) : 5670 (16260000)
.
.
.
iSCSI NAME              : iqn.1992-04.com.emc.5006048000061002
iSCSI IP Address        : 10.10.10.21
```

Configure Information in the VCMDB

5. Add a device to create a record in the VCMDB, using the following form:

```
symmask -sid SymmID -iscsi iscsi_name -dir # -p # add dev #
```

where:

- *SymmID* — The Symmetrix ID.
- *iscsi_name* — The iSCSI name (from step 3).
- *-dir #* — Symmetrix director number.
- *-p #* — Symmetrix port number.
- *add dev #* — Symmetrix device number(s).

For example:

```
symmask -sid 6208 -iscsi iqn.2002-07.com.microsoft:api210 -dir 3a -p 0 \
add dev 0023
```

6. Set the CHAP authentication in the VCMDB using the SYMCLI, which is done differently for each supported Enginuity version:

- For Enginuity Version **5670** or higher:

```
symmask -sid SymmID -iscsi iscsi_name
set authentication -type CHAP
-credential Credential -secret Secret
```

where:

- *SymmID* — The Symmetrix ID.
- *iscsi_name* — The host iSCSI name.
- CHAP — The authentication type.
- *CHAPcredential* — Eight alphanumeric characters.
- *CHAPsecret* — 12-16 alphanumeric characters.

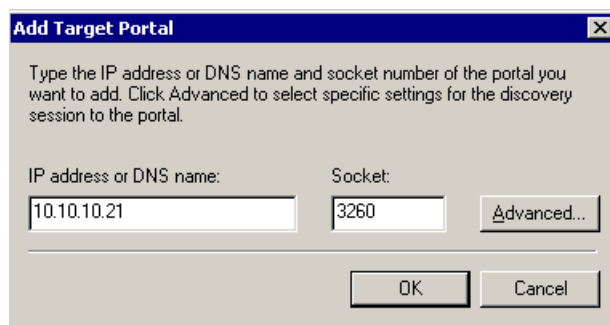
For details about setting iSCSI Authentication, refer to *iSCSI CHAP Authentication: Enginuity Version 56xx* on page 2-2.

7. Refresh the VCMDB, as shown in the following example:

```
symmask -sid 6208 refresh
```

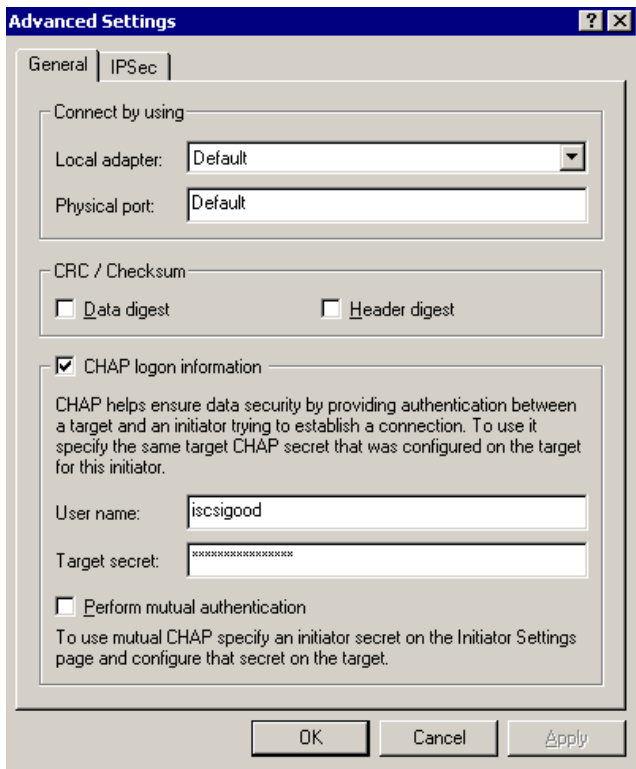
Update iSCSI Initiator with Symmetrix Information

8. From the iSCSI Initiator Properties window, click the **Target Portals** tab and click **Add**. The **Add Target Portal** dialog box appears.



9. Enter the iSCSI IP address (from step 4) of the Symmetrix multi-protocol director in the **IP address or DNS name** box and click **Advanced**.

The **Advanced Settings** dialog box displays. The iSCSI name automatically displays in the **User name** field. Do not use this for your credential.



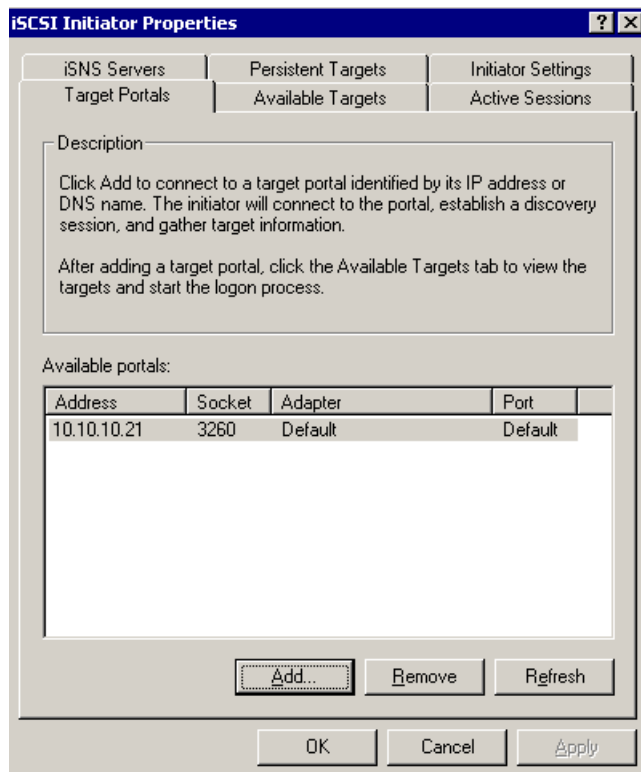
10. Check the box labeled **CHAP logon information**. Change the CHAP credential in the **User name** field, and enter a CHAP secret in the **Target secret** box. Click **OK**.

The credential name string must be between 8 and 256 characters. The CHAP protocol secret value on UNIX can be 32 ASCII characters, or 64 binary characters (binary values should be prefixed with the string 0x). On Windows the secret must be between 12 and 16 ASCII characters.

Important: Do not check or change anything else in this dialog box.

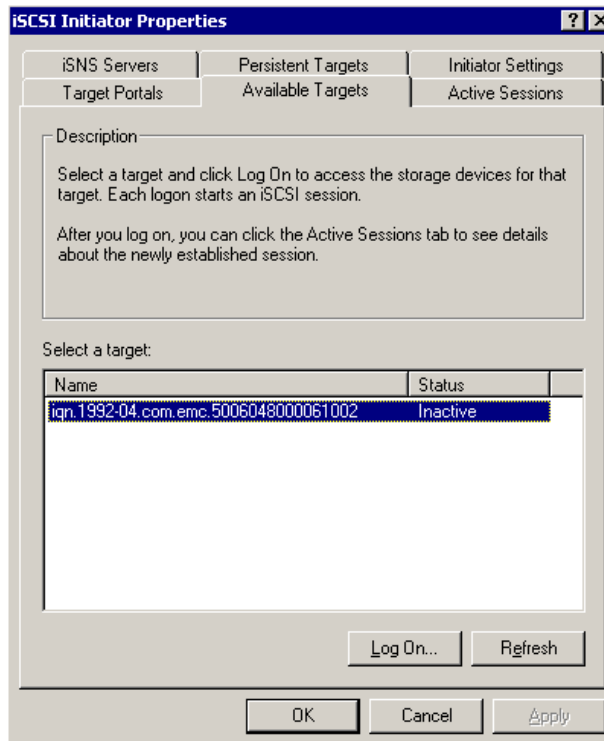
11. Click **OK** to close the **Advanced Settings** dialog box, and click **OK** to close the **Target Portal** dialog box.

The multi-protocol director IP address should appear in the **Available portals** list in the **Target Portals** window.

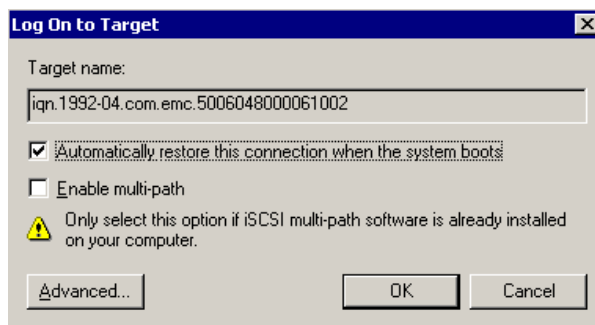


Note: If an error displays, select the IP address from the **Available portals** list and click **Remove**. Begin the configuration procedure again.

12. Click the **Available Targets** tab. The iSCSI name of the Symmetrix multi-protocol director (from step 4) displays in the **Select a target list**.

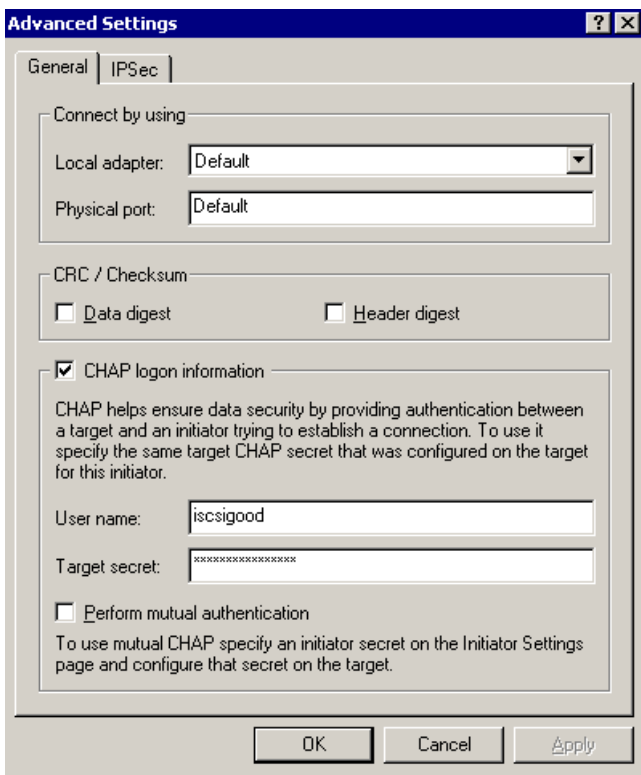


13. Click **Log On**. The **Log On to Target** window dialog box displays.



14. Check **Automatically restore this connection when the system boots**, and click **Advanced**.

The **Advanced Settings** dialog box displays. The iSCSI name automatically displays in the **User name** field. Do not use this for your credential.

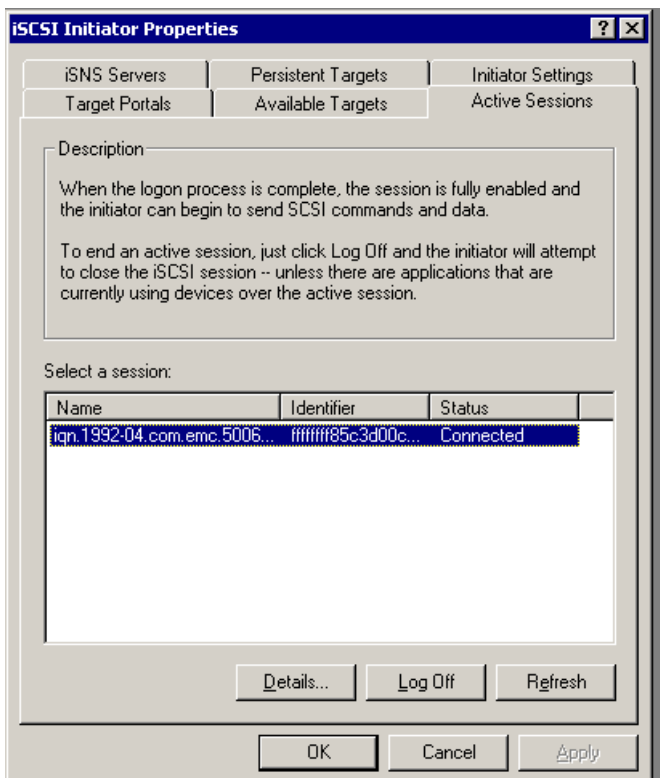


15. Check the box labeled **CHAP logon information**. Change the CHAP credential in the **User name** field, and enter a CHAP secret in the **Target secret** box. Click **OK**.

The credential name string must be between 8 and 256 characters. The CHAP protocol secret value on UNIX can be 32 ASCII characters, or 64 binary characters (binary values should be prefixed with the string 0x). On Windows the secret must be between 12 and 16 ASCII characters.

Important: Do not check or change anything else in this window.

16. From the iSCSI Initiator Properties window, click the **Active Sessions** tab. An active session should display in the **Select a session** list.



17. Select the session and click **Details** to display the disks found by the iSCSI driver.
18. Click **OK** to exit from the iSCSI Initiator.

Perform Disk Administration on the Symmetrix Devices

19. Perform any necessary disk administration, such as, formatting, write signatures, and assigning drive letters.
20. Reboot the host system.

Note: The configuration changes you made will not take effect until you reboot your host.

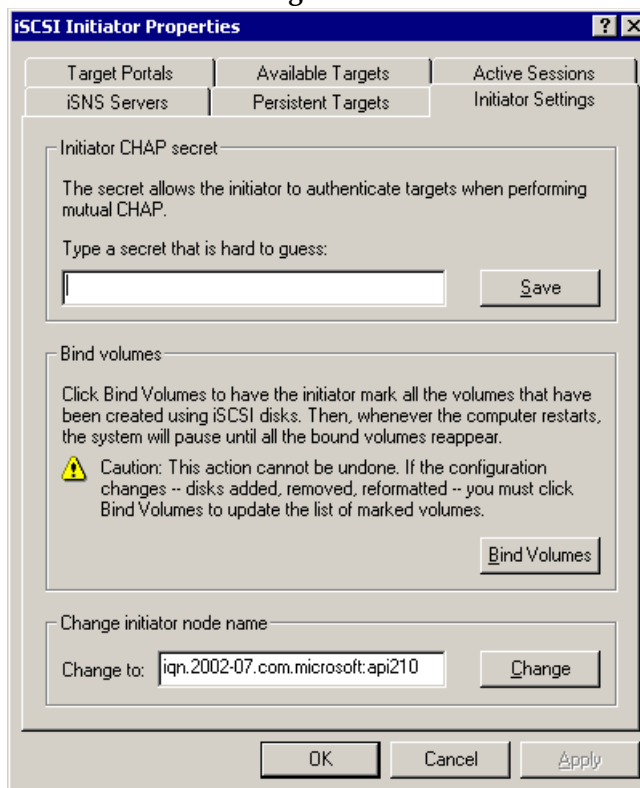
Configuring iSCSI without CHAP Authentication

To complete this configuration, you must obtain the iSCSI name of the host, and the iSCSI ID of the multi-protocol director.

Note: This procedure contains steps that require the use of the iSCSI Initiator Properties window and the SYMCLI command window, as follows.

Collect Information About the Host Computer and Symmetrix Director

1. Open the iSCSI Initiator on the host system.
2. Click the **Initiator Settings** tab.



3. Copy the iSCSI ID of your host from the **Change to** field at the bottom of the window.

Important: Do not enter any data in this window.

4. List the iSCSI name and IP address of the Symmetrix multi-protocol director, as shown in this example:

```
symcfg -sid 6208 -dir 3a list -v
```

The last two lines of the display contain the iSCSI name and IP address. For example:

```
Symmetrix ID: 000000006208

Product Model           : DMX2000P
Symmetrix ID            : 000000006208
Microcode Version (Number) : 5670 (16260000)
.
.
.
iSCSI NAME              : ign.1992-04.com.emc.5006048000061002
iSCSI IP Address        : 10.10.10.21
```

Configure Information in the VCMDB

5. From the command line, add a device to create a record in the VCMDB, using the following form:

```
symmask -sid SymmID -iscsi iscsi_name -dir # -p # add dev #
```

where:

- *SymmID* — The Symmetrix ID.
- *iscsi_name* — The iSCSI name copied in step 3.
- *-dir #* — Symmetrix director number.
- *-p #* — Symmetrix port number.
- *add dev #* — Symmetrix device number.

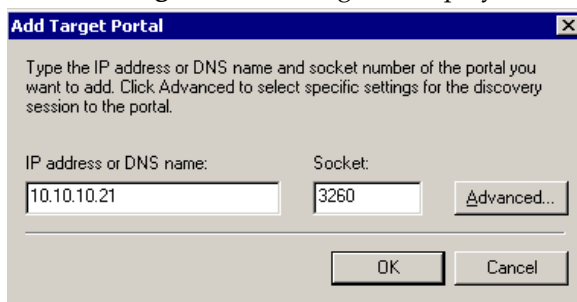
For example:

```
symmask -sid 6208 -iscsi ign.2002-07.com.microsoft:api210 -dir 3a -p 0 \
add dev 0023
```

6. Refresh the VCMDB, as shown in the following example:


```
symmask -sid 6208 refresh
```
7. From the iSCSI Initiator window, select the **Target Portals** tab and click **Add**.

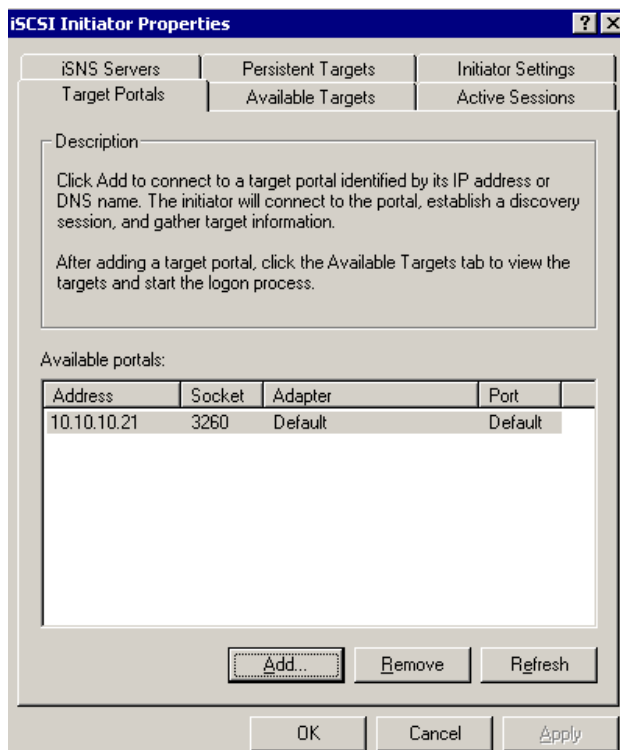
The **Add Target Portal** dialog box displays.



The **Add Target Portal** dialog box is shown. It has a title bar with a close button. The main text says: "Type the IP address or DNS name and socket number of the portal you want to add. Click Advanced to select specific settings for the discovery session to the portal." Below this, there are two input fields: "IP address or DNS name:" with the value "10.10.10.21" and "Socket:" with the value "3260". To the right of the socket field is an "Advanced..." button. At the bottom are "OK" and "Cancel" buttons.

8. Enter the iSCSI IP address (from step 4) of the Symmetrix multi-protocol director in the **IP address or DNS name** box and click **OK**.

The multi-protocol director IP address should appear in the **Available portals** list in the **Target Portals** window.

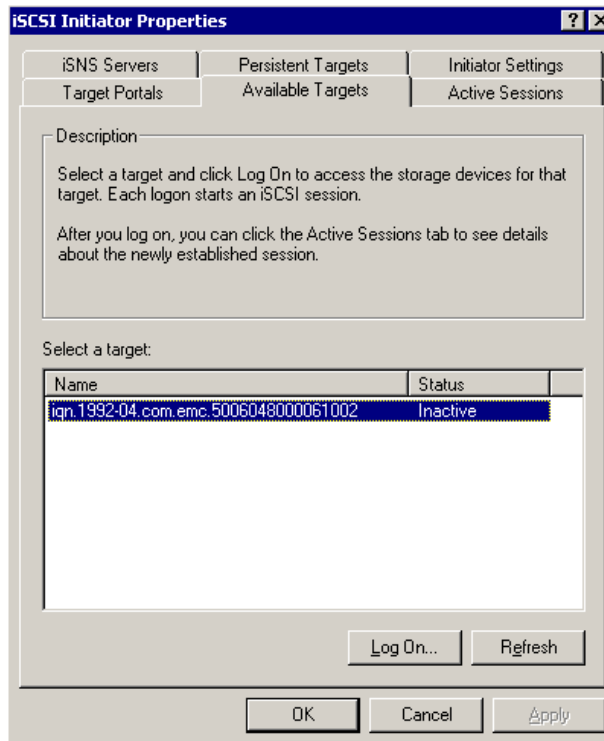


The **iSCSI Initiator Properties** dialog box is shown. It has a title bar with a help button and a close button. Below the title bar are four tabs: "iSNS Servers", "Persistent Targets", "Initiator Settings", and "Target Portals". The "Target Portals" tab is selected, showing a sub-tab "Available Targets". Below the tabs is a "Description" box with text: "Click Add to connect to a target portal identified by its IP address or DNS name. The initiator will connect to the portal, establish a discovery session, and gather target information. After adding a target portal, click the Available Targets tab to view the targets and start the logon process." Below the description is a table titled "Available portals:" with columns: "Address", "Socket", "Adapter", and "Port". The table contains one row: "10.10.10.21", "3260", "Default", and "Default". Below the table are "Add...", "Remove", and "Refresh" buttons. At the bottom are "OK", "Cancel", and "Apply" buttons.

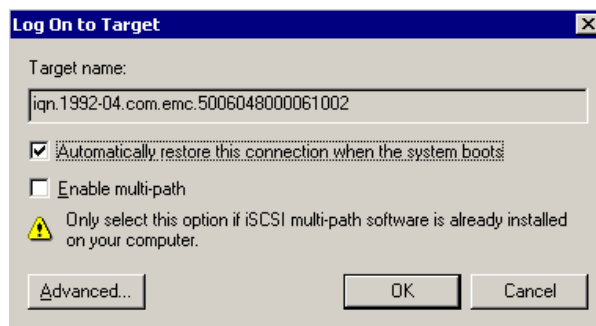
Address	Socket	Adapter	Port
10.10.10.21	3260	Default	Default

Note: If an error displays, select the IP address from the **Available portals** list and click **Remove**. Begin the configuration procedure again.

9. Click the **Available Targets** tab. The iSCSI name of the Symmetrix multi-protocol director (from step 4) displays in the **Select a target list**.

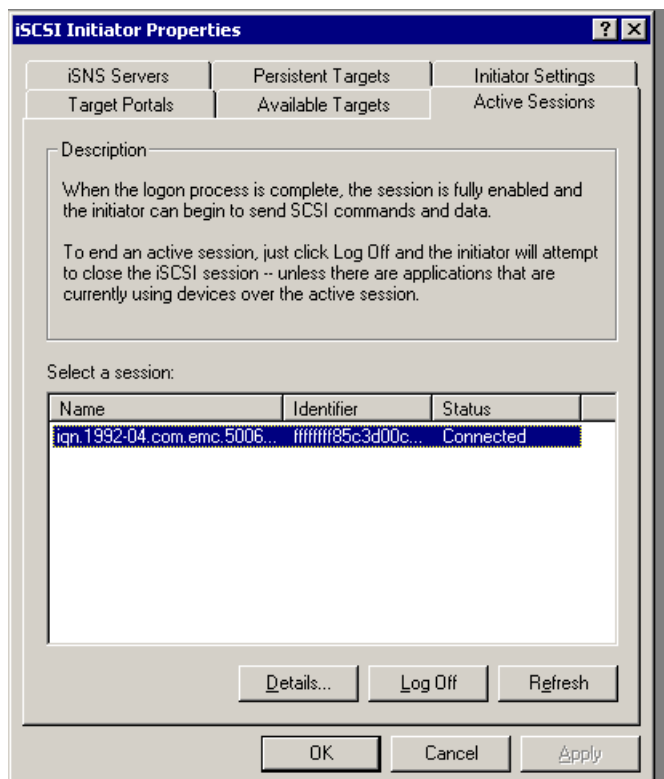


10. Click **Log On**. The **Log On to Target** dialog box displays.



11. Check **Automatically restore this connection when the system boots**, and click **OK**.

12. Click the **Active Sessions** tab. An active session should display in the **Select a session** list.



13. Select the session and click **Details** to display the disks found by the iSCSI driver.
14. Click **OK** to exit from the iSCSI Initiator Properties window.

Perform Disk Administration on the Symmetrix Devices

15. Perform any necessary disk administration, such as, formatting, write signatures, and assigning drive letters.
16. Reboot the host system.

Note: The configuration changes you made will not take effect until you reboot your host.

Device Access Management

This chapter describes the device masking concepts and how to confine host access to Symmetrix devices using the device masking commands of the SYMCLI. The chapter covers the following topics:

- ◆ Initial Device Masking Setup3-2
- ◆ Device Masking Configuration.....3-3
- ◆ Discovering Host HBAs3-6
- ◆ How to Add and Remove Masked Devices3-8
- ◆ Device Masking VCMDB Maintenance3-10
- ◆ HBA Initiator Management.....3-20
- ◆ Fibre Channel-to-Host Interface Management3-21

Initial Device Masking Setup

Before you begin to using the Solutions Enabler Device Masking, it is important to understand your device masking and test your scripts in a controlled environment.

When you setup your device masking environment, you should initialize the device masking VC MDB (see *Initializing the Database* on page 3-10). This should only be done on an initial setup, since it clears the device of any and all data.

Once you understand the Solutions Enabler Device Masking functionality described herein, you can begin to develop device masking scripts customized for your environment.

Access Control Environment Setup

If Symmetrix Access Control is being used to protect Symmetrix devices, the host from which you run the device masking commands must be configured in an access control group with an ACL (Access Control List) granting VLOGIX rights. Otherwise, attempted changes to the configuration records in the VC MDB would fail.

For more information about the Symmetrix Access Control `symacl` command, see the *EMC Solutions Enabler Symmetrix Access Control CLI Product Guide*.

Device Masking Configuration

Configuring device masking involves four steps:

1. Identify Configuration Components
2. Initialize and Update the Database
3. Enable Authentication
4. Recommendations for Activating the Configuration

You should be logged on to the control station as Administrator in an MS-DOS command prompt window (on a Windows system) or as root in an xterm window (on a UNIX system).

Identify Configuration Components

Figure 3-1 shows device masking components to identify.

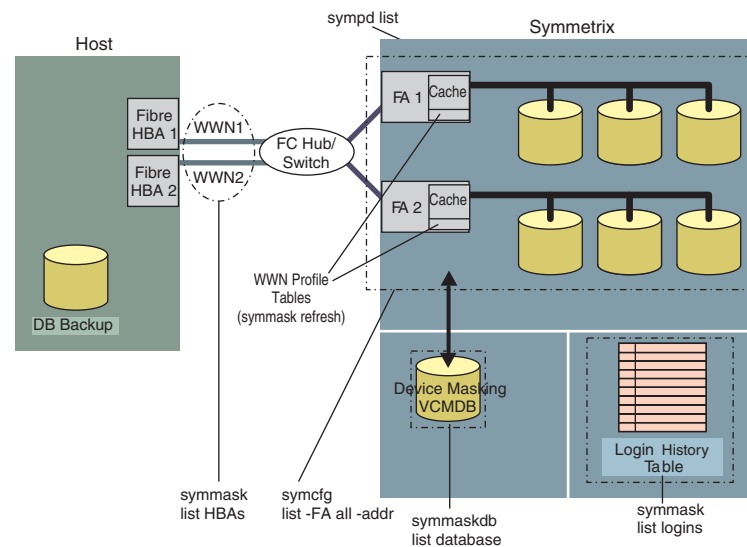


Figure 3-1 Device Masking Components

Use the commands in Table 3-1 to determine the identifiers of each element.

Table 3-1 Identifying Your Configuration

To Identify	Use
Symmetrix physical device names of all the device masking devices.	<code>sympd list -vcm</code>
Initiator (WWN/iSCSI) of each HBA on the host.	<code>symmask list hba</code>
Symmetrix director port to which each HBA on the host connects.	<code>symmask list logins</code>
Available Symmetrix devices for each director port.	<code>symcfg list -FA ALL -addr</code>

SYMCLI device masking supports both World Wide Name (WWN) and native iSCSI (iSCSI) HBA connections.

Initialize and Update the Database

After you identify each element, you can initialize the database and create records using the commands in Table 3-2.

When initializing the VCMDB device on a Symmetrix array running Enginuity Version 5670, if `-vcmdb_type` is not specified, a database will be created based on what size device is present. For more information regarding different VCMDB types, refer to *VCMDB Database Types* on page 3-17.

Table 3-2 Initializing and Updating the Database

To	Use
Initialize the device masking VCMDB device (initial creation only):	<code>symmaskdb init^a -file</code>
Designate, for a specified HBA port, which devices are masked to which HBA on this host. Use the names/identifiers displayed by the commands listed in Table 3-1: Database: <code>sympd list</code> HBA port: <code>symmask list hba</code> Director: <code>symmask list logins</code> Devices: <code>symcfg list all -addr -FA all</code> Repeat for each WWN/iSCSI in the configuration.	<code>symmask add devs</code>

- a. If no database type is specified, and a 96-cylinder device, a type 5 database is created. If no database type is specified, and a 48-cylinder device, a type 4 database is created. If no database type is specified, and a 24-cylinder device, a type 3 database is created.

Enable Authentication

For detailed information regarding initializing, setting, enabling, and disabling authentication, refer to Chapter 2, *iSCSI Setup*.

Recommendations for Activating the Configuration

To ensure that updates to the VCMDB become active and visible to your host, it is recommended that you:

1. Backup the device masking VCMDB to a file by calling `symmaskbd backup`.
2. Update the Symmetrix array with the configuration changes, by performing `symmask refresh`. This calls the Symmetrix director to refresh its WWN/iSCSI-related profile tables in cache with the contents of the device masking VCMDB.
3. Reboot all hosts that have had devices added or removed for the changes to take effect.

Note: When you reboot a host, you must run `symcfg discover` to scan the Symmetrix devices and refresh the SYMAPI configuration database.

4. When configuration of the database is complete, use `sympd list` to view the Symmetrix devices that can be seen by the host.

Discovering Host HBAs

During the initial setup, an administrator runs `symmask discover` on the controlling host to search the environment for Symmetrix devices on each HBA by using the following command:

```
symmask discover hba
```

When the `symmask discover` finds a host HBA, it reads the login history table and performs the following:

1. Checks whether an alias exists in the device masking VCMDB. If one does, this command writes it to the login history table.
2. If there is no alias in the device masking VCMDB record, or the login history table, it creates an ASCII alias and writes it to the login history table.

Note: There is a `-rename` option that can be used with this command to force the discovered hostname/HBA name (or IP address) to be written to the login history table and the device masking VCMDB. This will overwrite any existing AWWN/iSCSI record you have previously established.

3. Prints the initiator identifier (WWN/iSCSI) of the HBAs that are connected to the masked channel and Symmetrix array.
4. The initiator identifier and its ASCII alias are written to the device masking VCMDB.

The `symmask discover` command sends information about this connection back to its host system. The `discover` command is the primary mechanism by which hosts other than the control station can learn about their VCMDB paths to the Symmetrix array. This is displayed using the `symmask list hba` command.

Using Alias Names

Whether you have defined alias names (AWWNs/iSCSI) for the various HBAs, or choose to use those assigned by the SYMAPI server during discovery, alias names can be used in the command line, replacing the cumbersome numeric identifiers.

These names, which are stored in the Symmetrix array's login history table, identify the HBAs connected to the network interface. Alias names can be shorter in length and much more recognizable than the cryptic WWNs/iSCSIs.

ASCII Format

All alias names (auto-generated or user-defined) have two parts separated by a slash (/), such as *ALIAS/ALIAS*. An ASCII alias names generated by the `discover` action consists of two parts: the name of the host and the name of the HBA.

- ◆ For Fibre configurations, the adapter number takes the form of the WWN/iSCSI to guarantee uniqueness. For example, the AWWN for a host whose TCP/IP hostname is `john4554b`, on adapter `10000000c920cf87`, would be `john4554b/10000000c920cf87`.
- ◆ For Native iSCSI configurations, the values are hostname/IP address.

Renaming Identifiers

When using various `symmask` actions (such as adding or removing devices in the device mask) you can target an HBA path by specifying an AWWN or AISCISI in the command line. Once you have established the aliases with the identifiers in the history table and database, you can rename existing aliases with `symmask rename` action using the following form:

```
symmask -sid SymmID -iscsi iscsi rename aiscsiNew
```

For example, you are working with Symmetrix 0128 and you want to change your HBA of `20000000c920b484` to `Solar2b`, enter:

```
symmask -sid 0128 -wwn 20000000c920b484 rename Solar2b/b4
```

You can run `symmask list logins` to display the contents of the login history table to examine the existing alias names on a specified Symmetrix array.

How to Add and Remove Masked Devices

The Symmetrix devices you want to isolate can be assigned to a specified masked channel (HBA to director port). You can add or remove devices from these masked channels using their Symmetrix device name.

Adding Devices

To add a device or devices to a specified HBA/director-port channel, use the following syntax:

```
symmask -sid SymmID -wwn wwn|-awwn awwn|-iscsi iscsi |-aiscsi aiscsi
add devs startSymDevname:endSymDevname|SymDevname|SymDevname,,...\
-dir # -p # [-noprompt]
```

For example, to add devices 0014 and 0015 on Symmetrix 0128 for access to Host3b using director 16a, port 0, enter:

```
symmask -sid 0128 -awwn Host3b/4a add devs 0014,0015 -dir 16a -p 0
```

If the devices are not addressed to the specified FA, a warning message displays.

If the devices are already assigned in the database to any WWN, an informational prompt displays. To turn off this functionality, use the `-noprompt` option.

Adding Meta Devices

To add meta devices, add only the *SymDevname* of the device that is designated as the meta head.

Removing Devices

You can remove devices from a masked channel at any time. To remove a device or devices from a masked channel, use this syntax:

```
symmask -sid SymmID -wwn wwn|-awwn awwn|-iscsi iscsi|-aiscsi aiscsi remove devs  
startSymDevname:endSymDevname|SymDevname|SymDevname,,,...\-dir # -p # [-force]
```

The force (`-force`) option may be useful when you want to quickly remove a range of specified device names that might span device names not part of the existing noncontiguous masked channel. It may also be needed when working with meta devices.

After each set of changes, activate the configuration by performing a refresh (`symmask refresh`), back up the database (`symmaskdb backup`), and reboot the affected hosts.

Note: When ever you reboot a host, you must run `symcfg discover` on all the Symmetrix devices and refresh the SYMAPI database.

Removing Meta Members

To remove meta members from the device masking VCMDDB, but keep the meta heads in place, use the following form:

```
symmaskdb -sid SymmID -meta_member remove
```

Device Masking VCMDB Maintenance

After the initial setup, records are added, updated, and deleted from the device masking VCMDB each time a SYMCLI command is issued to add or remove devices in a masked channel, a WWN /iSCSI alias is renamed, one HBA is swapped for another, or an HBA is cleared, removing its device mask allocation.

Initializing the Database

For the initial setup of any device masking environment, a device reserved (VCM state enabled) in the Symmetrix array must be initialized and formatted for use as the device masking database, better known as the VCMDB. The initialization clears the disk device of any current data in the process of formatting the database.



CAUTION

This command is rarely used. Be sure you want to zero out the device masking VCMDB before proceeding.

To initialize and clear the database device, use the following syntax:

```
symmaskdb -sid SymmID init -file BackupFilename
```

For a safeguard, you must specify a backup filename, since this command will try to write the data from this device to a backup file on your host before it clears the current data.

For example, to initialize the database and create backup file BackupDevMask1 on Symmetrix 0128, enter:

```
symmaskdb -sid 0128 init -file BackupDevMask1
```

Activating Configuration Changes

After each set of changes, the new configuration must be activated by performing a refresh (`symmask refresh`), back up the database (`symmaskdb backup`), reboot the affected hosts, and run `symcfg discover` to refresh the SYMAPI database.



CAUTION

Before running the `symmask refresh` command, make sure there are no HBAs accessing devices in the masked channel (applications running or user activity).

Viewing the Login History Table

The `symmask list logins` command is used to view the login history table. This table in the Symmetrix array lists which hosts and HBAs are logged on to a Symmetrix array for all directors and their director ports. For example for Symmetrix 6196, enter:

```
symmask -sid 6196 list logins
```

The following is sample output from this command:

```
Symmetrix ID          : 000000006196
```

```
Director Identification : FA-2A
```

```
Director Port         : 1
```

Identifier	Type	User-generated		FCID	Logged On	
		Node Name	Port Name		In	Fabric
10000000c9238053	Fibre	api145	i@1f,4000,@2	260e13	Yes	Yes
5006048000060d21	Fibre	NULL	NULL	261e13	No	Yes

The identifier field indicates which HBA is communicating with the Symmetrix array. User-generated node and port names are identified as the AWWN or AISCsi alias associated with it. Columns labelled On Fabric and Logged In indicate whether the HBA is connected to a fabric and whether it is logged in to the Symmetrix system.

You can use the verbose (`-v`) option to view the last active login information.

Refreshing Director Profile Tables

The `symmask refresh` command refreshes the WWN/iSCSI profile tables in the director cache with the latest copy of the data in the device masking VCmdb. This refreshes the host-related profile data in the Symmetrix array only. Reboot any connected hosts and run the `symmask discover hba` command to update the login history table.

Viewing the Database

You can examine the entire contents of the device masking VCmdb in its entirety, by director and port, by WWN name (or alias), or by iSCSI name (or alias) using the following syntax:

```
symmaskdb -sid SymmID | -file Filename [-v]
[-dir all [-p all] | -dir # [-p <#|all>]]
[-wwn wwn | -awwn awwn |
-iscsi iscsi | -aiscsi aiscsi]
list database
```

Example: Entire VCMDB

For example, to view the device masking VCMDB on Symmetrix 6196, enter:

```
# symmaskdb -sid 6196 list database
```

The following is sample output from this command:

```
Symmetrix ID          : 000000006196
Last updated at       : 04:58:00 PM on Tue Mar 25,2004

Director Identification : FA-2A
Director Port          : 1

User-generated
Identifier             Type   Node Name          Port Name          Devices
-----
10000000c9238053      Fibre  api145             i@1f,4000,@2       0040:0043
10000000c924e04a      Fibre  HOST.23.65.70      10000000c924e04a   00BC:00BF
                                                                00C3:00C6

Director Identification : FA-2B
Director Port          : 1

User-generated
Identifier             Type   Node Name          Port Name          Devices
-----
10000000c9238053      Fibre  api145             i@1f,4000,@2       None
```

Example: iSCSI Connected Type 4 Database

The following is sample output for a Type 4 database connected through iSCSI:

```
Symmetrix ID          : 000000006208

Database Type          : Type4
Last updated at       : 03:29:45 PM on Fri Jul 25,2004

Director Identification : SE-3A
Director Port          : 0

User-generated
Identifier             Type   Node Name          Port Name          Devices
-----
iqn.2002-06.com*       iSCSI  iSCSI              microsoft:api210    0001
                                                                0005:0007
                                                                0047
                                                                004F

Director Identification : FA-14A
Director Port          : 0
```

User-generated

Identifier	Type	Node Name	Port Name	Devices
2234567812345678	Fibre	2234567812345678	2234567812345678	0060
1234567812345678	Fibre	1234567812345678	1234567812345678	0060

Director Identification : FA-14B
 Director Port : 0

Identifier	Type	Node Name	Port Name	Devices
iqn.2002-06.com*	iSCSI	iSCSI	microsoft:api210	004F

Director Identification : FA-14B
 Director Port : 1

Identifier	Type	Node Name	Port Name	Devices
iqn.2002-06.com*	iSCSI	iSCSI	microsoft:api210	0059:005A

Example: VCMDB Records for a Director

To examine the database for records concerning director 2b, port 1 on Symmetrix 6196, enter:

```
symmaskdb -sid 6196 list database -dir 2b -p 1
```

The following is sample output from this command:

```
Symmetrix ID          : 000000006196
Last updated at       : 04:58:00 PM on Tue Mar 25,2004
Director Identification : FA-2B
Director Port         : 1
```

Identifier	Type	Node Name	Port Name	Devices
10000000c9238053	Fibre	api145	i@1f,4000,@2	None

You can examine the masked assignment of devices to a specific HBA using the following syntax:

```
symmaskdb -sid SymmID list devs -wwn wwn | -awwn awwn|-iscsi iscsi |-aiscsi aiscsi
```

For example, to examine the devices on Symmetrix 6196 to which host 10000000c9238053 has access, enter:

```
symmaskdb -sid 6196 list devs -wwn 10000000c9238053
```

The following is sample output from this command:

```
Symmetrix ID      : 000000006196
```

```
Originator Port wwn : 10000000c9238053
```

```
User-generated Name : api145/i@1f,4000,@2
```

Sym Dev				LUN					
Name	Dir:P	Physical Device Name	VBUS	TID	SYMM	HOST	Attr	Cap(MB)	
0040	2A:1	/dev/rdisk/c1t0d1s2	0	0	1	1		187	
0041	2A:1	/dev/rdisk/c1t0d2s2	0	0	2	2		187	
0042	2A:1	/dev/rdisk/c1t0d3s2	0	0	3	3		187	
0043	2A:1	/dev/rdisk/c1t0d4s2	0	0	4	4		187	

Viewing Device Capacity

You can view the capacity of devices assigned to a particular host with the following command:

```
symmaskdb -sid SymmID list capacity -host HostName
```

For example, to view the capacity of host api145 on Symmetrix 6196, enter:

```
symmaskdb -sid 6196 list capacity -host api145
```

The following is sample output from this command:

```
Symmetrix ID      : 000000006196
```

```
Host Name         : api145
```

```
Identifiers Found : 10000000c9238053
```

Device	Cap(MB)	Attr	Dir:P
0040	187		2A:1
0041	187		2A:1
0042	187		2A:1
0043	187		2A:1

```
MB Total:    748
GB Total:    0.7
```

This command requires that the first part of the HBA alias be the host name.

You can view which HBAs have been assigned to specific devices with the following command:

```
symmaskdb -sid 6196 list assignment -dev 0040:0043
```

The following is sample output from this command:

```
Symmetrix ID : 000000006196
```

Device	Identifier	Type	Dir:P
-----	-----	-----	-----
0040	10000000c9238053	FIBRE	2A:1
0041	10000000c9238053	FIBRE	2A:1
0042	10000000c9238053	FIBRE	2A:1
0043	10000000c9238053	FIBRE	2A:1

Note: The `list database` and `list devs` commands can be targeted to a backup database file on your host by replacing the `-sid` option with a `-file` option that specifies your backup filename.

Managing a Backup VCMDb File

You can create a backup file containing the current contents of the device masking VCMDb. This is useful when you want to temporarily change the access rights or device masking assignments to various HBAs. Then at some point in time, you can return the device masking environment back to the original masked environment. Often, just backing up the database on a regular basis ensures you can recover your established masked environment in the event of some improper changes or failure.

Note: You cannot reuse any existing backup filename. The forced discipline is to always create a new file.

To create a backup database file, use the following syntax:

```
symmaskdb -sid SymmID backup -file BackupFilename
```

For example, to create backup file BackupDevMask on Symmetrix 0128, enter:

```
symmaskdb -sid 0128 backup -file BackupDevMask
```

The VCMDb backup files vary in length, depending on how much information is in them.

VCMDB Database Types

Device masking database types define the number of devices per database record and the number of records you can mask.

Solutions Enabler version 5.3 and Enginuity version 5670 introduced support for a Type 4 device masking VCMDB, which expanded the existing Type 3 VCMDB option.

Beginning with Solutions Enabler version 6.0 and Enginuity version 5671, a Type 5 device masking VCMDB is supported, and Enginuity version 5771 will only support a Type 6 VCMDB. The various VCMDB types are defined as:

- ◆ **Type 3** — supports up to 8K devices per record and 32 fibre/32 iSCSI initiator records per port (the VCMDB device must be 24 cylinders or larger)
- ◆ **Type 4** — supports up to 8K devices per record and 64 fibre/128 iSCSI initiator records per port (the VCMDB device must be 48 cylinders or larger)
- ◆ **Type 5** — supports up to 16K devices per record and 64 fibre/128 iSCSI initiator records per port (the VCMDB device must be 96 cylinders or larger)
- ◆ **Type 6** — supports up to 64K devices per record and 256 fibre/512 iSCSI initiator records per port. This type of database resides in the Symmetrix File System (SFS) and is valid only with Enginuity 5771.

When initializing the VCMDB database where no database currently exists, SYMCLI defaults to creating a database according the size of the VCMDB device being initialized. For example, a Type 4 VCMDB would be created for a 48-cylinder device. This default behavior is also true for the VCMDB device that currently holds a database (for example, a Type 4 database on a 96-cylinder device will be initialized as a Type 5 database). A Type 4 or 5 database initializes with direct I/O writes blocked to protect against outside sources corrupting the database. You can also block direct I/O writes to a Type 3 database using `set no_direct_io` option.

You can explicitly create a VCMDB of a specific type in the initialization procedure. This is especially important when you are considering backwards compatibility issues. If you had a larger VCMDB device size (96 cylinders, for example), but you have a need to be compatible with Solutions Enabler 5.3, you would probably want to specify the smaller size (Type 3 or 4, for example) to maintain

backward compatibility. The following command provides an example syntax specifying a VVCMDB type:

```
symmaskdb -sid 814 init -file MyInitBackup
          -vcmdb_type 4
```

Converting a VCMDB Type

You can convert a Type 3 database to Type 4 or Type 5, and a Type 4 to a Type 5, if the size of the VCMDB device on the specified Symmetrix array is large enough for the database type. The following is an example converts the VCMDB on Symmetrix 814 to a Type 5 database:

```
symmaskdb -sid 814 convert -vcmdb_type 5 -file MyCvrtBU
```

If you convert from a lower type database to a higher type, any hosts running a Solutions Enabler version that does not support the higher VCMDB type will not be able to access the database. For example, if one host running Solutions Enabler version 6.0 converts an existing VCMDB to Type 5, another connected host running Solutions Enabler version 5.4 will no longer have access to the database until this host is upgraded to version 6.0 or higher.

Restoring a Backup VCMDB

You can restore the database from the backup file stored on the host by using the following form:

```
symmaskdb -sid 0128 restore -file MyCvrtBU
```

The database is restored as is; Type 3 restores to Type 3, and Type 4 restores to Type 4. You can use the `convert` or `set` options to alter the resulting environments.

To restore the database from a backup file, but not the authentication information, enter:

```
symmaskdb -sid 0128 restore -file MyCvrtBU
          -skip_authentication
```

Restore a Backup and Convert its Type

To restore from a backup file and convert its database type in a single command specify the `-vcn_type` option and specify the type: 4 or 5. For example , enter:

```
symmaskdb -sid 0128 restore -file MyCvrtBU -vcn_type 5
```

Blocking Direct Writes to the VCMDb

If you have a Type 3 database and would like to block direct writes to the database, use the following form:

```
symmaskdb -sid SymmID set -no_direct_io
```

By setting this, you are indicating that hosts running SYMCLI versions prior to version 5.3 will not be able to write to the database.

If your environment is running Solutions Enabler SYMCLI Version 5.3 (or higher) and Enginuity 5670, enabling this attribute will provide additional security to your database.

Type 4 and 5 databases initialize with direct IO writes blocked by default.

HBA Initiator Management

In the event a host adapter fails, or needs replacement for any reason, you can replace the adapter and assign its set of devices to a new adapter by using the `replace` action in the following form:

```
symmask -sid SymmID -wwn wwn|-awwn awwn|-iscsi
iscsi|-aiscsi aiscsi replace wwnNew | iscsiNew
```

To swap HBAs, it is suggested to:

1. Run `symmask list logins` to view the old WWN/iSCSI HBAs.
2. Swap HBA boards.
3. Run `symmask list hba` or `discover` to view the new initiator (for example WWN).
4. Run `symmask replace` to substitute a new WWN for all occurrences in the database of the old WWN.
5. Run `symmask discover` to establish the new names in the history table, or run `symmask rename` to assign an AWWN to the new HBA in both the database and the history table.
6. Run `symmask refresh` to update the director profile tables (in cache) from the database.

Deleting HBA Associations

You can also delete (in the database) the set of devices associated to a host adapter by using the `symmask delete` action with the following syntax:

```
symmask -sid SymmID delete -wwn wwn|-awwn awwn|\
-iscsi iscsi|-aiscsi aiscsi
```

For this database record deletion, you can restrict the action to just devices on a specific Symmetrix director and port with the following option:

```
[-dir #|all -p #|all]
```

In addition, you can use the `-login` option to delete the entry from the login history table.

Fibre Channel-to-Host Interface Management

Using the device masking commands, you can adjust the protocol characteristics of the Fibre Channel-to-host interface to be compatible with your host platform-specific requirements.

For your specific host communication protocol, the `symmask set` command allows an *advanced* user to adjust the following attributes on a host adapter port basis:

- ◆ Fibre Channel ID (FCID) lock down
- ◆ Device LUN visibility
- ◆ LUN base/offset skip
- ◆ Heterogeneous host configuration

A record for the host adapter port assignment must already exist in the VCMDB for these channel attributes to be set.



CAUTION

Do not proceed with any of these adjustments unless you are comfortable with your understanding of the details of your HBA interfaces. Improper settings can disable the use of your host with the Symmetrix array.

Locking Down a Fibre Channel ID

Fibre Channel ID (FCID) lockdown is a security feature (with Engenuity 5x66 minimum) that limits host device access by adding Fibre Channel ID information of a switch within a fabric to device access records in the device masking VCMDB. This feature handles WWN spoofing and the threat it poses to your networked systems in a shared (same director port) storage port configuration.

For example, to implement the Fibre Channel ID lockdown feature on Fibre Channel 021300 for director 16A, port 0, enter:

```
symmask -sid 018 set lockdown on 021300  
-awwn SolarB/1f,0,fca@1,0 -dir 16A -p 0
```

This feature lets you set the Fibre Channel ID (FCID) of the WWN of the HBA you want to protect. The FCID is then added to the database record for the WWN of the specified HBA with the specified director and is locked. Once a Fibre Channel ID is locked, no user with a spoofed WWN can log in. If a user with a spoofed WWN is already logged in, that user loses all access through that HBA.



CAUTION

When an HBA logs into a director port, the Fibre Channel ID accompanies it, telling the director port where to send its response. By specifying Fibre Channel ID information of the switch (in addition to the WWN of the HBA in the device masking record), the valid physical path through the SAN for a particular HBA is locked down. Only an HBA with a Fibre Channel ID that matches the FCID specified in the device masking record is able to log in to the storage port. If the incorrect Fibre Channel ID is added to the device masking VCMDB, that HBA will lose access and the host utilities may hang on the server with the locked out WWN. It is recommended that at least two HBAs be available on the administrator host. If one HBA becomes locked out, the host will have access through the other HBA and can correct the record in the database.

Lockdown Steps

To find the Fibre Channel ID, lock it down, verify that it is locked down, and then force the change to take effect, use the following procedure:

1. Find the WWN. If the device for the device masking VCMDB is visible, run `symmask list hba` to find the device path of the HBA you want to protect.

Note: If the VCMDB is unmapped, no PDEVs will be visible whe the `symmask list hba` command is issued. The `sympd` command must be called to set an alternate path.

2. Find the Fibre Channel ID value by using one of the following methods:
 - Run `symmask list logins -pdev`, specifying the device path you found in step 1, to find the Fibre Channel ID of the WWN of the HBA you want to protect.
 - Find the Fibre Channel ID value on the switch (refer to *Finding the FCID of a Switch* on page 3-23).
3. Run `symmask set lockdown` set to on with the FCID of the Fibre Channel ID you found in step 2.
4. Run `symmaskdb list database` in verbose mode (`-v`) to verify that the Fibre Channel ID is locked down.

5. Either reboot the host or pull the cable from the director and then replace the cable. This causes the change to take effect. If you reboot, you must run `symcfg discover` to refresh the SYMAPI database.

Effects on Other Commands

This section describes how locking down a Fibre Channel ID affects other commands:

- ◆ `symmask delete`—Locking down a Fibre Channel ID has no effect on the `delete` action. The specified record is completely cleared from the database.
- ◆ `symmask replace`—Locking down a Fibre Channel ID has no effect on the `replace` action when the cable is simply moved from one HBA to another and not moved at the switch. In this case, the Fibre Channel ID value that is already in place in the database remains the same for the new HBA.

However, if the cable is moved from one port on the switch to another, the FCID value changes. Do not unlock the Fibre Channel ID during this swap. Instead, leave at least one path open to the database device, and reset the FCID value after the swap by recalling the `set` action.

Since you do not have a path from the HBA whose Fibre Channel ID you want to lock down, you cannot use `symmask list logins` to find the FCID value. Instead you must obtain the FCID value from the switch.

Finding the FCID of a Switch

This section describes how to find the Fibre Channel ID on Connectrix™ and Brocade switches:

- ◆ Connectrix switch: Through the hardware view, click the board and then the port of the switch whose Fibre Channel ID you want to find. Right-click to display the port properties window that includes the FCID value.
- ◆ Brocade switch: Telnet to the switch and run `nsShow`. Look for the PID value of the WWN of the HBA you want to protect, which is the Fibre Channel ID value.

Format of a FCID

The Fibre Channel ID basically incorporates the port and the domain ID of the switch in the fabric into which the HBA is plugged.

Connectrix ED-1032 and Brocade 1000 series:

2 2 0 4 1 3

Underlined text is the domain. ***Bold Italic text*** is the port.

In this example, the domain is 2 and the port is 04.

For Connectrix, the port is offset by 4.

Brocade 2000 series DS-16B:

0 2 1 3 0 0

Underlined text is the domain. ***Bold Italic text*** is the port.

In this example, the domain is 02 and the port is 3.

Setting Device LUN Visibility

The device LUN visibility feature allows the host driver to discover devices with noncontiguous LUN addresses. During the process of discovery, the host operating system scans for LUNs starting at 000 and continuing to a point where it does not find a LUN in the sequence. If there is no LUN 000 on the target director, or there is a break in the sequence of LUNs on that target, some operating systems do not detect the remaining LUNs and fail to discover noncontiguous devices.

The `symmask set visibility` command lets your host see all these devices. When you set visibility on, all devices attached to the specified Fibre Channel director are made available to the HBA and respond to the SYMCLI. The following command example turns on the device visibility on director 16A, port 0 when working with host SolarB:

```
symmask -sid 018 set visibility on -dir 16A -p 0
      -awwn SolarB/1f,0,fca@1,0
```

Setting the LUN Base/Offset Skip Adjustment

Certain host platforms require LUN 000 to be present when it scans the interface for devices. Also, these host types and others cannot see devices beyond the initial contiguous LUN sequence (they cannot skip over masked holes in an array of intended devices). In a device masking environment, this can be a problem when you need to mask out certain devices from the visibility range of certain host platforms.

For these host platforms, the device masking LUN base/offset skip adjustment feature (with 5x68 minimum) provides the ability to specify a LUN *base* and an *offset* hexadecimal value for the skip hole (recorded in the database). When the host asks for a LUN that is equal to, or greater than the skip hole base value, the offset is added to the LUN value requested by the host to render the actual LUN (device) in the Symmetrix array. The *base* value is essentially the host's first missing LUN in the skip hole. The *offset* is the hole size (number of addresses needed to skip over the hole).

To set LUN base and offset values for a skip hole within an HBA to director channel, use the following syntax:

```
symmask -sid SymmID set lunoffset on offset base \
        -awwn awwn -dir # -p #
```

For example, (via director 16A/port 0) to make LUNs (devices) 005 through 008 available to host HPB03/1, you need a LUN base address of 000 and an offset of 5 (to skip over 000-004):

```
symmask -sid 018 set lunoffset on 5 0 \
        -awwn HPB03/1 -dir 16A -p 0
```

Multiple Hosts and Broken Sequences

When you have multiple hosts that have the LUN mapping problems with broken sequenced arrays of devices, you need to implement these broken arrays with the `set lunoffset` action for each host.

As shown in Table 3-3 for Scenario 1, you could have LUN devices 000 through 006 assigned to Host A and 007 through 00A assigned to Host B. Because in this case, Host B needs to see LUN 000 first, you would have to set `lunoffset on` with a base value of 000 and an

offset of 7. For this case, Host A does not have a problem since there is no hole in its assigned device sequence and it starts with 000.

Table 3-3 LUN Base/Offset Scenarios for Multiple Hosts with Skip Holes

	Host A LUNs	Host B LUNs	<i>base</i>	<i>offset</i>
Scenario 1	000-006		-	-
		007-00A	000	7
Scenario 2	000-002		-	-
	007-008		003	4
		003-006	000	3

For Scenario 2, you could have LUNs 000 through 002 and 007 through 008 assigned to Host A. Host B could have LUNs 003 through 006. Host A's 000-002 is not a problem, but LUNs 007-008 require a skip hole base value of 003 (because the first visible sequence stopped at 002) and an offset of 4 (hole size). Also, Host B's LUNs 003-006 requires a skip base value of 000 and an offset of 3. This scenario would require two commands: one targeting Host A and one targeting Host B. Only one skip hole per HBA channel can be recorded in the database.

Setting the Heterogeneous Host Configuration

Heterogeneous host configuration is a feature (with Enginuity 5x68 minimum) that allows different host types to share a single director port even though they may require different port settings for their distinctive interface protocol.

Turning on heterogeneous host enables that record to override the current port flag settings on the given director/port (for the given WWN or iSCSI), concerning the host interface characteristic and protocol. If this feature is enabled for one host type for a WWN, it must be disabled for that WWN before a new host type can be assigned.

This feature can be used in conjunction with the LUN offset skip feature to allow the different hosts their own LUN addressing scheme. With that scheme, the devices they see are different from those seen by any other host on the director.

The following syntax is used to set certain heterogeneous host configuration flags to optimize the host-to-director interface:

```
symmask -sid SymmID -wwn wwn -dir # -p #
set heterogeneous on HostConfigFlag
```

Possible *HostConfigFlag* values are listed in the last column of Table 3-4.

Table 3-4 Host Platforms and Interface Configuration Flags

Host Platform	Requirements	Bit ^a	Host Configuration Flag (<i>HostConfigFlag</i>)
AS/400		AS4	AS400
AS/400	Load source extender	AS4, V	AS400_LSE
Bull Escala/AIX			BULL_AIX
Bull Escala/AIX	PowerPath® V1.5.x or earlier	D	BULL_AIX_PP15
HP/DEC AlphaServers Tru64 UNIX 5.x FC-SW		OVMS	DEC_UNIX
HP/DEC OpenVMS		SC3, OVMS	DEC_OVMS
Data General AViiON NUMA 25000 Server		D	DG_AViiON
FSC BS2000/OSD Servers		C, D	FSC_2000
FSC PRIMEPOWER GP7000F Series host			PRIMEPOWER
FSC PRIMEPOWER GP7000F Series host	PowerPath V1.5.x or earlier	D	PRIMEPOWER_PP15
FSC PRIMEPOWER GP7000F Series host	VERITAS DMP	C, D	PRIMEPOWER_DMP
Fujitsu Services ICL Open VME		C	ICL_OPEN
Hewlett-Packard HP-UX		C, V	HP_UX
IBM AIX with FC 6227, 6228, 6239		SC3	IBM_AIX
IBM AIX with FC 6227, 6228, 6239	PowerPath V1.5.x or earlier	SC3, D	IBM_AIX_PP15
IBM AIX with FC 6227, 6228, 6239		C, SCS	IBM_AIX_DMP
IBM AIX with FC 6227, 6228, 6239		C, D, SCS	IBM_AIX_DMP_PP15
IBM AIX with EMC Fibre Channel			IBM EMC
IBM AIX with EMC Fibre Channel	PowerPath V1.5.x or earlier	D	IBM EMC_PP15
Linux			LINUX
Linux		C	LINUX_DMP

Table 3-4 Host Platforms and Interface Configuration Flags (continued)

Host Platform	Requirements	Bit ^a	Host Configuration Flag (HostConfigFlag)
NCR MP-RAS/Windows NT			NCR
NCR MP-RAS/Windows NT	Multiple vendor platforms	D	NCR_MP
NCR MP-RAS/Windows NT	If Windows NT is used with TNT, set FBA Env. Sense key to 4; otherwise, set it to 6	E	NCR_NT
NCR MP-RAS/Windows NT	Multiple vendor platforms: If Windows NT is used with TNT, set FBA Env. Sense key to 4; otherwise, set it to 6	D, E	NCR_NT_MP
Novell NetWare			NOVELL
Novell NetWare	Cluster	D	NOVELL_CLUSTER
Windows NT/Windows 2000			WINDOWS
Windows NT/Windows 2000	PowerPath V1.5.x or earlier	D	WINDOWS_PP15
Windows NT/Windows 2000	HP/Agilent controllers	V	WINDOWS_HP
Windows NT/Windows 2000	PowerPath V1.5.x or earlier, HP/Agilent controllers	D, V	WINDOWS_HP_PP15
Windows NT/Windows 2000	VERITAS VxVM DMP	C	WINDOWS_DMP
Windows NT/Windows 2000	HP/Agilent controllers VERITAS VxVM DMP	C, V	WINDOWS_HP_DMP
Windows NT/Windows 2000	PowerPath V1.5.x or earlier, VERITAS VxVM DMP	C, D	WINDOWS_DMP_PP15
Windows NT/Windows 2000	HP/Agilent and PowerPath V1.5.x, VERITAS VxVM DMP	C, D, V	WINDOWS_HP_DMP_PP15
Sequent NUMA-Q		E, C, SEQ	SEQUENT
Sequent NUMA-Q	FC-SW configurations only	E, C, SEQ, V	SEQUENT_FCSW
FSC Reliant UNIX RM series		E, D, S	RELIANT
Sun			SOLARIS
Sun	PowerPath V1.5.x or earlier	D	SOLARIS_PP15

Table 3-4 Host Platforms and Interface Configuration Flags (continued)

Host Platform	Requirements	Bit ^a	Host Configuration Flag (<i>HostConfigFlag</i>)
Sun	VERITAS DMP	C, D	SOLARIS_DMP
Sun	Sun Cluster (ealier than 3.0)	C, D, SCL	SUN_CLUSTER
Sun	Sun Cluster (3.0 or later)	C	SUN_CLUSTER30
VERITAS Cluster (VCS), EMC GeoSpan for VCS		D	VERITAS
VERITAS Cluster (VCS), EMC GeoSpan for VCS	VERITAS DMP	C, D	VERITAS_DMP
VERITAS Cluster (VCS), EMC GeoSpan for VCS	VSC 2.0 or later		VERITAS20
VMWare		C, SCS	VMWARE

a. The following defines the host characteristic for each of the bits used in the table:

AS4	AS/400 secondary port
C	Common serial number for multipaths
D	Disable Queue Reset on Unit Attention (UA)
E	Environmental reports to host from Symmetrix
S	Enable Siemens host RM/400 - RM/600
SCL	Enable Sunapee (for Sun PDB clusters)
SC3	SCSI 3 interface
SEQ	Sequent Host (DYNIX/ptx)
OVMS	OpenVMS Fibre connection
V	Enable volume set addressing

A

- adding devices 3-8
- ASCII World Wide Names (AWWN)
 - establishing 3-6
 - format 3-7
 - usage 3-7

B

- backup file
 - creating a database 3-16
- Brocade switch
 - finding the FCID for 3-23

C

- CHAP
 - configuring 2-6
 - for iSCSI 1-6
- configuration
 - identifying 3-4
- Connectrix switch
 - finding the FCID for 3-23
- conventions 1-x

D

- device LUN visibility 3-24
- device masking
 - architecture 1-2
 - configuration steps 3-3
 - functionality 1-2
- device masking database
 - activating a new configuration 3-5
 - backup file for 3-16

- blocking direct writes to 3-19
- discover 1-9
- examining 3-11
- external lock, releasing 1-9
- initializing 3-10
- maintenance 3-10
- restore and convert 3-18
- restoring 3-18
- security for 1-7
- using syscalls with 1-8

devices

- adding 3-8
- capacity of 3-14
- removing 3-9

director ports

- identifying 3-4

directors

- refresh 3-11

discover

- using 1-9

E

- external lock
 - on VCMDB 1-9

F

- Fibre Channel ID (FCID)
 - finding the FCID 3-23
 - for Brocade switch 3-23
 - for Connectrix switch 3-23
 - format 3-24
 - lock down 3-21
 - lock down effects on commands 3-23

lock down procedure 3-22

H

HBA

- alias names 3-6
- management 3-20
- supported initiators 1-6
- swapping 3-20

heterogenous host configuration 3-26

I

identifiers, determining 3-4

iSCSI

- configuring the software driver for 2-4
- support requirements 2-5
- topology 1-6
- with CHAP authentication 2-6
- without CHAP authentication 2-14

L

lock

- on VCMDB 1-9
- releasing 1-9

login history table

- contents 3-11
- usage 3-6

LUN

- skip hole 3-25
- visibility 3-24

LUN offset

- hexadecimal value 3-25

M

masked channel 1-2

meta devices 3-8

meta members

- removing from the database 3-9

P

profile tables 3-11

R

refresh directors 3-11

removing devices 3-9

restoring a database 3-18

S

SCSI writes

- blocking from the database 3-19

security

- CHAP protocol 1-6

skip hole

- hexadecimal value 3-25
- LUN base/offset 3-25

symcfg actions

- list all 3-4

symmask

- command overview 1-10

symmask actions

- add dev 3-4
- list hba 3-4
- list hbas 3-4
- list logins 3-4

symmaskdb

- command overview 1-10

symmaskdb actions

- backup 3-16
- init 3-4, 3-10
- list database 3-11

V

VCMDB. See device masking database

visibility

- devices 3-24

Volume Logix

- command conversion 1-12

W

World Wide Name (WWN) 3-6

- identifying 3-4

- profile tables 3-11