



A Commands

This chapter covers the following commands:

- [aaa authentication enable](#), page 2-2
- [aaa authentication iscsi](#), page 2-5
- [aaa authentication login](#), page 2-8
- [aaa generate password](#), page 2-11
- [aaa group server radius](#), page 2-12
- [aaa group server radius deadtime](#), page 2-14
- [aaa group server radius server](#), page 2-16
- [aaa group server tacacs+](#), page 2-18
- [aaa group server tacacs+ server](#), page 2-20
- [aaa new-model](#), page 2-22
- [aaa test authentication](#), page 2-24
- [accesslist](#), page 2-26
- [accesslist A.B.C.D/bits](#), page 2-28
- [accesslist chap-username](#), page 2-30
- [accesslist description](#), page 2-32
- [accesslist iscsi-name](#), page 2-34
- [admin contactinfo](#), page 2-36
- [admin password](#), page 2-38

aaa authentication enable

To configure authentication, authorization and accounting (AAA) services for Administrator mode access to the CLI (via the CLI **enable** command), use the **aaa authentication enable** command. To disable this authentication, use the **no** form of this command.

```
aaa authentication enable default services1 [services2...]
```

```
no aaa authentication enable default
```

Syntax Description

default	The name of the authentication list. The list name must be <i>default</i> .
<i>services1 [services2...]</i>	At least one of the services described in Table 2-1 .

Defaults

If the default list is not configured, only the Administrator mode password is checked. This has the same effect as the following command:

```
aaa authentication enable default enable
```

Command Modes

Administrator.

Command History

Release	Modification
2.5.1	This command was introduced for the SN 5428.
3.2.1	This command was introduced for the SN 5428-2.

Usage Guidelines

Administrator mode access (“Enable”) authentication uses AAA services to provide authentication of users that request Administrator mode access to the storage router via the CLI **enable** command. Because the **enable** command does not require you to enter a user name, the special user name *\$enab15\$* is used if RADIUS or TACACS+ servers are used for authentication.

AAA attempts to use each service in the order listed in the default authentication list, until authentication succeeds or fails. If the service fails to find a user name and password match, authentication fails and access is denied. If AAA returns an error (because the RADIUS or TACACS+ server is not available, for example), AAA attempts to use the next service in the list for authentication. To specify that the authentication should succeed even if all methods return an error (not if they return an authentication failure), specify **none** as the final method in the command line. Use the **show aaa** command to display the current authentication lists.

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **aaa authentication enable** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

**Note**

Enable authentication extends to users accessing the storage router via an FTP session. An FTP session requires the user name *admin* and the password that would be entered for the CLI **enable** command.

In [Table 2-1](#), the **group radius** and **group tacacs+** methods refer to all previously defined RADIUS or TACACS+ servers; the **group name** method refers to a previously defined group of one or more RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the servers, and the **aaa group server radius** and **aaa group server tacacs+** commands to create server groups.

Table 2-1 *aaa authentication enable default services*

Keyword	Description
enable	Uses the configured Administrator mode password for authentication.
group name	Uses a named group of defined RADIUS or TACACS+ servers for authentication, using the user name <i>\$enab15\$</i> .
group radius	Uses the list of all RADIUS servers for authentication, using the user name <i>\$enab15\$</i> .
group tacacs+	Uses the list of all TACACS+ servers for authentication, using the user name <i>\$enab15\$</i> .
monitor	Uses the configured Monitor mode password for authentication.
none	Uses no authentication.

Examples

The following example creates a default AAA authentication list to be used to perform Enable authentication. When Administrator access of the storage router is requested via the CLI **enable** command, AAA first attempts to contact a RADIUS server, using the *\$enab15\$* username and the entered password. If no server is found, AAA returns an error and authentication is performed by checking the entered password against the configured Administrator mode password. If there is no match, authentication fails and you are denied Administrator access.

```
[SN5428-2A]# aaa authentication enable default group radius enable
```

Related Commands	Command	Description
	aaa group server radius	Create a named group of RADIUS servers for AAA authentication services.
	aaa group server tacacs+	Create a named group of TACACS+ servers for AAA authentication services.
	aaa authentication login	Configure AAA authentication services for Monitor mode access to the storage router via the CLI.
	aaa test authentication	Enable testing of the specified AAA authentication list.
	debug aaa	Enable debugging for the AAA authentication services.
	radius-server host	Configure remote RADIUS servers for AAA authentication services.
	restore aaa	Restore AAA authentication services from the named configuration file.
	save aaa	Save the current AAA configuration information.
	show aaa	Display AAA configuration information.
	tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.

aaa authentication iscsi

To configure authentication, authorization and accounting (AAA) services for iSCSI authentication of IP hosts requesting access to storage via SCSI routing instances, use the **aaa authentication iscsi** command. To disable this authentication, use the **no** form of this command.

```
aaa authentication iscsi {listname | default} services1 [services2...]
```

```
no aaa authentication iscsi {listname | default}
```

Syntax Description

<i>listname</i>	The name of the authentication list. Enter a maximum of 31 characters.
default	The name of the default authentication list.
<i>services1 [services2...]</i>	At least one of the services described in Table 2-2 .

Defaults

If iSCSI authentication is enabled and the named authentication list is not configured, authentication fails.

If iSCSI authentication is enabled using the default list but the default list is not configured, only the local user database is selected. This has the same effect as the following command:

```
aaa authentication iscsi default local
```

Command Modes

Administrator.

Command History

Release	Modification
2.2.1	This command was introduced for the SN 5428.
2.5.1	The <i>listname</i> variable was added.
3.2.1	This command was introduced for the SN 5428-2.

Usage Guidelines

iSCSI authentication uses AAA services to provide authentication of IP hosts that request access to storage from SCSI routing instances that have authentication enabled.

AAA attempts to use each service in the order listed in the specified iSCSI authentication list, until authentication succeeds or fails. If the service fails to find a user name match, authentication fails. If AAA returns an error (because the RADIUS or TACACS+ server is not available, for example), AAA attempts to use the next service in the list for authentication.

If either local or local-case is the first service on the iSCSI authentication list and AAA fails to find a user name match, AAA attempts to use the next method on the list for authentication. If the local or local-case service is in any other position on the list and AAA fails to find a user name match, authentication fails and access is denied. If a RADIUS or TACACS+ server fails to find a user name match (regardless of position on the iSCSI authentication list), authentication fails and access is denied.

Use the **show aaa** command to display the current authentication lists.

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **aaa authentication iscsi** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

In [Table 2-2](#), the **group radius** and **group tacacs+** methods refer to all previously defined RADIUS or TACACS+ servers; the **group name** method refers to a group of one or more RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the servers, and the **aaa group server radius** and **aaa group server tacacs+** commands to create server groups.

**Note**

A named server group must be defined to be used as an authentication method. However, verification of server groups occurs only at runtime. If a server group is not defined, the authentication process generates error messages and the server group is skipped. This could cause unexpected authentication failures.

Table 2-2 *aaa authentication iscsi services*

Keyword	Description
group name	Uses a named group of defined RADIUS or TACACS+ servers for authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
none	Uses no authentication.

If the local authentication service is selected, the user name validation is not case-sensitive. If local-case authentication service is selected, the user name validation is case-sensitive. The password validation for both the local service and the local-case service is case-sensitive.

Examples

The following example creates a new AAA authentication list named *webtest* and enables iSCSI authentication for the SCSI routing instance named *myCompanyWebserver2*, using the *webtest* authentication list. When iSCSI authentication is required, AAA first tries to use the local username database for authentication. If no match is found, AAA attempts to contact a TACACS+ server. If no server is found, AAA returns an error and the IP host is allowed access with no authentication.

```
[SN5428-2A]# aaa authentication iscsi webtest local group tacacs+ none
[SN5428-2A]# scsirouter myCompanyWebserver2 authentication webtest
```

Related Commands	Command	Description
	aaa group server radius	Create a named group of RADIUS servers for AAA authentication services.
	aaa group server tacacs+	Create a named group of TACACS+ servers for AAA authentication services.
	aaa test authentication	Enable testing of the specified AAA authentication list.
	debug aaa	Enable debugging for the AAA authentication services.
	radius-server host	Configure remote RADIUS servers for AAA authentication services.
	restore aaa	Restore AAA authentication services from the named configuration file.
	save aaa	Save the current AAA configuration information.
	scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
	show aaa	Display AAA configuration information.
	tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.

aaa authentication login

To configure authentication, authorization and accounting (AAA) services for Monitor mode access to the storage router via the CLI, use the **aaa authentication login** command. To disable this authentication, use the **no** form of this command.

```
aaa authentication login default services1 [services2...]
```

```
no aaa authentication login default
```

Syntax Description

default	The name of the authentication list. The list name must be <i>default</i> .
<i>services1 [services2...]</i>	At least one of the services described in Table 2-3 .

Defaults

If the default list is not configured, only the Monitor mode password is checked. This has the same effect as the following command:

```
aaa authentication login default monitor
```



Note

If the default list is not configured, you are only prompted to enter a password; you are not prompted to enter a user name.

Command Modes

Administrator.

Command History

Release	Modification
2.5.1	This command was introduced for the SN 5428.
3.2.1	This command was introduced for the SN 5428-2.

Usage Guidelines

Monitor mode access (“Login”) authentication uses AAA services to provide authentication of users that request Monitor mode access to the storage router via the CLI. A user attempting Monitor mode access of the storage router via the CLI will be prompted for a user name and password.

AAA attempts to use each service in the order listed in the default authentication list, until authentication succeeds or fails. If the service fails to find a user name match, authentication fails. If AAA returns an error (because the RADIUS or TACACS+ server is not available, for example), AAA attempts to use the next service in the list for authentication. To specify that the authentication should succeed even if all methods return an error (not if they return an authentication failure), specify **none** as the final method in the command line.

If either local or local-case is the first service on the default authentication list and AAA fails to find a user name match, AAA attempts to use the next method on the list for authentication. If the local or local-case service is in any other position on the list and AAA fails to find a user name match, authentication fails and access is denied. If a RADIUS or TACACS+ server fails to find a user name match (regardless of position on the default authentication list), authentication fails and access is denied.

If the Enable service is used, the user name is ignored and the password is authenticated against the configured Administrator mode password. If the Monitor service is used, the user name is ignored and the password is authenticated against the configured Monitor mode password.

**Note**

AAA does not provide authentication for access via the GUI (using HTTP or HTTPS).

Use the **show aaa** command to display the current authentication lists.

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **aaa authentication login** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

In [Table 2-3](#), the **group radius** and **group tacacs+** methods refer to all previously defined RADIUS or TACACS+ servers; the **group name** method refers to a previously defined group of one or more RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the servers, and the **aaa group server radius** and **aaa group server tacacs+** commands to create server groups.

Table 2-3 *aaa authentication login default services*

Keyword	Description
enable	Uses the configured Administrator mode password for authentication. The user name is ignored.
group name	Uses a named group of defined RADIUS or TACACS+ servers for authentication.
group radius	Uses the list of all RADIUS servers for authentication.
group tacacs+	Uses the list of all TACACS+ servers for authentication.
local	Uses the local username database for authentication.
local-case	Uses case-sensitive local username authentication.
monitor	Uses the configured Monitor mode password for authentication. The user name is ignored.
none	Uses no authentication.

If the local authentication service is selected, the user name validation is not case-sensitive. If local-case authentication service is selected, the user name validation is case-sensitive. The password validation for both the local service and the local-case service is case-sensitive.

Examples

The following example creates a default AAA authentication list to be used to perform Login authentication. AAA first attempts to contact a RADIUS server. If no server is found, AAA returns an error and authentication is performed by checking the local username database. If no match is found, AAA performs authentication by checking the entered password against the configured Monitor mode password.

```
[SN5428-2A] # aaa authentication login default group radius local monitor
```

Related Commands	Command	Description
	aaa authentication enable	Configure AAA authentication services for Administrator mode access to the storage router via the CLI enable command.
	aaa group server radius	Create a named group of RADIUS servers for AAA authentication services.
	aaa group server tacacs+	Create a named group of RADIUS servers for AAA authentication services.
	aaa test authentication	Enable testing of the specified AAA authentication list.
	debug aaa	Enable debugging for the AAA authentication services.
	radius-server host	Configure remote RADIUS servers for AAA authentication services.
	restore aaa	Restore AAA authentication services from the named configuration file.
	save aaa	Save the current AAA configuration information.
	scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
	show aaa	Display AAA configuration information.
	tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.

aaa generate password

To generate a long random password, use the **aaa generate password** command.

aaa generate password

Syntax Description This command has no arguments or keywords.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	2.5.1	This command was introduced for the SN 5428.
	3.2.1	This command was introduced for the SN 5428-2.

Usage Guidelines Use this command to generate a long random password. From a CLI management session, you can cut and paste this password into other commands or applications, using the conventions appropriate to your specific Telnet or SSH client, or operating system.

Examples The following example generates a long random password:

```
[SN5428-2A]# aaa generate password
Password: 28b79da19608342a99642ce92fbdd3114
```

Related Commands	Command	Description
	aaa test authentication	Enable testing of the specified AAA authentication list.
	admin password	Set the login password for administrative access to the storage router management interface.
	monitor password	Set the login password for view-only access to the storage router management interface.
	username password	Add a user name and optional password to the local username database.

aaa group server radius

To create a named group of RADIUS servers to be used for AAA authentication, use the **aaa group server radius** command. To disable an existing group of RADIUS servers, use the **no** form of this command.

aaa group server radius *name*

no aaa group server radius *name*

Syntax Description

<i>name</i>	The name of the group of RADIUS servers to be used for AAA authentication. Enter a maximum of 31 characters.
-------------	--

Defaults

None. All configured RADIUS servers belong to the group named *radius*.

Command Modes

Administrator.

Command History

Release	Modification
2.5.1	This command was introduced for the SN 5428.
3.2.1	This command was introduced for the SN 5428-2.

Usage Guidelines

Use this command to create a subset of RADIUS servers to be used for AAA authentication. The named group can then be added to a AAA authentication methods list, allowing the specified set of RADIUS servers to be used for authentication. After creating the named group, use the **aaa group server radius server** command to add a RADIUS server to the group.

Use the **radius-server host** command to configure a RADIUS server to be used by the storage router for AAA authentication.

Group names must be unique across the storage router; you cannot have a group of RADIUS servers named *labauth* and a group of TACACS+ servers named *labauth*. The default group name of *radius* includes all configured RADIUS servers.

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **aaa group server radius** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

Examples

The following example creates a RADIUS server group named *region2*:

```
[SN5428-2A]# aaa group server radius region2
```

Related Commands	Command	Description
	aaa authentication enable	Configure AAA authentication services for Administrator mode access to the storage router via the CLI enable command.
	aaa group server radius deadline	Specify the length of time the storage router can skip a RADIUS server in the named group that is marked as unavailable.
	aaa group server radius server	Add the specified RADIUS server to the named RADIUS server group.
	aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
	aaa authentication login	Configure AAA authentication services for Monitor mode access to the storage router via the CLI.
	aaa test authentication	Enable testing of the specified AAA authentication list.
	radius-server deadline	Specify the length of time the storage router can skip a RADIUS server that is marked as unavailable.
	radius-server host	Configure remote RADIUS servers for AAA authentication services.
	radius-server key	Sets the global authentication and encryption key for all RADIUS communications between the storage router and the RADIUS daemon.
	radius-server retransmit	Specifies how many times the storage router resends the RADIUS request to a server before giving up.
	radius-server timeout	Sets the interval the storage router waits for a RADIUS server to reply before retransmitting.
	restore aaa	Restore AAA authentication services from the named configuration file.
	save aaa	Save the current AAA configuration information.
	scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
	show aaa	Display AAA configuration information.

aaa group server radius deadline

To improve RADIUS response time when some servers might be unavailable, use the **aaa group server radius deadline** command to cause the storage router to skip the unavailable servers in the specified group immediately. To set the dead time to 0, effectively preventing the storage router from skipping any RADIUS server in the specified group, use the **no** form of this command.

aaa group server radius *name* **deadline** *minutes*

no aaa group server radius *name* **deadline**

Syntax Description		
	<i>name</i>	The name of the group of RADIUS servers. Enter a maximum of 31 characters.
	<i>minutes</i>	The length of time, in minutes, for which a RADIUS server in the specified group is skipped over by the storage router when requesting AAA authentication services, up to a maximum of 1440 minutes (24 hours).

Defaults The dead time is set to zero (0) by default.

Command Modes Administrator.

Command History	Release	Modification
	2.5.1	This command was introduced for the SN 5428.
	3.2.1	This command was introduced for the SN 5428-2.

Usage Guidelines Use this command to cause the storage router to mark as “dead” any RADIUS servers in the specified group that fail to respond to authentication requests, thus avoiding the wait for the authentication request to time out before trying the next configured server. A RADIUS server marked as dead is skipped by additional requests for the specified number of minutes, unless all RADIUS servers in the specified list are marked as dead. If all RADIUS servers in a group are marked as dead, the deadline setting is ignored.

This command overrides the global setting that applies to all configured RADIUS servers. If the deadline is not set for a RADIUS server group, the global dead time setting applies.

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **aaa group server radius deadline** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

Examples The following example specifies a dead time of five minutes for all RADIUS servers in the group named *region2* that fail to respond to AAA authentication requests:

```
[SN5428-2A]# aaa group server radius region6 deadline 5
```

The following example effectively sets a dead time of zero minutes for all RADIUS servers in the group named *region6*. The global dead time value, if set, will apply to all RADIUS server in the group.

```
[SN5428-2A]# no aaa group server radius region6 deadline
```

Related Commands	Command	Description
	radius-server deadline	Specify the length of time the storage router can skip a RADIUS server that is marked as unavailable.
	show aaa	Display AAA configuration information.

aaa group server radius server

To add a RADIUS server to a named group of RADIUS servers to be used for AAA authentication, use the **aaa group server radius server** command. To remove a RADIUS server from an existing group of RADIUS servers, use the **no** form of this command.

aaa group server radius *name server ip-address* [**auth-port** *port-number*]

no aaa group server radius *name server ip-address* [**auth-port** *port-number*]

Syntax Description

<i>name</i>	The name of the group of RADIUS servers. Enter a maximum of 31 characters.
<i>ip-address</i>	The IP address of the RADIUS server.
auth-port <i>port-number</i>	(Optional) The UDP destination port for authentication requests. If unspecified, the port number defaults to 1645.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
2.5.1	This command was introduced for the SN 5428.
3.2.1	This command was introduced for the SN 5428-2.

Usage Guidelines

Use this command to add a RADIUS server to a group of RADIUS servers to be used for AAA authentication. Use the **radius-server host** command to define a RADIUS server for use by the storage router.

During authentication, the servers are accessed in the order in which they are added to the group.



Note

Verification of IP addresses in a server group occurs only at runtime. If a RADIUS server group contains an IP address that is not defined as a RADIUS server, the authentication process generates error messages and the IP address is skipped. This could cause unexpected authentication failures.

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **aaa group server radius server** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

Examples

The following example identifies the servers with IP address *10.5.0.53* and *10.6.0.61* as RADIUS servers, using the default port for authentication. It creates a RADIUS server group named *region2* and adds the previously configured RADIUS servers to the *region2* group.

```
[SN5428-2A]# radius-server host 10.5.0.53
[SN5428-2A]# radius-server host 10.6.0.61
[SN5428-2A]# aaa group server radius region2
[SN5428-2A]# aaa group server radius region2 server 10.5.0.53
[SN5428-2A]# aaa group server radius region2 server 10.6.0.61
```

The following example removes the RADIUS server with IP address *10.5.0.53* from the RADIUS server group named *region2*:

```
[SN5428-2A]# no aaa group server radius region2 server 10.5.0.53
```

Related Commands

Command	Description
aaa authentication enable	Configure AAA authentication services for Administrator mode access to the storage router via the CLI enable command.
aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
aaa authentication login	Configure AAA authentication services for Monitor mode access to the storage router via the CLI.
aaa group server radius	Create a named group of RADIUS servers for AAA authentication services.
aaa group server radius deadline	Specify the length of time the storage router can skip a RADIUS server in the named group that is marked as unavailable.
aaa test authentication	Enable testing of the specified AAA authentication list.
radius-server deadline	Specify the length of time the storage router can skip a RADIUS server that is marked as unavailable.
radius-server host	Configure remote RADIUS servers for AAA authentication services.
radius-server key	Sets the global authentication and encryption key for all RADIUS communications between the storage router and the RADIUS daemon.
radius-server retransmit	Specifies how many times the storage router resends the RADIUS request to a server before giving up.
radius-server timeout	Sets the interval the storage router waits for a RADIUS server to reply before retransmitting.
restore aaa	Restore AAA authentication services from the named configuration file.
save aaa	Save the current AAA configuration information.
scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
show aaa	Display AAA configuration information.

aaa group server tacacs+

To create a named group of TACACS+ servers to be used for AAA authentication, use the **aaa group server tacacs+** command. To disable an existing group of TACACS+ servers, use the **no** form of this command.

aaa group server tacacs+ name

no aaa group server tacacs+ name

Syntax Description

<i>name</i>	The name of the group of TACACS+ servers to be used for AAA authentication. Enter a maximum of 31 characters.
-------------	---

Defaults

None. All configured TACACS+ servers belong to the group named *tacacs+*.

Command Modes

Administrator.

Command History

Release	Modification
2.5.1	This command was introduced for the SN 5428.
3.2.1	This command was introduced for the SN 5428-2.

Usage Guidelines

Use this command to create a subset of TACACS+ servers to be used for AAA authentication. The named group can then be added to a AAA authentication methods list, allowing the specified set of TACACS+ servers to be used for authentication. After creating the named group, use the **aaa group server tacacs+ server** command to add a TACACS+ server to the group.

Use the **tacacs-server host** command to configure a TACACS+ server to be used by the storage router for AAA authentication.

Group names must be unique across the storage router; you cannot have a group of TACACS+ servers named *labauth* and a group of RADIUS servers named *labauth*. The default group name of *tacacs+* includes all configured TACACS+ servers.

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **aaa group server tacacs+** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

Examples

The following example creates a TACACS+ server group named *region3*:

```
[SN5428-2A]# aaa group server tacacs+ region3
```

Related Commands	Command	Description
	aaa authentication enable	Configure AAA authentication services for Administrator mode access to the storage router via the CLI enable command.
	aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
	aaa authentication login	Configure AAA authentication services for Monitor mode access to the storage router via the CLI.
	aaa group server tacacs+ server	Add the specified TACACS+ server to the named TACACS+ server group.
	aaa test authentication	Enable testing of the specified AAA authentication list.
	restore aaa	Restore AAA authentication services from the named configuration file.
	save aaa	Save the current AAA configuration information.
	scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
	show aaa	Display AAA configuration information.
	tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.
	tacacs-server key	Sets the global authentication and encryption key for all TACACS+ communications between the storage router and the TACACS+ daemon.
	tacacs-server timeout	Sets the interval the storage router waits for a TACACS+ server to reply.

aaa group server tacacs+ server

To add a TACACS+ server to a named group of TACACS+ servers to be used for AAA authentication, use the **aaa group server tacacs+ server** command. To remove a RADIUS server from an existing group of TACACS+ servers, use the **no** form of this command.

aaa group server tacacs+ name server ip-address [auth-port port-number]

no aaa group server tacacs+ name server ip-address [auth-port port-number]

Syntax Description

<i>name</i>	The name of the group of TACACS+ servers. Enter a maximum of 31 characters.
<i>ip-address</i>	The IP address of the TACACS+ server.
auth-port <i>port-number</i>	(Optional) The server port number. Valid port numbers range from 1 to 65535. If unspecified, the port number defaults to 49.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
2.5.1	This command was introduced for the SN 5428.
3.2.1	This command was introduced for the SN 5428-2.

Usage Guidelines

Use this command to add a TACACS+ server to a group of TACACS+ servers to be used for AAA authentication. Use the **tacacs-server host** command to define a TACACS+ server for use by the storage router.

During authentication, the servers are accessed in the order in which they are added to the group.



Note

Verification of IP addresses in a server group occurs only at runtime. If a TACACS+ server group contains an IP address that is not defined as a TACACS+ server, the authentication process generates error messages and the IP address is skipped. This could cause unexpected authentication failures.

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **aaa group server tacacs+ server** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

Examples

The following example identifies the servers with IP address *172.29.39.46* and *10.7.0.72* as TACACS+ servers, using the default port for authentication. It creates a TACACS+ server group named *region3* and adds the previously configured TACACS+ servers to the *region3* group.

```
[SN5428-2A] # tacacs-server host 172.29.39.46
[SN5428-2A] # tacacs-server host 10.7.0.72
[SN5428-2A] # aaa group server tacacs+ region3
[SN5428-2A] # aaa group server tacacs+ region3 server 172.29.39.46
[SN5428-2A] # aaa group server tacacs+ region3 server 10.7.0.72
```

The following example removes the TACACS+ server with IP address *10.7.0.72* from the TACACS+ server group named *region3*:

```
[SN5428-2A] # no aaa group server tacacs+ region3 server 10.7.0.72
```

Related Commands

Command	Description
aaa authentication enable	Configure AAA authentication services for Administrator mode access to the storage router via the CLI enable command.
aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
aaa authentication login	Configure AAA authentication services for Monitor mode access to the storage router via the CLI.
aaa group server tacacs+	Create a named group of TACACS+ servers for AAA authentication services.
aaa test authentication	Enable testing of the specified AAA authentication list.
restore aaa	Restore AAA authentication services from the named configuration file.
save aaa	Save the current AAA configuration information.
scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
show aaa	Display AAA configuration information.
tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.
tacacs-server key	Sets the global authentication and encryption key for all TACACS+ communications between the storage router and the TACACS+ daemon.
tacacs-server timeout	Sets the interval the storage router waits for a TACACS+ server to reply.

aaa new-model

To enable the AAA access control model, issue the **aaa new-model** command.

aaa new-model

no aaa new-model

Syntax Description This command has no arguments or keywords.

Defaults AAA is enabled. AAA cannot be disabled on the storage router.

Command Modes Administrator.

Command History

Release	Modification
2.2.1	This command was introduced for the SN 5428.
3.2.1	This command was introduced for the SN 5428-2.

Usage Guidelines

This command enables the AAA access control model. The **no aaa new-model** command is available for completeness only; AAA cannot be disabled for the storage router.

AAA authentication services are used to provide the following authentication types:

- iSCSI authentication—provides authentication of IP hosts requiring access to storage via SCSI routing instances
- Login authentication—provides authentication of users requiring Monitor mode access to the storage router via the CLI
- Enable authentication—provides authentication of users requiring Administrator mode access to the storage router via the CLI **enable** command

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **aaa new-model** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

Examples

The following example initializes AAA:

```
[SN5428-2A]# aaa new-model
```

Related Commands	Command	Description
	aaa authentication enable	Configure AAA authentication services for Administrator mode access to the storage router via the CLI enable command.
	aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
	aaa authentication login	Configure AAA authentication services for Monitor mode access to the storage router via the CLI.
	aaa group server radius	Create a named group of RADIUS servers for AAA authentication services.
	aaa group server tacacs+	Create a named group of TACACS+ servers for AAA authentication services.
	aaa test authentication	Enable testing of the specified AAA authentication list.
	debug aaa	Enable debugging for the AAA authentication services.
	radius-server host	Configure remote RADIUS servers for AAA authentication services.
	restore aaa	Restore AAA authentication services from the named configuration file.
	save aaa	Save the current AAA configuration information.
	scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
	show aaa	Display AAA configuration information.
	tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.

aaa test authentication

To test authentication using the specified authentication list, use the **aaa test authentication** command.

```
aaa test authentication {enable | login} default username password
```

```
aaa test authentication iscsi {listname | default} username password
```

```
aaa test authentication cancel
```

Syntax Description		
enable default	Use the services in the Enable authentication list for testing. The name of the list must be <i>default</i> .	
login default	Use the services in the Login authentication list for testing. The name of the list must be <i>default</i> .	
iscsi listname	Use the services in the named iSCSI authentication list for testing.	
iscsi default	Use the services in the iSCSI authentication list for testing. The name of the list must be <i>default</i> .	
<i>username</i>	The user name to be tested.	
<i>password</i>	The password associated with the specified user name.	
cancel	Cancel any outstanding test authentication requests.	

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	2.2.1	This command was introduced for the SN 5428.
	2.5.1	The enable and login keywords, and the <i>listname</i> variable, were added.
	3.2.1	This command was introduced for the SN 5428-2.

Usage Guidelines AAA uses the services in the specified authentication list to perform Enable, Login or iSCSI authentication. Use this command to test iSCSI authentication prior to enabling authentication for SCSI routing instances or for troubleshooting purposes.

Use the **cancel** keyword to terminate any outstanding test authentication requests. For example, if a RADIUS or TACACS+ server is configured with a very long timeout value, you can cancel the request rather than waiting for the timeout to occur.

In a cluster environment, AAA management functions are handled by a single storage router. To determine which storage router is performing AAA management functions, issue the **show cluster** command. If you issue the **aaa test authentication** command from a storage router that is not performing AAA management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

Examples

The following example tests iSCSI authentication using the default authentication list for the user named *user1*, with a password of *password1*:

```
[SN5428-2A]# aaa test authentication iscsi default user1 password1
```

The following example tests iSCSI authentication using the authentication list named *webtest1*, for the user named *user2*, with a password of *password2*:

```
[SN5428-2A]# aaa test authentication iscsi webtest1 user2 password2
```

The following example tests Enable authentication for the user named *\$enab15\$*, with a password of *admin*:

```
[SN5428-2A]# aaa test authentication enable default $enab15$ admin
```

The following example tests Login authentication for the user named *monitor*, with a password of *cisco*:

```
[SN5428-2A]# aaa test authentication login default monitor cisco
```

Related Commands

Command	Description
aaa authentication enable	Configure AAA authentication services for Administrator mode access to the storage router via the CLI enable command.
aaa authentication iscsi	Configure the AAA authentication services to be used for iSCSI authentication.
aaa authentication login	Configure AAA authentication services for Monitor mode access to the storage router via the CLI.
aaa group server radius	Create a named group of RADIUS servers for AAA authentication services.
aaa group server tacacs+	Create a named group of TACACS+ servers for AAA authentication services.
debug aaa	Enable debugging for the AAA authentication services.
radius-server host	Configure remote RADIUS servers for AAA authentication services.
restore aaa	Restore AAA authentication services from the named configuration file.
save aaa	Save current AAA configuration information.
scsirouter authentication	Enable iSCSI authentication for the named SCSI routing instance.
show aaa	Display AAA configuration information.
tacacs-server host	Configure remote TACACS+ servers for AAA authentication services.

accesslist

To create an access list entity, use the **accesslist** command.

accesslist *name*

Syntax Description

<i>name</i>	The name of the access list entity created by this command. Enter a maximum of 31 characters.
-------------	---

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
2.2.1	This command was introduced for the SN 5428.
3.2.1	This command was introduced for the SN 5428-2.

Usage Guidelines

Access lists identify the IP hosts allowed to access a common set of storage resources and are associated with specific storage targets. IP hosts can be identified by:

- IP address
- CHAP user name (used for iSCSI authentication)
- iSCSI Name

An access list can contain one or more types of identification entries. If an identification entry type exists in the access list, the IP host attempting to access the associated storage target must have a matching entry defined in the access list. For example, if an access list contains both IP address and iSCSI Name identification entry types, then every IP host that requires access to the associated set of storage resources must have a matching IP address and iSCSI Name entry in the access list.

There is a maximum of 100 access lists per storage router or per storage router cluster. There is a maximum of 200 access list identification entries across all access lists in the storage router or storage router cluster.



Note

If there is a CHAP user name entry in the access list, the SCSI routing instance used to access the storage target must also have iSCSI authentication enabled. Refer to the appropriate *Cisco Storage Router Software Configuration Guide* for your storage router model for more information about AAA and iSCSI authentication.

In a cluster environment, access list management functions are handled by a single storage router. To determine which storage router is performing access list management functions, issue the **show cluster** command. If you issue an **accesslist** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

Refer to the appropriate *Cisco Storage Router Software Configuration Guide* for your storage router model for more information about operating the storage router in a cluster.

Examples

The following command creates an access list named *webserver2*:

```
[SN5428-2A] # accesslist webserver2
```

Related Commands

Command	Description
accesslist A.B.C.D/bits	Add IP addresses to an access list.
accesslist chap-username	Add CHAP user name entries to an access list.
accesslist description	Add a description to an access list.
accesslist iscsi-name	Add iSCSI Name entries to an access list.
delete accesslist	Delete a specific access list entry or an entire access list.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
save accesslist	Save configuration data for the named access list or all access lists.
scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
show accesslist	Display the contents of the named access list or all access lists.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

accesslist A.B.C.D/bits

To add the IP address and subnet mask of IP hosts to the named access list, use the **accesslist A.B.C.D/bits** command.

```
accesslist name A.B.C.D/bits | A.B.C.D/1.2.3.4 [A.B.C.D/bits | A.B.C.D/1.2.3.4] . . .
[A.B.D.F/bits | A.B.C.D/1.2.3.4]
```

Syntax Description

<i>name</i>	The name of an access list to which you are adding information.
<i>A.B.C.D/bits</i>	IP address and subnet mask of the IP host being added to the access list. <i>A.B.C.D</i> is the dotted quad notation of the IP address. The <i>/bits</i> specifies the subnet mask in CIDR style.
<i>A.B.C.D/1.2.3.4</i>	The IP address and subnet mask of the IP host being added to the access list. <i>A.B.C.D</i> is the dotted quad notation of the IP address. <i>1.2.3.4</i> is the dotted quad notation of the subnet mask.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
2.2.1	This command was introduced for the SN 5428.
3.2.1	This command was introduced for the SN 5428-2.

Usage Guidelines

Use the **accesslist A.B.C.D/bits** command after creating an access list to populate the list with IP address entries. Enter multiple addresses and masks, separating each by a space.

Access lists identify the IP hosts allowed to access a common set of storage resources and are associated with specific storage targets. IP hosts can be identified by:

- IP address
- CHAP user name (used for iSCSI authentication)
- iSCSI Name

An access list can contain one or more types of identification entries. If an identification entry type exists in the access list, the IP host attempting to access the associated storage target must have a matching entry defined in the access list. For example, if an access list contains both IP address and iSCSI Name identification entry types, then every IP host that requires access to the associated set of storage resources must have a matching IP address and iSCSI Name entry in the access list.

There is a maximum of 100 access lists per storage router or per storage router cluster. There is a maximum of 200 access list identification entries across all access lists in the storage router or storage router cluster.

In a cluster environment, access list management functions are handled by a single storage router. To determine which storage router is performing access list management functions, issue the **show cluster** command. If you issue an **accesslist A.B.C.D/bits** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

Refer to the appropriate *Cisco Storage Router Software Configuration Guide* for your storage router model for more information about operating the storage router in a cluster.

Examples

The following commands add the specified entries to the named access lists:

```
[SN5428-2A]# accesslist myAccessList 192.168.54.12/32 192.168.54.15/32
*[SN5428-2A]# accesslist Webserver5 209.165.201.1/255.255.255.0
209.165.201.5/255.255.255.0
```

Related Commands

Command	Description
accesslist	Create an access list entity.
accesslist chap-username	Add CHAP user name entries to an access list.
accesslist description	Add a description to an access list.
accesslist iscsi-name	Add iSCSI Name entries to an access list.
delete accesslist	Delete a specific access list entry or an entire access list.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
save accesslist	Save configuration data for the named access list or all access lists.
scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
show accesslist	Display the contents of the named access list or all access lists.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

accesslist chap-username

To add the CHAP user name of IP hosts to the named access list, use the **accesslist chap-username** command.

```
accesslist name chap-username username
```

Syntax Description	
<i>name</i>	The name of an access list to which you are adding information.
<i>username</i>	The CHAP user name (used for iSCSI authentication purposes) configured for the IP host that requires access to storage.

Defaults	
	None.

Command Modes	
	Administrator.

Command History	Release	Modification
	2.3.1	This command was introduced for the SN 5428.
	3.2.1	This command was introduced for the SN 5428-2.

Usage Guidelines

Use the **accesslist chap-username** command after creating an access list to populate the list with CHAP user name entries. A CHAP user name is required for iSCSI authentication.

Access lists identify the IP hosts allowed to access a common set of storage resources and are associated with specific storage targets. IP hosts can be identified by:

- IP address
- CHAP user name (used for iSCSI authentication)
- iSCSI Name

An access list can contain one or more types of identification entries. If an identification entry type exists in the access list, the IP host attempting to access the associated storage target must have a matching entry defined in the access list. For example, if an access list contains both IP address and iSCSI Name identification entry types, then every IP host that requires access to the associated set of storage resources must have a matching IP address and iSCSI Name entry in the access list.

There is a maximum of 100 access lists per storage router or per storage router cluster. There is a maximum of 200 access list identification entries across all access lists in the storage router or storage router cluster.

The iSCSI driver is configured with a CHAP user name and password when SCSI routing instances have iSCSI authentication enabled. AAA authentication services authenticate the IP host using the CHAP user name and password. An access list can also use the CHAP user name to identify IP hosts allowed access to a common set of storage resources.

**Note**

If there is a CHAP user name entry in the access list, the SCSI routing instance used to access the storage target must also have iSCSI authentication enabled. Refer to the appropriate *Cisco Storage Router Software Configuration Guide* for your storage router model for more information about AAA and iSCSI authentication.

In a cluster environment, access list management functions are handled by a single storage router. To determine which storage router is performing access list management functions, issue the **show cluster** command. If you issue an **accesslist chap-username** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

Refer to the appropriate *Cisco Storage Router Software Configuration Guide* for your storage router model for more information about operating the storage router in a cluster.

Examples

The following commands add the specified entries to the named access lists:

```
[SN5428-2A] # accesslist myAccessList chap-username foo
*[SN5428-2A] # accesslist Webserv5 chap-username server1
```

Related Commands

Command	Description
accesslist	Create an access list entity.
accesslist A.B.C.D/bits	Add IP addresses to an access list.
accesslist description	Add a description to an access list.
accesslist iscsi-name	Add iSCSI Names to an access list.
delete accesslist	Delete a specific access list entry or an entire access list.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
save accesslist	Save configuration data for the named access list or all access lists.
scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
show accesslist	Display the contents of the named access list or all access lists.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

accesslist description

To add a description to an existing access list entity, use the **accesslist description** command.

```
accesslist name description "text"
```

Syntax Description

<i>name</i>	The name of an existing access list entity.
<i>text</i>	User-defined identification information associated with this access list. Enclose the description string in quotes. Enter a maximum of 64 characters.

Defaults

None.

Command Modes

Administrator.

Command History

Release	Modification
2.2.1	This command was introduced for the SN 5428.
3.2.1	This command was introduced for the SN 5428-2.

Usage Guidelines

Access lists identify the IP hosts allowed to access a common set of storage resources and are associated with specific storage targets. IP hosts can be identified by:

- IP address
- CHAP user name (used for iSCSI authentication)
- iSCSI Name

An access list can contain one or more types of identification entries. If an identification entry type exists in the access list, the IP host attempting to access the associated storage target must have a matching entry defined in the access list. For example, if an access list contains both IP address and iSCSI Name identification entry types, then every IP host that requires access to the associated set of storage resources must have a matching IP address and iSCSI Name entry in the access list.

There is a maximum of 100 access lists per storage router or per storage router cluster. There is a maximum of 200 access list identification entries across all access lists in the storage router or storage router cluster.

In a cluster environment, access list management functions are handled by a single storage router. To determine which storage router is performing access list management functions, issue the **show cluster** command. If you issue an **accesslist description** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

Refer to the appropriate *Cisco Storage Router Software Configuration Guide* for your storage router model for more information about operating the storage router in a cluster.

Examples

The following command adds a description to the access list named *webserver2*:

```
[SN5428-2A]# accesslist webserver2 description "Access list for company web servers"
```

Related Commands

Command	Description
accesslist	Create an access list entity.
accesslist A.B.C.D/bits	Add IP addresses to an access list.
accesslist chap-username	Add CHAP user name entries to an access list.
accesslist iscsi-name	Add iSCSI Name entries to an access list.
delete accesslist	Delete a specific access list entry, or an entire access list.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
save accesslist	Save configuration data for the named access list or all access lists.
scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
show accesslist	Display the contents of the named access list or all access lists.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

accesslist iscsi-name

To add the iSCSI Name of IP hosts to the named access list, use the **accesslist iscsi-name** command.

```
accesslist name iscsi-name string
```

Syntax Description		
<i>name</i>		The name of an access list to which you are adding information.
<i>string</i>		The iSCSI Name of IP host that requires access to storage. The iSCSI Name is a UTF-8 character string based on iSCSI functional requirements. It is a location-independent permanent identifier for an iSCSI node. An iSCSI node can be either an initiator, a target, or both.

Defaults	None.
----------	-------

Command Modes	Administrator.
---------------	----------------

Command History	Release	Modification
	2.3.1	This command was introduced for the SN 5428.
	3.2.1	This command was introduced for the SN 5428-2.

Usage Guidelines Use the **accesslist iscsi-name** command after creating an access list to populate the list with iSCSI Name entries.

If you do not know the iSCSI Name of the IP host, configure the IP host and attempt to access the desired storage targets. Use the **show scsirouter** command with the **host table** keywords to then display the iSCSI Name (along with the initiator alias, IP address and CHAP user name) of all IP hosts that have attempted to access storage resources.

Access lists identify the IP hosts allowed to access a common set of storage resources and are associated with specific storage targets. IP hosts can be identified by:

- IP address
- CHAP user name (used for iSCSI authentication)
- iSCSI Name

An access list can contain one or more types of identification entries. If an identification entry type exists in the access list, the IP host attempting to access the associated storage target must have a matching entry defined in the access list. For example, if an access list contains both IP address and iSCSI Name identification entry types, then every IP host that requires access to the associated set of storage resources must have a matching IP address and iSCSI Name entry in the access list.

There is a maximum of 100 access lists per storage router or per storage router cluster. There is a maximum of 200 access list identification entries across all access lists in the storage router or storage router cluster.

In a cluster environment, access list management functions are handled by a single storage router. To determine which storage router is performing access list management functions, issue the **show cluster** command. If you issue an **accesslist iscsi-name** command from a storage router that is not performing access list management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.

Refer to the appropriate *Cisco Storage Router Software Configuration Guide* for your storage router model for more information about operating the storage router in a cluster.

Examples

The following command add the specified iSCSI Name to the access list named *foo*:

```
[SN5428-2A]# accesslist foo iscsi-name ign.1987-05.com.cisco.01.88e8b25a6bf3372a34567123f
```

Related Commands

Command	Description
accesslist	Create an access list entity.
accesslist A.B.C.D/bits	Add IP addresses to an access list.
accesslist chap-username	Add CHAP user name entries to an access list.
accesslist description	Add a description to an access list.
delete accesslist	Delete a specific access list entry or an entire access list.
restore accesslist	Restore the named access list or all access lists from the named configuration file.
save accesslist	Save configuration data for the named access list or all access lists.
scsirouter target accesslist	Associate an access list with a specific SCSI routing instance target or all targets.
show accesslist	Display the contents of the named access list or all access lists.
show scsirouter	Display configuration and operational information for the named SCSI routing instance.

admin contactinfo

To provide basic contact information for the system administrator of this storage router, use the **admin contactinfo** command.

```
admin contactinfo [name "string" | email "string" | phone "string" | pager "string"]
```

```
admin contact info name "string" email "string" phone "string" pager "string"
```

Syntax Description	name <i>string</i>	(Optional) The name of the storage router administrator.
	email <i>string</i>	(Optional) The e-mail address of the storage router administrator. This is an address to which alerts may be sent.
	phone <i>string</i>	(Optional) The phone number of the storage router administrator.
	pager <i>string</i>	(Optional) The pager number of the storage router administrator.

Defaults None.

Command Modes Administrator.

Command History	Release	Modification
	2.2.1	This command was introduced for the SN 5428.
	3.2.1	This command was introduced for the SN 5428-2.

Usage Guidelines Use the **admin contactinfo** command to provide site-specific information for the storage router system administrator. The command accepts each parameter separately, or all parameters together. If all parameters are specified, they must be in the sequence shown. Usage is completely site-specific.

Enclose each string containing spaces in single or double quotes. If a string contains a single quote, enclose it in double quotes; if it contains a double quote, enclose it in single quotes. A string cannot contain both single and double quotes.

Examples The following commands set the system administrator name and e-mail address:

```
[SN5428-2A]# admin contactinfo name "Pat Hurley"
[SN5428-2A]# admin contactinfo email "hurley@abc123z.com"
```

The following command sets all system administrator contact information:

```
[SN5428-2A]# admin contactinfo name "Chris Smith" email "chris.smith@zxy478x.com" phone
"123.555.5555 ext 97" pager "555.3444 pin 2234"
```

Related Commands	Command	Description
	admin password	Set the login password for administrative access to the storage router management interface.
	restore system	Restore selected system information from the named configuration file.
	save all	Save all configuration information, including the system administrator contact information.
	save system	Save selected system configuration information, including the system administrator contact information.
	show admin	Display system administrator contact information.

admin password

To set the password used for administrative access to the storage router management interface, use the **admin password** command. Access may be via Telnet or SSH (for CLI), or web-based GUI.

admin password *string*

Syntax Description

<i>string</i>	The password associated with administrative access to the storage router management interface. The string can be enclosed in quotes, and must be enclosed in quotes if the password includes one or more spaces. A string value of "" clears the password. The default password is <i>cisco</i> .
---------------	---

Defaults

The default password is *cisco*.

Command Modes

Administrator.

Command History

Release	Modification
2.2.1	This command was introduced for the SN 5428.
3.2.1	This command was introduced for the SN 5428-2.

Usage Guidelines

The management interface is password protected. You must enter passwords when accessing the storage router via Telnet or SSH (for CLI) or web-based GUI. The Monitor mode password provides view-only access to the management interface, while the Administrator mode password allows you to create entities and make changes to the configuration of the storage router. Password protection can also be extended to the storage router console, using the **restrict console** command.

The password can contain one or more spaces, if the password string is enclosed in quotes. A string value of "" clears the password, effectively setting it to nothing.

In a cluster environment, the Administrator mode and Monitor mode passwords are cluster-wide configuration elements and apply to all storage routers in a cluster. The password management functions are handled by a single storage router. To determine which storage router is performing password management functions, issue the **show cluster** command. If you issue the **admin password** command from a storage router that is not performing password management functions, the CLI displays an informational message with the name of the node that is currently handling those functions.



Note

The password is displayed in clear text as the command is entered, but it is changed to a series of number signs (#####) when the change is acknowledged.

Examples

The following example sets the Administrator mode password to *foo73G*. All passwords are case sensitive.

```
[SN5428-2A]# admin password foo73G
```

The following example sets the Administrator mode password to “*xZm! 673*”:

```
[SN5428-2A]# admin password "xZm! 673"
```

Related Commands

Command	Description
aaa generate password	Generate a long random password.
enable	Enter Administrator mode.
exit	Leave Administrator mode and enter Monitor mode.
monitor password	Set the login password for view-only access to the storage router management interface.
restrict console	Enable or disable password checking on the storage router console interface.
save all	Save all configuration information, including the administrator password.
save system	Save selected system configuration information, including the Administrator mode passwords.
setup access	Run the wizard to configure Monitor mode and Administrator mode passwords.

■ admin password