

**EMC Solutions Enabler
Symmetrix Access Control CLI**
Version 6.0

PRODUCT GUIDE

**P/N 300-000-879
REV A07**

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, copying, and 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 Access Control

Symmetrix Access Control Operations Overview	1-2
Access Control Command Summary	1-3
Access Control Database	1-4
How to Create or Modify Access Control Data.....	1-6
Command File Execution	1-6
Minimum Access Control Configuration.....	1-7
Initial ACL Setup	1-8
How to Create and Manage Access Groups	1-9
Setting Up an Access Group	1-9
User Access IDs (PINs) for the AdminGrp	1-10
Editing and Managing an Access Group	1-11
How to Create and Manage Limited Access to Access Pools .	1-13
Setting Up Access Pools.....	1-13
Editing and Managing Access Pools.....	1-14
How to Create and Manage Access Control Entries.....	1-16
How to Obtain Access Control Information	1-20
How to Release Pending Locked Sessions	1-22
Grant/Deny Access Strategies.....	1-23
Initially Grant All Rights to Everybody	1-23
Granting and Denying Default and Legacy Access.....	1-23
BCV Setup Strategy	1-25
TimeFinder/Snap Setup Strategy.....	1-26
SRDF Setup Strategy	1-26
How to Backup and Restore the Access Control Database.....	1-27
Create a Backup File.....	1-27
Restore the Backup File to the Access Control Database..	1-27

Index..... i-1

Figures

1-1	ACLs and ACEs in the Symmetrix Access Control Database	1-4
1-2	An Access Controlled Symmetrix Site	1-5
1-3	Creating Access Pools	1-13
1-4	Removing Devices from a Pool	1-15

Tables

1-1	Symmetrix Access Control Command Summary	1-3
1-2	Initial Access Groups Set	1-7
1-3	Initial Delivered ACLs Setup	1-8
1-4	Access Types to Specified Devices	1-16

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 EMC 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 EMC 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 Access Control SYMCLI commands.

Organization The manual describes how to set up an access control environment and execute certain access control operations on your Symmetrix resources and user restrictions using the SYMCLI commands of the EMC Solutions Enabler software. The following defines the structure of this manual:

Chapter 1, *Access Control*, describes how to set up access control mechanisms and update the access controls on the Symmetrix environment, using SYMCLI.

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 Installation Guide*, EMC Corporation
- ◆ *EMC Solutions Enabler Symmetrix Base Management CLI Product Guide*, EMC Corporation
- ◆ *EMC Solutions Enabler Symmetrix Device Masking CLI Product Guide*, EMC Corporation
- ◆ *EMC Solutions Enabler Symmetrix SRDF Family CLI Product Guide*, EMC Corporation
- ◆ *EMC Solutions Enabler Symmetrix TimeFinder Family CLI Product Guide*, EMC Corporation
- ◆ *EMC Solutions Enabler Support Matrix*

Conventions Used in this Manual

The following conventions are used in this manual:

In this manual, every use of the word SYMCLI means EMC Solutions Enabler.

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 Web site 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.

Your technical enhancement suggestions for future development consideration are welcome. To send a suggestion, log on to **<http://powerlink.emc.com>**, follow the path **Support, Contact Support**, and choose **Software Product Enhancement Request** from the Subject menu.

This chapter describes how to set up access control mechanisms and how to perform Symmetrix access control actions using SYMCLI.

- ◆ Symmetrix Access Control Operations Overview1-2
- ◆ How to Create and Manage Access Groups1-9
- ◆ How to Create and Manage Limited Access to Access Pools....1-13
- ◆ How to Create and Manage Access Control Entries.....1-16
- ◆ How to Obtain Access Control Information1-20
- ◆ How to Release Pending Locked Sessions1-22
- ◆ Grant/Deny Access Strategies1-23
- ◆ How to Backup and Restore the Access Control Database.....1-27

Symmetrix Access Control Operations Overview

Today, anyone with access to Symmetrix-based management software can execute any function on any Symmetrix device. Many product applications such as EMC® ControlCenter™, TimeFinder®, SRDF®, Optimizer®, Resource View, Database Tuner, and various ISV products can issue management commands to any device in a Symmetrix® complex. Open systems hosts can manipulate mainframe devices, Windows hosts can manipulate UNIX data, and vice versa.

Shared systems, such as these, may be vulnerable to one host, accidentally or intentionally, tampering with another's devices. To prevent this, the `symacl` command can be used by an administrator of the Symmetrix storage site to set up and restrict host access to defined sets of devices (access pools) across the various Symmetrix arrays.

Access Control Command Summary

This SYMCLI component supports Symmetrix access control requirements. The access control command allows you to set up and maintain an access controlled environment over the Symmetrix resource (access pools). The command (`symacl`) sets up access control mechanisms and changes access control entries in the access control database.

Table 1-1 provides a summary of Symmetrix access control command operations:

Table 1-1 Symmetrix Access Control Command Summary

Command	Description
<code>symacl</code>	Performs management operations on the Symmetrix access control environment. Possible operations are: • Lists all access control entries (ACEs), access pools, or access groups. • Shows the state of the access control environment on a Symmetrix. • Shows detailed information about the access group or pool. • Releases or aborts any pending access control session lock. • Previews or verifies the contents of the command file for proper syntax and correctness. • Prepares or checks the command file for appropriateness of the requested access control entry against the current state of the Symmetrix array. • Commits all access control commands as entries to the access control database. • Backs-up the access control database for the specified Symmetrix to the specified file. • Restore the contents of the access control database with the contents of the specified file.

For more information about the syntax of the `symacl` command, refer to the *EMC Solutions Enabler Symmetrix CLI Command Reference*.

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

Access Control Database

A Symmetrix-based access control database (shown in Figure 1-1) contains all the mechanisms or information to govern access to Symmetrix access pools.

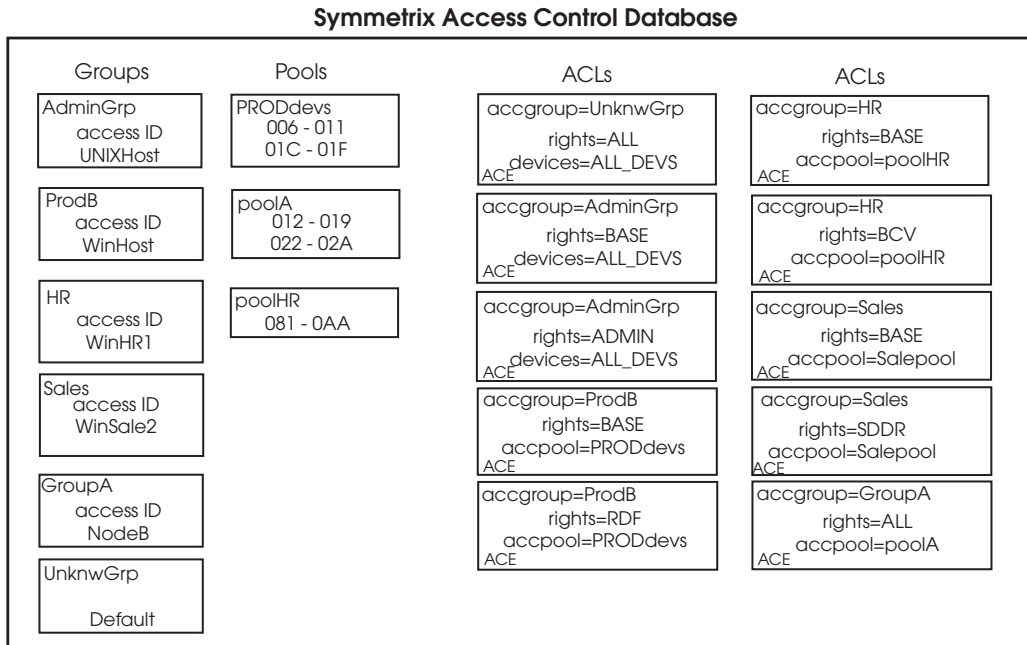


Figure 1-1 ACLs and ACEs in the Symmetrix Access Control Database

Information about the following access control mechanisms comprise the access control database:

- ◆ **Access control groups** — Unique *access IDs* and *names* are assigned (together) to hosts and then sorted into access control *groups* according to similar needs (determined by an Administrator). Access groups are allowed to act on access pools based on *rights (access types)* granted by the Administrator. *The unique host ID for open systems can be viewed by running symacl -unique.*
- ◆ **Access pools** — Access rights (types), such as BCV, SRDF, ADMIN, give permission to a host to perform certain Solutions Enabler functionality on a specified set of devices. These sets of devices are referred to as access pools or `accpool`.

- ◆ **Access Control Entries (ACES)** — Once the group and access pool mechanisms are established, the *access control entries* (ACEs) are created, which grant access rights to these pools. The ACEs of the various access groups (along with groups and pools) are managed and stored in the access control database.
- ◆ **Access Control Lists (ACLs)** — A group of ACEs that are associated with the same group. For example, in Figure 1-1, the ACEs that are associated to group HR comprise an ACL in the database.

Figure 1-2 illustrates a Symmetrix site that is managing the access rights of various types of host connections to the Symmetrix devices. Each Symmetrix has its own access control database, which are separately managed by `symacl`.

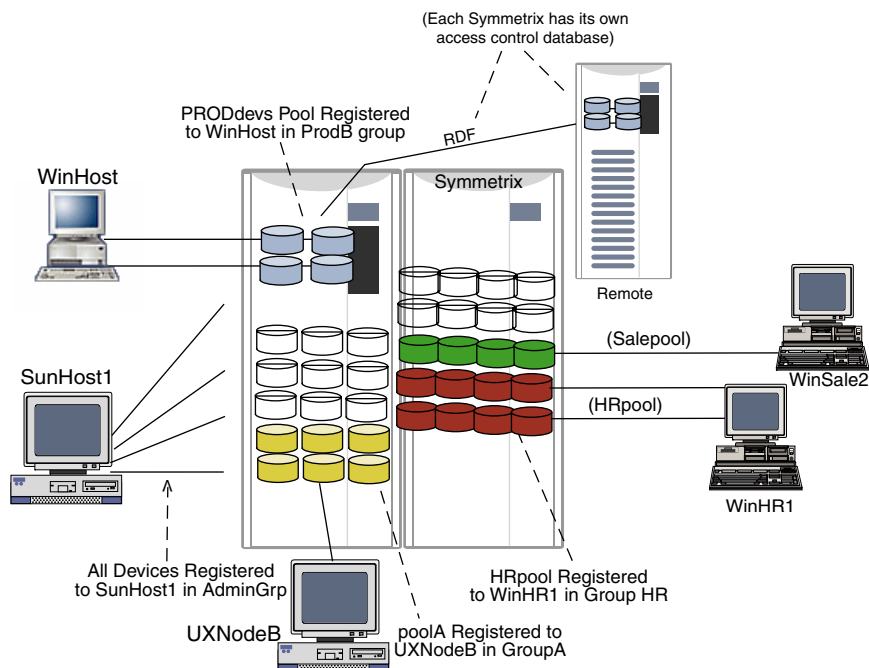


Figure 1-2 An Access Controlled Symmetrix Site

How to Create or Modify Access Control Data

To create or change the access control information in the database, you need to enter the changes in a command file and eventually commit the file to the access control database.

The command file format contains various command entries terminated with a semicolon (;). The command syntax is parsed case insensitive, but any variable parameter entered must be case sensitive.

The following are various types of rights creation and changes possible in the command file:

- ◆ Create new access groups
- ◆ Add and remove access IDs to access groups
- ◆ Move an access ID from one group to another
- ◆ Create new access pools
- ◆ Add and remove devices to access pools
- ◆ Delete access pools and access groups
- ◆ Add ACEs to grant access
- ◆ Remove ACEs to deny access

Command File Execution

To safely apply any of these access control actions (command file entries) to the access control database, you should perform the following progressive `symacl` operations on the command file:

- ◆ Preview
- ◆ Prepare
- ◆ Commit

After you first create the command file, the *preview* operation verifies the syntax and correctness of the contents of the entries in the command file.

The *prepare* operation (also before you commit) performs the preview checks but also verifies the appropriateness of the requested access control modifications against the current state of the access control database in the Symmetrix array.

The *commit* operation performs both the preview and prepare checks and then commits the contents of the command file to the Symmetrix access control database.

Note that it is not mandatory to execute a preview or prepare action prior to a commit. However, these actions can ensure that the commit action will not be rejected or can be used to debug the command file entries.

Minimum Access Control Configuration

Typically, following initial delivery and set up of a Symmetrix array on a site, an EMC Engineer will need to set some minimal access control parameters to enable you to begin administrative actions, such as the following example:

Table 1-2 Initial Access Groups Set

Access Groups	ID Names
AdminGrp	SunHost1 ACCPIN
UnknwGrp	unknown

The name `SunHost1` shown in the table above (associated with `AdminGrp`) is the ID name that designates the machine from which you administer access controls. In order to perform prepare, commit, and release actions, an access ID (PIN) with the name `ACCPIN` was created in the delivered setup. This ID name is also used for the value setting of `SYMCLI_ACCESS_PIN`. For more information, see *How to Create and Manage Access Groups*.

As shown in the following table for a delivered setup, access group `AdminGrp` has access to all devices (`ALL_DEVS`) and this group was granted both `ADMIN` and `ALL` rights. Also in the initial setup, a group called `UnknwGrp` is established with rights to all devices in the Symmetrix. At the outset of system usage, this gives all unknown hosts `BASE` rights to all devices (`ALL_DEVS`) until such time it becomes clear as to what restrictions should be established.

Initial ACL Setup

The initial `UnknwGrp` setup also grants ALL rights to any devices not already assigned to a pool (!INPOOLS).

Table 1-3

Initial Delivered ACLs Setup

Access Groups	Rights (access types)	Access Pools
AdminGrp	ADMIN ALL	ALL_DEVS
UnknwGrp	BASE	ALL_DEVS
UnknwGrp	ALL	!INPOOLS

Note: The access type ALL excludes ADMIN privileges.

VLOGIX Behavior

During initial setup of the system the access group `UnknwGrp !INPOOLS ALL` is present, as shown in the table above. In this scenario, the VLOGIX privilege returns as true since you are granted access to all devices in the Symmetrix access. Initially, since no pools are present the VLOGIX privilege is associated implicitly with all devices by this ACL.

Once a user creates an access pool and adds a device to it, the VLOGIX privilege is no longer implicitly associated with all devices and, therefore, a check for the VLOGIX privilege would now fail. In order for the `UnknwGrp` to still have VLOGIX privilege, that privilege must be explicitly granted to the `UnknwGrp` and associated will `ALL_DEVS`.

How to Create and Manage Access Groups

Typically various sets of users tend to use the same applications that utilize common Solutions Enabler features from a given host. They typically require the same device resources and rights of access to these shared devices. For this reason, hosts are registered in groups identified with a group name, which serves as a root for all ACEs in the group (see Figure 1-1 on page 1-4).

Access groups contain groups of access IDs and their ID names. Any ID and name must belong to just one group and are entered into the database together.

For ease of management, it is highly recommended that you choose an access ID name that best associates with the particular host in use. For example, SunHost1 is more appropriate than a name such as JRSMITH.

Once the group is created, the group name can be used to create access control entries (ACEs).

Setting Up an Access Group

To set up an access control group, you need to create a group and then add the various access IDs of the hosts as members of that group.

Initially, you can check to see if the host you are using has the administrative authority to make access control changes using the following command:

```
symacl list -v [-sid SymmID|ALL]
```

Create a Group

For example, in the command file (**addnewgroups.cmd**), to create access groups named HR and Sales in Symmetrix 12345, enter:

```
create accgroup HR;  
create accgroup Sales;
```

You can now commit the file or wait until you have added access IDs to the group. To commit the file (**addnewgroups.cmd**) that executes the creation of the groups, enter:

```
symacl -sid 12345 commit -file addnewgroups.cmd
```

At this point, you may be prompted for your 4 - 12 character access PIN (if environment variable SYMCLI_ACCESS_PIN is not already set to this PIN value).

Add Host Access IDs to a Group

To add a host access ID to an access group, use the following command in the command file:

```
add host accid Id name IdName to accgroup GroupName;
```

For example, in the command file (**addnewgroups.cmd**), to add WinHost with an encrypted ID 73900158-06174491-16225515 to the ProdB group, enter:

```
add host accid 73900158-06174491-16225515 name WinHost
to accgroup ProdB;
```

Also in this example, add UXNodeB with encrypted ID 73900158-06174491-16225515 to the group GroupA, enter:

```
add host accid 23300178-56078991-00665410 name UXNodeB
to accgroup GroupA;
```

Note that to preserve access ID security for any host, host IDs are encrypted. Use `symacl -unique` to get this encrypted value.

Then you must commit the file (**addnewgroups.cmd**) to execute the addition of these IDs to their groups (and any create group entries if you have not already committed them):

```
symacl -sid 12345 commit -file addnewgroups.cmd
```

User Access IDs (PINs) for the AdminGrp

A user access ID is a 4 - 12 character PIN that allows a host to perform commit, prepare, or release operations as the AdminGrp. When a host attempts a commit, prepare, or release operation as the AdminGrp, `symacl` will prompt for this PIN.

To change the user access ID for the AdminGrp access group, use the following command syntax in the command file:

```
add user accid Id name IdName to accgroup AdminGrp;
```

For example, in the command file (**addnewgroups.cmd**), to change the administrative user access ID for JOEPIN to 1234PIN, enter:

```
add user accid 1234PIN name JOEPIN to accgroup
AdminGrp;
```

User access ID's may only be set for the AdminGrp access group. Setting an ID for other groups will not return an error, nor prompt for a PIN in most scenarios.

If a host is ever prompted for a PIN, the host should enter 1234PIN. The **addnewgroups.cmd** file must be committed to execute the addition of these new IDs:

```
symacl -sid 12345 commit -file addnewgroups.cmd
```

Editing and Managing an Access Group

Once access groups are established, you can remove access IDs or ACEs from a group, move IDs from one group to another, or delete an entire group.

Remove an Access ID from a Group

To remove an access ID from an access group, use the following command syntax in the command file:

```
remove accid name IdName from accgroup GroupName;
```

For example, in the command file (**removeaces.cmd**), to remove user HRUser2 from the HR group, enter:

```
remove accid name HRUser2 from accgroup HR;
```

At some point, you must commit the file (**removeaces.cmd**) to execute the removal of this ACE from group HR.

Move an Access ID to Another Group

To move an access ID from one access group to another, use the following command syntax in the command file:

```
move accid name IdName to accgroup GroupName;
```

For example, in the command file (**moveaces.cmd**), to move user HRUser1 to GroupA, enter:

```
move accid name HRUser2 to accgroup GroupA;
```

Then you must commit the file (**moveaces.cmd**) to execute the move of this ACE to GroupA.

Remove all ACEs from a Group

To remove all ACEs from an access group, use the following command syntax in the command file:

```
remove aces from accgroup GroupName;
```

For example, in the command file (**removeaces.cmd**), to remove all ACEs from the HR group, enter:

```
remove aces from accgroup HR;
```

At some point, you must commit the file (**removeaces.cmd**) to execute the removal of the ACEs from group HR.

Delete a Group

To delete an access group from the database, use the following command syntax in the command file:

```
delete accgroup GroupName [remove_aces=true];
```

Note that when you need to delete a group you either must have removed all ACEs from the group or you can optionally remove all ACEs with the [remove_aces=true] option within this delete command.

For example, in the command file (**deletegroup.cmd**), to delete group HR and any registered ACEs in that group, enter:

```
delete accgroup HR remove_aces=true;
```

At some point, you must commit the file (**deletegroup.cmd**) to execute the removal of access group HR.

How to Create and Manage Limited Access to Access Pools

Access pools are groups of devices controlled by access groups. When the various Symmetrix devices used by a host application must function as non-shareable resources, the target devices must be identified and assigned into an access pool for protection. Once an access pool is created, the pool can be a target to create access control entries (ACEs). More than one access group can access a pool with different rights. For example, group AdminGrp might access PoolA with ALL rights, while group HR could access the same PoolA with just BASE rights.

Note: Once an access pool is created, any host in the access group UnknwGrp is denied access to `symmaskdb list database` commands. In addition, when a host in UnknwGrp calls the `symmaskdb list database` command, only its own devices will be returned in the list. To provide hosts in access group UnknwGrp with full access to the `symmask` commands, grant the access type VLOGIX to access group UnknwGrp. For more information on granting access types, refer to *Grant Rights to an Access Group* on page 1-16

Setting Up Access Pools

You can create an access pool and add devices to a pool.

Initially, you can check to see if the host you are using has the administrative authority to make access control changes using the following command syntax:

```
symacl list -v [-sid SymmID|ALL]
```

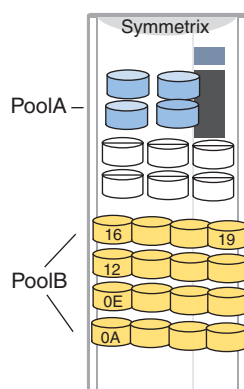


Figure 1-3 Creating Access Pools

Create a Pool

In this example, 16 devices are assigned to PoolB.

For example, in the command file (**addnewpool.cmd**), to create a access pool named PoolB in Symmetrix 12345, enter:

```
create accpool PoolB;
```

You can now commit the file or wait until you have added devices to the pool. To now commit the file (**addnewpool.cmd**) to execute the creation of the pool, enter:

```
symacl -sid 12345 commit -file addnewpool.cmd
```

Add Devices to a Pool

To add the specific Symmetrix devices to a pool, use the following command syntax in the command file:

```
add dev StartDevName[:EndDevName] to accpool PoolName;
```

For example, in the command file (**addnewpool.cmd**), to assign Symmetrix device names 0A through 19 to PoolB, enter:

```
add dev 00A:019 to accpool PoolB;
```

Then you must commit the file (**addnewpool.cmd**) to the database:

```
symacl -sid 12345 commit -file addnewdevs.cmd
```

Editing and Managing Access Pools

You can edit and manage the existing access pool information in the access control database.

Remove Devices from a Pool

To remove specific Symmetrix devices from a pool, use the following command syntax in the command file:

```
remove dev StartDevName[:EndDevName] from accpool  
PoolName;
```

For example, in the command file (**removedevs.cmd**), to assign Symmetrix device names 16 through 19 for removal in PoolB, enter:

```
remove dev 016:019 from accpool PoolB;
```

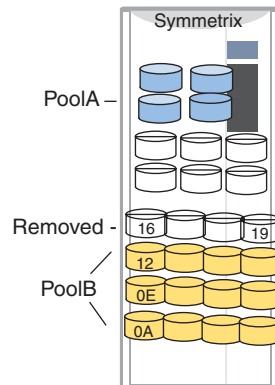


Figure 1-4 Removing Devices from a Pool

At some point, you must commit the file (**removedevs.cmd**) to execute the removal of devices 16 through 19 from PoolB.

Delete a Access Pool

You can delete an access pool and optionally at the same time remove any associated access control entries (ACEs) with the specified pool. Note that all ACEs must be removed before you can delete a pool.

To delete an access pool and remove all ACEs, use the following command syntax in the command file:

```
delete accpool PoolName [remove_aces=true];
```

For example, in the command file (**deletepool.cmd**), to remove PoolB and any associated ACEs, enter:

```
delete accpool PoolB remove_aces=true;
```

At some point, you must commit the file (**deletepool.cmd**) to execute the removal of PoolB.

How to Create and Manage Access Control Entries

Once you have created groups and access pools, you can now create access control entries (ACEs) that grant access rights to the groups and pools.

A group can have multiple access rights and pools, which requires an ACE for each.

Initially, you can check to see if the host you are using has the administrative authority to make access control changes using the following command syntax:

```
symacl list -v [-sid SymmID|ALL]
```

Grant Rights to an Access Group

Once you have created an access group, you need to determine and grant, to the access group, the rights (*AccessType*) of access to a specified pool or to all the devices in the Symmetrix (or all devices not in a pool) using the following command syntax:

```
grant access=<AccessType,,> to accgroup GroupName  
for <accpool PoolName> | <ALL|NON-POOLED devs>;
```

The *AccessType* parameter specifies the rights to the SYMCLI or SYMAPI features or functionality that is to be granted to selected devices.

The possible rights values are listed and described in Table 1-4.

Table 1-4 Access Types to Specified Devices

Rights (<i>AccessType</i>)	Rights Description	Commands Affected
ADMIN ^b	Grants administrator privilege to grant/deny access control entries to hosts and users.	symacl <prepare, commit, release, list, show>
ADMINRD ^b	Grants read access only to all access control information.	symacl <list, show>
ALL ^b	All possible access types granted except ADMIN and ADMINRD. Must be directed to ALL devices.	All
BASE	Allows the discovery of devices and to obtain states and statistics from the Symmetrix array (directors and devices).	Base component commands
BASECTRL	Allows base control operations on devices and device groups.	symld <controls>

Table 1-4 Access Types to Specified Devices (continued)

Rights (AccessType)	Rights Description	Commands Affected
BCV	Allows TimeFinder (BCV) control and status operations.	symmir <controls>
CACHCTRL	Allows Cache control operations concerning LRU partition management.	symqos <set LRU >
CFGDEV	Allows powerful configuration control operations that manage various types of configuration changes on devices in the Symmetrix.	symconfigure
CFGSYM ^b	Allows access to set Symmetrix attributes, set port flags, and swap RA groups with <i>symconfigure</i> . Must be directed to ALL devices.	symconfigure
CHECKSUM	Allows Symmetrix device Oracle checksum operations.	symchksum <controls>
CREATEDV ^b	Allows the creation of Symmetrix devices (part of <i>symconfigure</i>). Must be directed to ALL devices.	symconfigure
DIRCTRL ^b	Allows you to take directors and their ports offline and online. Must be directed to ALL devices.	symcfg <online/offline>
ECC ^{a, b}	Allows the ECC symmetrix agent to run on the requested host.	Not applicable
ERASE	EMC Symmetrix Secure Erase allows the user to permanently and securely erase Symmetrix devices.	symerase
OPTMZR	Allows user configurable attributes that may affect the Optimizer behavior.	symoptmz <controls>
POWRPATH ^{a, b}	Access to PowerPath™-directed devices in an RDF consistency group. Must be directed to ALL devices.	Not applicable
QOS	Allows the execution of Quality of Service (QOS) performance control operations. Excludes LRU cache control functionality.	symqos <set pace>
RDF	Allows SRDF control and set operations.	symrdf <control
SDDF	Allows the DeltaMark™ (Change Tracker) functionality that monitors track changes.	symchg

Table 1-4 Access Types to Specified Devices (continued)

Rights (<i>AccessType</i>)	Rights Description	Commands Affected
SDR	Allows mapping/unmapping of devices to directors/ports for the Symmetrix Disk Reallocation (SDR) feature.	symconfigure
SNAP	TimeFinder/Snapshot allows the creation and management of virtual copy sessions between a source device and multiple virtual (VDEV) target devices.	symsnap
VLOGIX ^{a, b}	Enables access to Device Masking or Volume Logix devices.	symmask, symmaskdb

a. See the appropriate product documentation for use of these access types.

b. These access types must be granted to either ALL devices or all NON-POOLED devices in a Symmetrix.

Before you can grant a group the rights to any value-added non-base feature, you must first grant the group BASE rights.

To grant BASE rights to access group ProdB for all devices, use the following command in the command file (**grantrights.cmd**):

```
grant access=BASE to accgroup ProdB for ALL devs;
```

To grant BASE rights to access group ProdB for poolPRODdevs, specify:

```
grant access=BASE to accgroup ProdB
for accpool PRODdevs;
```

Note: When restricting a host to BASE access to a pool of devices, only devices that are visible after a discover will be those devices in the pool. All other devices will appear to be unconfigured. In addition, remote (SRDF) arrays and their devices will not be discovered and the Symmetrix application registration database and the audit logs cannot be accessed since these may contain data relevant to other hosts.

To grant RDF rights to access group ProdB for pool PRODdevs, use the following command in the command file (**grantrights.cmd**):

```
grant access=RDF to accgroup ProdB
for accpool PRODdevs;
```

To grant BCV and SDR rights to access group HR for pool poolHR, use the following command in the command file:

```
grant access=BCV, SDR to accgroup HR for accpool  
poolHR;
```

Note that these command examples created three ACEs for BASE, BCV, and the SDR rights, which now could be committed.

To make any non-registered (*unknown*) host have BASE rights to access group UnknwGrp for all devices in the Symmetrix environment, use the following command in the command file:

```
grant access=BASE to accgroup UnknwGrp for ALL devs;
```

At some point, you must commit the file (**grantrights.cmd**) to execute the granting of rights with these various command entries.

Remove Rights from an Access Group

To remove rights for an access group, use the following command in the command file:

```
remove access=<AccessType,,,> from accgroup GroupName  
for <accpool PoolName> | <ALL|NON-POOLED devs>;
```

To remove SDR rights from access group HR for poolHR, use the following command in the command file:

```
remove access=SDR from accgroup HR for accpool poolHR;
```

At some point, you must commit the file (**grantrights.cmd**) to execute the change of rights with these entries.

How to Obtain Access Control Information

You can check the current Symmetrix access control database to view the various groups, pools, and also the ACLs. Only if you have ADMIN or ADMINRD rights, can you view all access objects in the access control database.

Using the list action when you don't have administrative rights, you only see access objects that are associated with the access group to which your host belongs.

Listing Access Control Information

Using the list argument in the following command, you can list information about groups, pools, and ACLs with the following syntax:

```
symacl [-sid SymmID|ALL] list -accgroup |  
                                -accpool |  
                                -acl |  
                                -v
```

For example, the following command lists the access groups on Symmetrix 0133:

```
symacl -sid 0133 list -accgroup
```

The following command example lists all the access pools on Symmetrix 0133:

```
symacl -sid 0133 list -accpool
```

The following example lists all the ACEs (with their pools and access types) for the entire Symmetrix environment:

```
symacl list -acl
```

Showing Access Control Information

Using the show actions when you don't have administrative rights, you only see access objects that are associated with the access group to which your host belongs.

To show detail information about a specified group or pool, use the following syntax:

```
symacl -sid SymmID|ALL show accgroup GroupName |  
show accpool PoolName
```

For example, the following command shows all the detail about access group ProdB on Symmetrix 0133:

```
symacl -sid 0133 show accgroup ProdB
```

The following command example shows all the detail about the PRODdevs access pool on Symmetrix 0133:

```
symacl -sid 0133 show accpool PRODdevs
```

Getting Your Host Access ID

You can get the access ID for the host you are using. The following command will return a unique access ID in an encrypted format:

```
symacl -unique
```

The -unique option returns the encrypted access ID in the following segmented, 24-digit numeric form:

```
xxxxxxxx-yyyyyyyy-zzzzzzzz
```

For example:

```
12301558-94200021-00347892
```

How to Release Pending Locked Sessions

During the processing of the command file, the `prepare` and `commit` actions are critical SYMCLI or SYMAPI operations that are considered access control *sessions*. In the event a host machine or application should abnormally fail and stop processing any `prepare` or `commit` access operation on its command file, you can abort this locked session from your current host or another host using the following command:

```
symacl release -sid SymmID
```

Note that if you are the security administrator and you intend to release a lock on the command file session, you must either set environment variable `SYMCLI_ACCESS_PIN` to your access ID or enter your PIN every time `symacl` prompts you.

Verifying a Locked Session

To verify an access controlled session is locked on any Symmetrix, you can use:

```
symacl list -v
```

This command can tell you how long the session has been locked and who locked it.

Grant/Deny Access Strategies

This section describes the access control strategies that can be applied in an access controlled Symmetrix environment. Several strategies can be considered for establishing or restricting access for a node or group of users or hosts to your Symmetrix environment. These strategies should be considered when you are setting up an access control environment for the first time.

Initially Grant All Rights to Everybody

The initial (delivered) strategy is to employ a default ID that controls all nodes not yet explicitly registered. This default ID can be used to grant a certain level or a minimal level of access for all unregistered nodes.

In the following example, when the Symmetrix was initially configured (delivered), a group named UnknwGrp was created for non-registered hosts (with no ID).



A special *Default* access ID named unknown was added to the group granting all unknown hosts and users ALL access rights.

Next, an ACE was created for group UnknwGrp granting them ALL rights to all the Symmetrix devices. In this scenario, all users and hosts can perform any of the SYMCLI command set operations.

Granting and Denying Default and Legacy Access

The delivered setup of Symmetrix access control grants legacy applications and hosts whose access IDs have not yet been registered, ALL access to all Symmetrix devices (within the exception of ADMIN and ADMINRD privileges). This was done by creating a group called UnknwGrp, and putting the default access ID into it. The name of that default ID was called unknown. An access control entry was then granted to the group UnknwGrp with a grant of ALL to access all Symmetrix devices.

If this ID is removed from the group UnknwGrp or this group is removed, and then you need to add it back to a certain group, use the following syntax:

```
add default accid name IdName to accgroup GroupName;
```

Once the default ID has been added to the group, then all legacy applications and hosts whose access IDs are not yet or never will be registered in the access control database, will default to using the ACEs established for this group.

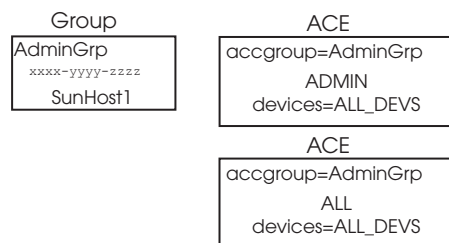
If the default ID is not present, then the access ID of all hosts that need to communicate to the Symmetrix must be registered in the database and granted sufficient access rights to accomplish the functions they need to perform.

Finally, an ACE was created for group UnknwGrp granting them ALL rights to all the Symmetrix devices. In this scenario, all users and hosts can perform any of the SYMCLI command set operations.

Establishing an Administrator

As shown in Figure 1-1 on page 1-4 and Figure 1-2 on page 1-5, the delivered setup allows at least one host assigned with administrative (ADMIN) privileges to be designated the administrator of the information in the access control database.

In the following example, when the Symmetrix was initially configured, an access group named AdminGrp was created. Then a UNIX workstation named SunHost1 with an encrypted access ID (of the form *xxxxxxx-yyyyyyyy-zzzzzzzz*) was added to the AdminGrp group. (The access ID was obtained by running `symacl -unique`.)

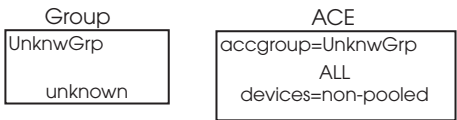


Next, two ACEs were created; one granting ADMIN rights and one granting ALL rights to group AdminGrp for all devices in the Symmetrix.

Grant all Rights to the Non-Pooled Devices

A second possible strategy once access controlled access pools have been established is to allow no restrictions on all the Symmetrix devices that are not otherwise registered (*Non-Pooled*) in any access pool.

In the following example, the ACE for the access group named UnknwGrp was modified to restrict access to only those devices not registered in an access control pool.



General Absolute Control Strategy

A third strategy, which is more controlled, is to only register access to certain devices on an as-needed basis. In this scenario, the UnknwGrp group was removed. Therefore, a node must be known to the Symmetrix, and only specific users/hosts in defined groups with limited or unlimited rights have access to certain devices defined in their working pools.

Initial Setup Summary

Whatever strategy you apply during the initial building of the access control database, you need to survey all user needs, organize their limitations into groups, determine what Symmetrix devices to allocate to who, and what access rights are appropriate for each group. It is highly recommended to use the preview and prepare actions on your first major command file before you commit it; particularly if it is an extensive list. The preview and prepare will identify any coding errors or mistakes in the logic.

BCV Setup Strategy

To set up an access controlled environment for TimeFinder operations, you need set up both the standard and BCV devices as follows:

- 1. Define your working access pool to contain both the standard and BCV SymDevnames.
- 2. For your group name, grant BASE rights to access all devices.
- 3. For your group name, grant BCV rights to the access pool holding the pairs.

TimeFinder/Snap Setup Strategy

To set up an access controlled environment for TimeFinder/Snap operations, you need set up both the source and target devices and the SAVE devices as follows:

Source and Target Strategy

1. Define your working access pool to contain both the source and target device's SymDevnames.
2. For your group name, grant BASE rights to access all devices.
3. For your group name, grant SNAP rights to the access pools holding the pairs.

SAVE Device Strategy

1. Define your working access pool to contain the SAVE device's.
2. For your group name, grant BASE rights to access the SAVE devices.
3. For your group name, grant CFGSYM rights to create and delete the SAVE devices.
4. For your group name, grant SNAP rights to manage the SAVE devices.

SRDF Setup Strategy

To set up an access controlled environment for SRDF operations, you need set up both the local Symmetrix and remote Symmetrix. Because both Symmetrix arrays have their own access controlled database, you must:

1. With the ADMIN host, create an access control group for the local Symmetrix. Then with an ADMIN local or remote host, define the same access control group name for the remote Symmetrix.
2. With an ADMIN host, create a access pool defined with the R1 SymDevnames. Then with the ADMIN local or remote host, define a access pool with the R2 SymDevnames.
3. Grant BASE rights for the group to access all devices. Then with an ADMIN host, grant BASE rights to access all devices.
4. Grant RDF rights for the group to access the R1 access pool. Then with an ADMIN host, grant RDF rights for the group to access the R2 access pool.

How to Backup and Restore the Access Control Database

When working with access control, it is a good practice to create a backup file of your existing access control database prior to making changes.

Create a Backup File

You can create a backup of your current access control database, using the following command:

```
symacl -sid SymmID backup -file CommandFile
```

The backup operation saves the contents of the access control database in the file specified by the file option. The file must not previously exist. The backup file created is compatible for use with the symacl utility.

Note: The backup file contains encrypted versions of the unique IDs, therefore if you compare the values in the backup file to the original file used to create the database, they will be different.

Restore the Backup File to the Access Control Database

In the event a host machine or application makes undesirable changes to your access control configuration, you can utilize a backup file you've created to restore the previous configuration data to the access control database.

When you restore a backup using `symacl` you use the `-restore` option as shown below:

```
symacl      -sid SymmID commit [-v|-noecho]  
            -restore -file CommandFile
```

The restore operation replaces the contents of the access control database with the contents of the file specified by the file option. It eliminates whatever currently exists in the Symmetrix configuration database and replaces it with the contents of the backup.

Note: The backup file contains encrypted versions of the unique IDs, therefore if you compare the values in the backup file to the original file used to create the database, they will be different.

A

Abort

- locked session 1-22

Access control commands

- introduction 1-3

Access control database 1-5

Access control entries

- creating 1-16

- see also* ACEs 1-5

Access control lists

- see also* ACLs 1-5

Access groups 1-4

- access IDs (PINs) 1-10

- adding access IDs 1-10

- creating 1-9

- deleting 1-12

- editing/managing 1-11

- granting rights 1-16

- listing 1-20

- moving access IDs 1-11

- removing access IDs 1-11

- removing ACEs 1-11

- removing rights 1-19

- setting up 1-9

- showing 1-21

- unknown 1-24

Access IDs 1-4, 1-10

- viewing 1-21

Access pools 1-2, 1-13

- add devices 1-14

- creating 1-13

- deleting 1-15

- editing/managing 1-14

- listing 1-20

- remove device 1-14

- setting up 1-13

- showing 1-21

Access types 1-16

ACEs

- listing 1-20

- showing 1-21

ACLs

- listing 1-20

Admin rights 1-13, 1-16

Administrator

- establishing 1-24

Authority

- admin rights 1-13, 1-16

B

Backup database 1-27

BCV strategy 1-25

C

Command file 1-6

- command types 1-6

- commit 1-7

- prepare 1-6

- preview 1-6

Commit command file 1-7

Creating access pools 1-13

D

Database

- backup 1-27

restore 1-27
Databases
 access control 1-5
Device pools. *See* Access pools

G

Granting rights 1-16
Groups 1-9

L

Listing ACLs 1-20
Locked session
 release 1-22

M

Managing access groups 1-9
Managing access pools 1-13

P

Pools 1-13
Prepare command file 1-6
Preview command file 1-6

R

Release locked session 1-22
Restore database 1-27
Rights 1-16
 removing 1-19

S

Showing ACEs 1-21
SRDF devices 1-3
SRDF strategy 1-26
Strategies
 access control 1-23
SYMCLI commands
 symacl 1-3

T

TimeFinder strategy 1-25
TimeFinder/Snap strategy 1-26

U

Unknown access groups 1-24
User access IDs, PINs 1-10

V

Viewing access controls 1-20