



Technical Report

Storage-Level Access Guard Quick Start Guide

Nagesh Sharyathi, Reena Gupta, NetApp
March 2011 | TR-3596

NEW SECURITY LAYER IN DATA ONTAP

This guide describes how to configure Storage-Level Access Guard in Data ONTAP[®] on a NetApp[®] storage system. It provides information about this new security layer in Data ONTAP, its behavior, and the tools used to configure it. All commands and options referred to in this document are based on Data ONTAP version 7.2.2 and above.

TABLE OF CONTENTS

1	INTRODUCTION TO STORAGE-LEVEL ACCESS GUARD	3
1.1	TYPES OF SECURITY LAYERS	3
1.2	STORAGE-LEVEL ACCESS GUARD BEHAVIOR	3
1.3	BUSINESS EXAMPLES	4
2	STORAGE-LEVEL ACCESS GUARD CONFIGURATION	4
2.1	JOB DEFINITION FILE FORMAT	4
2.2	SECURITY DESCRIPTOR DEFINITION LANGUAGE (SDDL) FORMAT	5
2.3	STORAGE SECURITY EDITOR (SECEDIT) TOOL	5
2.4	FSECURITY COMMANDS	8
2.5	FSECURITY SCREENSHOTS	10
3	REVISION HISTORY	11

1 INTRODUCTION TO STORAGE-LEVEL ACCESS GUARD

Starting with Data ONTAP 7.2.2, an additional layer of security, called Storage-Level Access Guard, has been introduced on the storage object level. With this feature, storage administrators can set security (permissions and auditing) for all objects on volumes and qtrees using the `fsecurity` console command. This security level cannot be set or modified by normal CIFS or NFS administrative clients. This prevents these clients from overriding policies that should be managed at the storage level, not the protocol level.

1.1 TYPES OF SECURITY LAYERS

Storage-Level Access Guard security provides a third type of security layer for a storage object:

- **NTFS, UNIX[®], and NFSv4 security (native file-level security):** Exists on any directory or file that represents a storage object. This is the same security that you can set from a client.
- **Export (NFS) and share (CIFS) security:** Applies to client accesses to a given NFS export or CIFS share. Can be managed by CIFS and NFS clients with administrative privileges.
- **Storage-Level Access Guard:** Applies to all accesses from all protocols to the storage object to which the Storage-Level Access Guard has been applied. Applies to all the files and/or all the directories in a storage object, although settings are maintained separately for files versus directories.
 - **File security:** Applies to every file in the storage object. Does not affect access to or auditing of directories.
 - **Directory security:** Applies to every directory in the storage object. Does not affect access to or auditing of files.

Note: At this time, only NTFS-style access permissions are supported for Storage-Level Access Guard, but it can be applied to a UNIX security volume/qtree as well. For a UNIX user to perform a security check on a qtree or volume where Storage-Level Access Guard has been applied, the UNIX user must be mapped to a Windows[®] user in a NetApp system. It doesn't apply to an environment that is UNIX only, where CIFS is not enabled. In other words, if a UNIX user does not map to a Windows user in this situation, the NTFS-style Storage-Level Access Guard will be ignored.

1.2 STORAGE-LEVEL ACCESS GUARD BEHAVIOR

- Storage-Level Access Guard security applies to all files and/or directories in a storage object; hence, inheritance is not required to be propagated. If you view the security settings on a file or directory, you do not see the Storage-Level Access Guard security. It's applied at the storage object level and stored in the metadata used to determine the effective permissions.
- Volumes and qtrees are independent storage objects on which Storage-Level Access Guard can be applied.
- Access to a file or directory in Data ONTAP is determined by the combined effect of both the native permissions applied to files and/or directories and the Storage-Level Access Guard permissions set on qtrees and/or volumes. For CIFS/NFS client access, three levels of security checks are performed to determine effective permissions. The checks are performed in this order:
 1. Storage-Level Access Guard permissions
 2. CIFS share or NFS export-level permissions
 3. NTFS file/folder access control lists (ACLs) or UNIX mode bits

All accesses must pass all levels of security checks.

- Storage-level security cannot be revoked from a client, even by a system (Windows or UNIX) administrator. It is designed to be modified by storage administrators only, which precedes the share/export permission and the Windows ACLs or UNIX mode bits.

- A qtree cannot be deleted unless Storage-Level Access Guard is removed from it.
- Qtree SnapMirror® does *not* propagate the Storage-Level Access Guard security descriptor with the data replication; volume SnapMirror *does*. NetApp recommends volume SnapMirror for replicating Storage-Level Access Guard security.
- Special dispensation for virus scanners and FPolicy® servers: Exceptional access is allowed to these servers to screen the files and folders, even if Storage-Level Access Guard denies access to the object.
- This also applies to MultiStore® environments for the storage objects owned by the virtual storage systems.
- Storage-Level Access Guard security checks have a small performance impact.

1.3 BUSINESS EXAMPLES

Storage-Level Access Guard provides additional security at the storage level, which is not visible from a client side; therefore, it cannot be revoked by any of the users or administrators from their desktops. This feature makes it most commonly used in the following scenarios:

- Intellectual property protection by auditing and controlling all users' access at the storage level
- Storage for financial services companies, which include both banking and trading groups
- Government services with separate file storage for individual departments
- Universities protecting all student files

2 STORAGE-LEVEL ACCESS GUARD CONFIGURATION

To apply Storage-Level Access Guard to a storage object, follow these steps:

1. Create a job definition file using either a text editor or the Storage Security Editor tool (*secedit*), a Windows tool provided by NetApp. The job definition file is a Unicode text file that contains various pieces of information such as security descriptors and paths.
2. After creating the job definition file, copy it to a location on the storage system. There are no specific requirements for the name and location of this file; for example, `/vol/vol0/templates/security-base.sec`.
3. Use the **fsecurity apply** command on the NetApp storage system console to validate and apply the security definitions. This command creates a job that runs in the background on the storage system.
4. Check the status of the job that is running or the history of 15 jobs at once by using the **fsecurity status** command.

2.1 JOB DEFINITION FILE FORMAT

The job definition file used for providing security descriptors and paths can be in either UTF8 or Unicode file format, representing an entire job with one or more subtasks. The security definition format is defined as follows:

```
security_type,security_level,security_target_object_path,propagation_mode,security_definition
```

Example:

```
cb56f6f4
1,1,"/vol/vol0/qtree",0,"D:(A;CIOI;0x1f01ff;;;DOMAIN\Administrator)"
```

```
1,0,"/vol/vol0/qtreet1/dir/dir1",0,"S:P(AU;CIOISAFA;0xf01ff;;;DOMAIN\user)D:P(A;CIOI;0x1200a9;;;Everyone)(A;CIOI;0x1f01ff;;;DOMAIN\user)(A;CIOI;0x1f01ff;;;FILER\administrator)"
```

- cb56f6f4 is the signature for the `fsecurity` file and must be present on the first line.
- In the second line of the example:
 - 1 refers to an NTFS security type*.
 - 1 refers to the Storage-Level Access Guard security definition.
security_levels: 0 = file/directory-level security; 1 = storage-level security
 - /vol/vol0/qtreet is the path of the security target object.
 - Propagation mode is not on since this is storage-level security.
0: Propagates inheritable permissions to all subfolders and files (Propagate).
1: Does not allow permissions on this file or folders to be replaced (Ignore).
2: Replaces existing permissions on all subfolders and files with inheritable permissions (Replace).
- Note:** Propagation mode is not applicable for Storage-Level Access Guard, regardless of the value present in the job definition.
 - D:(A;CIOI;0x1f01ff;;;DOMAIN\Administrator) is the SDDL representation of a DACL that gives DOMAIN\Administrator full control.
- Note:** security_definition: SDDL representation of DACL (D:) and SACL (S:) (see section 2.2).
- The third line is a file/directory-level security definition, used for applying bulk security settings (permissions and auditing) as described in [TR-3597: Bulk Security Quick Start Guide](#).

* NTFS security refers to NTFS-style configuration. Currently UNIX mode bits are not supported in this configuration file. UNIX users must be mapped to Windows users in order to go through the security checks for Storage-Level Access Guard.

2.2 SECURITY DESCRIPTOR DEFINITION LANGUAGE (SDDL) FORMAT

DACL and SACL in the definition file are represented in the SDDL format. The fields of ACE are in the following order and are separated by semicolons:

```
ace_type;ace_flags;rights;object_guid;inherit_object_guid;account
```

Example of an SDDL security definition:

```
S:P(AU;CIOISAFA;0xf01ff;;;domain\user)D:P(A;CIOI;0x1200a9;;;Everyone)(A;CIOI;0x1f01ff;;;domain\user)(A;CIOI;0x1f01ff;;;filer\administrator)
```

For more information about the SDDL format, refer to <http://msdn.microsoft.com/en-us/library/aa379570%28v=VS.85%29.aspx>.

2.3 STORAGE SECURITY EDITOR (SECEDIT) TOOL

NetApp Storage Security Editor is a Windows client application that assists in creating job definition files for the `fsecurity apply` command. This tool can be downloaded from the NetApp Support (formerly NOW™) site: <http://now.netapp.com/NOW/download/tools/secedit/>. Customers can use it on an as-needed basis.

- It is very similar to the Windows Explorer Security tab.
- It has the ability to read, import, and generate Storage-Level Access Guard security definition files.

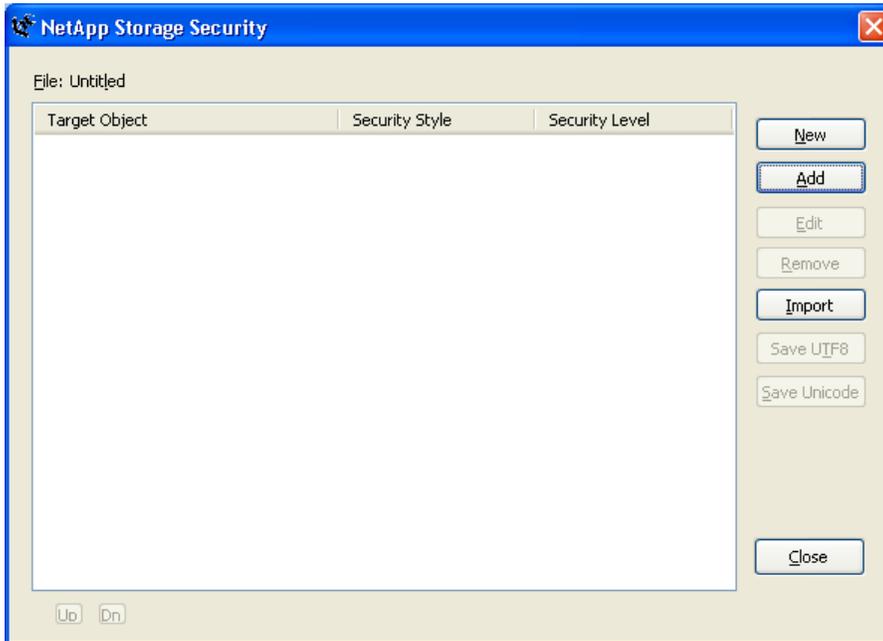
- It generates a file in modified SDDL format, which can be used with the `fsecurity apply` command.

Note: The modified SDDL format uses hex codes for the access rights rather than alphabetical codes.

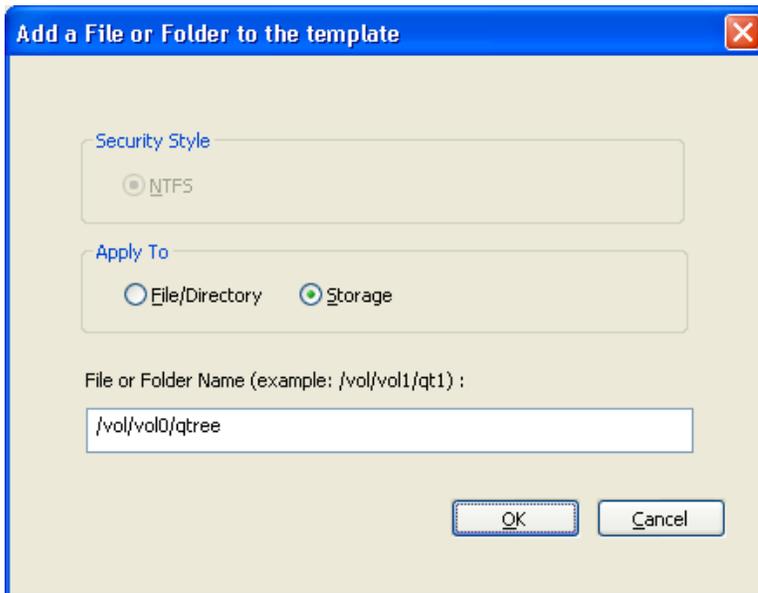
Example: `A;C:IOI;0x1f01ff;;;filer\administrator`

To set storage-level or file/directory security or auditing using the Storage Security Editor tool, do the following:

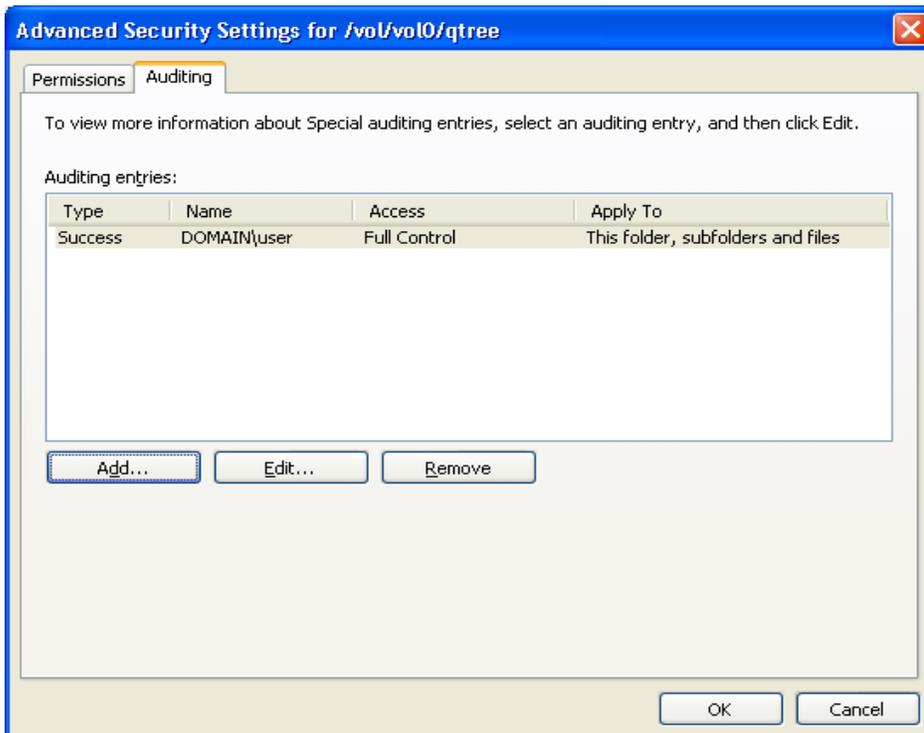
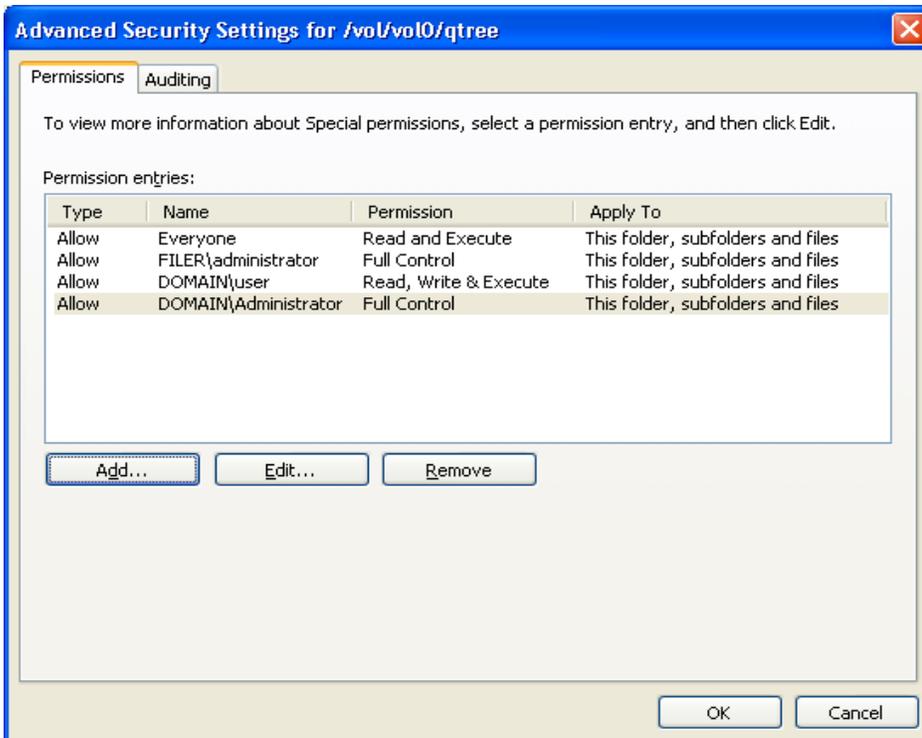
1. Run "secedit.exe" to launch the **Storage Security Editor** tool.



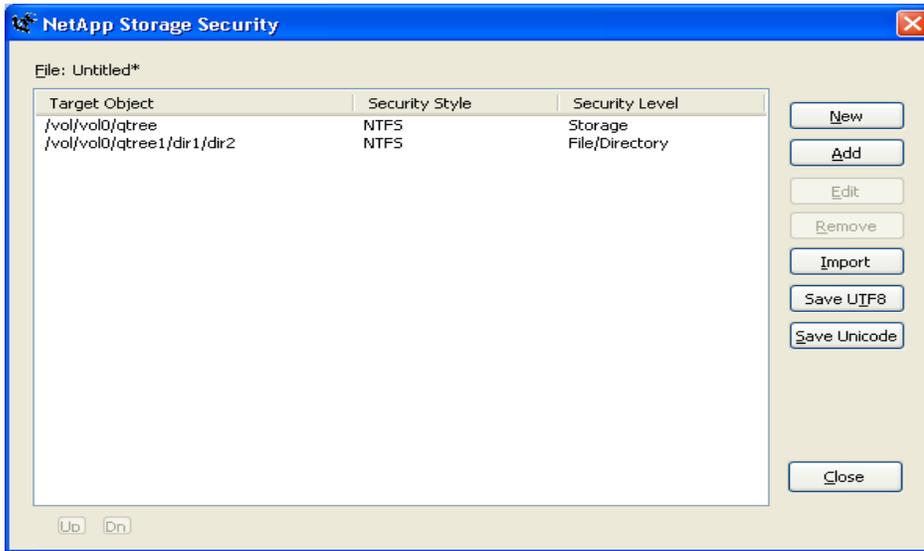
2. Select Storage-Level Access Guard and the **Storage** object.



3. Select the appropriate users and groups with the required **Permissions** or the required **Auditing** settings.



4. SLAG can be applied to all files and/or folders under the Storage object.



2.4 FSECURITY COMMANDS

The `fsecurity` command, introduced in Data ONTAP 7.2.2, is a vFiler[®]-specific console command that requires storage administrator privileges for execution.

- `fsecurity apply <definition file path> [<options>]`

Options:

- `-c` = Checks job validity without actually applying the contents
- `-i` = Ignores errors and continues job processing
- `-v` = Displays each task within the job as it is generated

The `fsecurity apply` command reads a file generated in a valid `fsecurity` security definition format, each line of which includes a full path to an object in the file system and the desired security for that object (and possibly child objects). Each line represents a task, and the entire contents of the file represent a single job. The tasks within a job will run sequentially. Jobs themselves run asynchronously and are not tied to the storage system console while they run. This job is given an ID that can be used with the `fsecurity status` and `fsecurity cancel` commands to retrieve the status or cancel the job, respectively. When the job is complete, the result is reported to the console.

Note: Security jobs can run simultaneously. It is possible to generate two security jobs that conflict with each other by defining common paths or subpaths within the tasks and running both jobs simultaneously. This behavior is no different from an external client changing security settings while a job is running, but this should be taken into account when generating these files and determining when and how they are applied.

- `fsecurity status [<job id>]`

The `fsecurity status` command displays the current status of any outstanding `fsecurity` jobs as well as the completion status of the previous 15 jobs. If a job ID is specified, the detailed status of that particular job is displayed.

- `fsecurity cancel { all | <job id> }`

The `fsecurity cancel` command cancels outstanding security jobs that are not completed.

- `fsecurity show [-v <volume>|-s <share>] <path> [<options>]`
- `fsecurity show -v <volume> -i <inum> [<options>]`

Options:

- `-c` = Includes security descriptor control information
- `-d` = Includes directories in wildcard searches
- `-l` = Disables name lookups
- `-x` = Expands mask values

The `fsecurity show` command displays the full security information related to the target file or directory. Paths to volumes and qtrees (which are represented in the file system by directories) can be specified as well. When specifying the path, wildcards can be used to list security for the contents of a directory.

The security style contains the security style of the qtree that the file or directory resides in. The effective style varies in mixed qtree styles, depending on which security style is currently active on the object.

- `fsecurity remove-guard <path>`

The `fsecurity remove-guard` command removes the storage-level security from a volume or a qtree.

- `fsecurity help [<command>]`

The `fsecurity help` command displays a list of `fsecurity` commands or provides additional information about a specified `fsecurity` command.

For more information on `fsecurity` command usage and examples, see the [fsecurity\(1\)](#) man page.

2.5 FSECURITY SCREENSHOTS

The following figures show the screenshots for the `fsecurity` console command while applying the security definition in a configuration file.

```
fas2020c-svl13.iop.eng.netapp.com - PuTTY
fas2020c-svl13*>
fas2020c-svl13*>
fas2020c-svl13*> fsecurity apply /vol/volA/security_unicode.conf -v
Task 1, NTFS, Guard, N/A, /vol/volA/qtrees1 ... Added.
Task 2, NTFS, Normal, Propagate, /vol/volB/qtrees2 ... Added.
Added security job 1006.
fas2020c-svl13*> fsecurity: Job 1006 (/vol/volA/security_unicode.conf) completed successfully.
```

```
fas2020c-svl13.iop.eng.netapp.com - PuTTY
fas2020c-svl13*>
fas2020c-svl13*> fsecurity status
[History - Previous 15 jobs]
Job  Status  Tasks Definition
1002 Success 2      /vol/volA/security_unicode.conf
1003 Success 2      /vol/volA/security_unicode.conf
1004 Success 2      /vol/volA/security_unicode.conf
1005 Success 2      /vol/volA/security_unicode.conf
1006 Success 2      /vol/volA/security_unicode.conf
fas2020c-svl13*>
```

```
fas2020c-svl13.iop.eng.netapp.com - PuTTY
fas2020c-svl13*>
fas2020c-svl13*> fsecurity show /vol/volA/* -d
[/vol/volA/qtrees1 - Directory (inum 100)]
Security style: NTFS
Effective style: NTFS

DOS attributes: 0x0030 (---AD---)

Unix security:
uid: 0 (root)
gid: 0 (daemon)
mode: 0777 (rwxrwxrwx)

NTFS security descriptor:
Owner: BUILTIN\Administrators
Group: BUILTIN\Administrators
DACL:
Allow - Everyone - 0x001f01ff (Full Control)
Allow - Everyone - 0x10000000 - OI|CI|IO

Storage-Level Access Guard security:
DACL (Applies to Directories):
Allow - Everyone - 0x001200a9 (Read and Execute)
Allow - W2K3R2\reena - 0x001f01ff (Full Control)
SACL (Applies to Directories):
All - W2K3R2\facilities - 0x000f01ff (Full Control)
DACL (Applies to Files):
Allow - Everyone - 0x001200a9 (Read and Execute)
Allow - W2K3R2\reena - 0x001f01ff (Full Control)
SACL (Applies to Files):
All - W2K3R2\facilities - 0x000f01ff (Full Control)
[/vol/volA/security_unicode.conf - File (inum 101)]
Security style: NTFS
Effective style: Unix

DOS attributes: 0x0020 (---A---)

Unix security:
uid: 0 (root)
gid: 1 (daemon)
mode: 0755 (rwxr-xr-x)

No security descriptor available.
fas2020c-svl13*>
```

3 REVISION HISTORY

Date	Name	Description
March 2011	Sharyathi Nagesh	Revised
May 2008	Reena Gupta	Revised
July 2007	Reena Gupta	Creation

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.