



U Commands

This chapter covers the following commands:

- [username password](#), page 17-2

username password

To build a local user name database for use with the local method of AAA authentication services, use the **username password** command. Use the **no** form of this command to delete the specified user name.

username *user-name* **password** *password-string*

no username *user-name*

Syntax Description

<i>user-name</i>	A valid user name. Enter a maximum of 63 characters.
<i>password-string</i>	The password associated with the specified user name. If the password is encrypted (starts with “9”), enter a maximum of 170 characters. If the password is unencrypted (starts with “0”), enter a maximum of 66 characters. If the password is entered as an unencrypted text string, 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

Use the **username password** command to build the local username database. The AAA authentication service, *local-case*, performs a case-sensitive user name match; the *local* service user name match is not case-sensitive. Both *local* and *local-case* use case-sensitive password matching for authentication.

Use the **aaa authentication iscsi** or **aaa authentication login** command to configure the an authentication list to use *local* or *local-case* authentication services.

To display the contents of the local username database, issue the **show aaa** command.

The following rules apply to passwords:

- Passwords are entered in clear text. However, they are changed to “XXXXXX” in the CLI command history cache, and are stored in the local username database in an encrypted format.
- If the password contains embedded spaces, enclose it with single or double quotes.
- After initial entry, passwords display in their encrypted format. Use the **show aaa** command to display the local username database entries. The following is an example display:

```
username "foo" password "9 ea9bb0c57ca4806d3555f3f78a4204177a"
```

The initial “9” in the example display indicates that the password is encrypted.

- You can re-enter an encrypted password using the normal **username password** command. Enter the encrypted password in single or double quotes, starting with 9 and a single space. For example, copying and pasting password “9 ea9bb0c57ca4806d3555f3f78a4204177a” from the example above into the **username pat** command would create an entry for *pat* in the username database. The user named *pat* would have the same password as the user named *foo*. This functionality allows user names and passwords to be restored from saved configuration files.
- When entering a password, a zero followed by a single space indicates that the following string is not encrypted; 9 followed by a single space indicates that the following string is encrypted. To enter a password that starts with 9 or zero, followed by one or more spaces, enter a zero and a space and then enter the password string. For example, to enter the password “0 123” for the user named *pat*, enter this command:

```
username pat password "0 0 123"
```

To enter the password “9 73Zjm 5” for user name *lab1*, use this command:

```
username lab1 password '0 9 73Zjm 5'
```

Examples

The following example configures two user names (*foo* and *foo2*) and password (*foopassword* and *foo2password*):

```
[SN5428-2A]# username foo password foopassword
[SN5428-2A]# username foo2 password foo2password
```

To display the user name database, issue the **show aaa** command. The following is example output from the **show aaa** command:

```
[SN5428-2A]# show aaa
aaa new-model
aaa authentication iscsi default group tacacs+ local none
username foo password <password>
username foo2 password <password>
```

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 generate password	Generate a long random password.
aaa test authentication	Enable testing of the specified AAA authentication list.
debug aaa	Enable debugging for the 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.

