2

Configuring Username and Password Security

Contents

Overview

Feature	Default	Menu	CLI	Web
Set Usernames	none	—	—	page 2-9
Set a Password	none	page 2-6	page 2-8	page 2-9
Delete Password Protection	n/a	page 2-7	page 2-8	page 2-9
show front-panel-security	n/a	—	page 1-13	—
front-panel-security		—	page 1-13	—
password-clear	enabled	—	page 1-13	—
reset-on-clear	disabled	—	page 1-14	—
factory-reset	enabled	—	page 1-15	—
password-recovery	enabled	—	page 1-15	—

Console access includes both the menu interface and the CLI. There are two levels of console access: Manager and Operator. For security, you can set a *password pair* (username and password) on each of these levels.

Notes

Usernames are optional. Also, in the menu interface, you can configure passwords, but not usernames. To configure usernames, use the CLI or the web browser interface.

Beginning with software release K.12.*xx*, usernames and passwords for Manager and Operator access can also be configured using SNMP. For more information, refer to "Using SNMP To View and Configure Switch Authentication Features" on page 6-21.

Level	Actions Permitted
Manager:	Access to all console interface areas. *This is the default level.* That is, if a Manager password has *not* been set prior to starting the current console session, then anyone having access to the console can access any area of the console interface.
Operator:	Access to the Status and Counters menu, the Event Log, and the CLI*, but no Configuration capabilities. On the Operator level, the configuration menus, Download OS, and Reboot Switch options in the Main Menu are not available.

*Allows use of the ping, link-test, show, menu, exit, and logout commands, plus the enable command if you can provide the Manager password.

To configure password security:

1. Set a Manager password pair (and an Operator password pair, if applicable for your system).
2. Exit from the current console session. A Manager password pair will now be needed for full access to the console.

If you do steps 1 and 2, above, then the next time a console session is started for either the menu interface or the CLI, a prompt appears for a password. Assuming you have protected both the Manager and Operator levels, the level of access to the console interface will be determined by which password is entered in response to the prompt.

If you set a Manager password, you may also want to configure an inactivity timer. This causes the console session to end after the specified period of inactivity, thus giving you added security against unauthorized console access. You can use either of the following to set the inactivity timer:

- **Menu Interface:** System Information screen (Select "2. Switch Configuration.)
- **CLI:** Use the **console inactivity-timer < 0 | 1 | 5 | 10 | 15 | 20 | 30 | 60 | 120 >**

Notes

The manager and operator passwords and (optional) usernames control access to the menu interface, CLI, and web browser interface.

If you configure only a Manager password (with no Operator password), and in a later session the Manager password is not entered correctly in response to a prompt from the switch, then the switch does not allow management access for that session.

If the switch has a password for both the Manager and Operator levels, and neither is entered correctly in response to the switch's password prompt, then the switch does not allow management access for that session.

Passwords are case-sensitive.

When configuring an operator or manager password a message will appear indicating that (USB) autorun has been disabled. For more information on the autorun feature, refer to the Appendix A on "File Transfers" in the *Management and Configuration Guide* for your switch.

Caution

If the switch has neither a Manager nor an Operator password, anyone having access to the switch through either Telnet, the serial port, or the web browser interface can access the switch with full manager privileges. Also, if you configure only an Operator password, entering the Operator password enables full manager privileges.

The rest of this chapter covers how to:

- Set passwords
- Delete passwords
- Recover from a lost password
- Maintain front-panel security

Configuring Local Password Security

Menu: Setting Passwords

As noted earlier in this section, usernames are optional. Configuring a username requires either the CLI or the web browser interface.

1. From the Main Menu select:

   3. Console Passwords

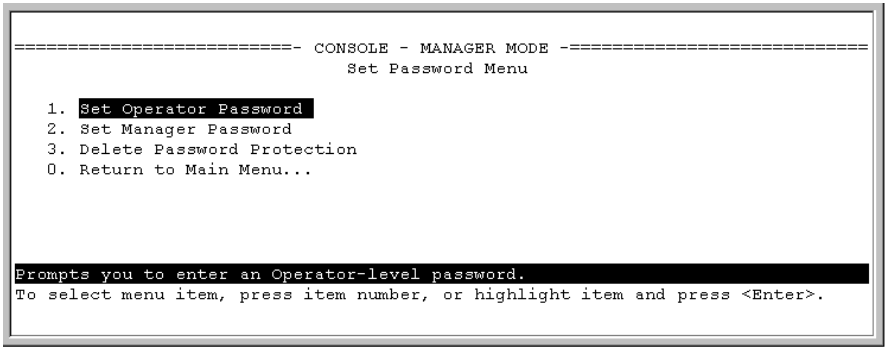


Figure 2-1. The Set Password Screen

2. To set a new password:
   a. Select **Set Manager Password** or **Set Operator Password**. You will then be prompted with **Enter new password**.
   b. Type a password of up to 16 ASCII characters with no spaces and press **[Enter]**. (Remember that passwords are case-sensitive.)
   c. When prompted with **Enter new password again**, retype the new password and press **[Enter]**.

After you configure a password, if you subsequently start a new console session, you will be prompted to enter the password. (If you use the CLI or web browser interface to configure an optional username, the switch will prompt you for the username, and then the password.)

To Delete Password Protection (Including Recovery from a Lost Password): This procedure deletes *all* usernames (if configured) and passwords (Manager and Operator).

If you have physical access to the switch, press and hold the Clear button (on the front of the switch) for a minimum of one second to clear all password protection, then enter new passwords as described earlier in this chapter.

If you do not have physical access to the switch, you will need Manager-Level access:

1. Enter the console at the Manager level.
2. Go to the **Set Passwords** screen as described above.
3. Select **Delete Password Protection**. You will then see the following prompt:

   Continue Deletion of password protection? No

4. Press the Space bar to select **Yes**, then press **[Enter]**.
5. Press **[Enter]** to clear the Password Protection message.

To Recover from a Lost Manager Password: If you cannot start a console session at the Manager level because of a lost Manager password, you can clear the password by getting physical access to the switch and pressing and holding the Clear button for a minimum of one second. This action deletes all passwords and usernames (Manager and Operator) used by both the console and the web browser interface.

CLI: Setting Passwords and Usernames

Commands Used in This Section

password	See below.

Configuring Manager and Operator Passwords.

Note

The password command has changed. You can now configure manager and operator passwords in one step. See "Saving Security Credentials in a Config File" on page 2-10 of this guide.

Syntax: [no] password <manager | operator | all | port-access>
[*user-name ASCII-STR*] [<plaintext | sha1> ASCII-STR]

```
ProCurve(config)# password manager
New password: *******
Please retype new password: *******
ProCurve(config)# password operator
New password: ********
Please retype new password: ********
```

- Password entries appear as asterisks.
- You must type the password entry twice.

Figure 2-2. Example of Configuring Manager and Operator Passwords

To Remove Password Protection. Removing password protection means to eliminate password security. This command prompts you to verify that you want to remove one or both passwords, then clears the indicated password(s). (This command also clears the username associated with a password you are removing.) For example, to remove the Operator password (and username, if assigned) from the switch, you would do the following:

```
ProCurve(config)# no password
Password protection will be deleted, do you want to continue [y/n]? y
ProCurve(config)#
```

Press **[Y]** (for yes) and press **[Enter]**.

Figure 2-3. Removing a Password and Associated Username from the Switch

The effect of executing the command in figure 2-3 is to remove password protection from the Operator level. (This means that anyone who can access the switch console can gain Operator access without having to enter a username or password.)

If you want to remove both operator and manager password protection, use the **no password all** command.

Web: Setting Passwords and Usernames

In the web browser interface you can enter passwords and (optional) usernames.

To Configure (or Remove) Usernames and Passwords in the Web Browser Interface.

1. Click on the **Security** tab.

Click on **[Device Passwords]**.

2. Do one of the following:
   - To set username and password protection, enter the usernames and passwords you want in the appropriate fields.
   - To remove username and password protection, leave the fields blank.
3. Implement the usernames and passwords by clicking on **[Apply Changes]**.

SNMP: Setting Passwords and Usernames

Beginning with software release K.12.*xx*, usernames and passwords for Manager and Operator access can also be configured using SNMP. For more information, refer to “Using SNMP To View and Configure Switch Authentication Features” on page 6-21.

Saving Security Credentials in a Config File

You can store and view the following security settings in the running-config file associated with the current software image by entering the **include-credentials** command (formerly this information was stored only in internal flash memory):

- Local manager and operator passwords and (optional) user names that control access to a management session on the switch through the CLI, menu interface, or web browser interface
- SNMP security credentials used by network management stations to access a switch, including authentication and privacy passwords
- Port-access passwords and usernames used as 802.1X authentication credentials for access to the switch
- TACACS+ encryption keys used to encrypt packets and secure authentication sessions with TACACS+ servers
- RADIUS shared secret (encryption) keys used to encrypt packets and secure authentication sessions with RADIUS servers
- Secure Shell (SSH) public keys used to authenticate SSH clients that try to connect to the switch.

Benefits of Saving Security Credentials

The benefits of including and saving security credentials in a configuration file are as follows:

- After making changes to security parameters in the running configuration, you can experiment with the new configuration and, if necessary, view the new security settings during the session. After verifying the configuration, you can then save it permanently by writing the settings to the startup-config file.
- By permanently saving a switch's security credentials in a configuration file, you can upload the file to a TFTP server or Xmodem host, and later download the file to the ProCurve switches on which you want to use the same security settings without having to manually configure the settings (except for SNMPv3 user parameters) on each switch.

- By storing different security settings in different files, you can test different security configurations when you first download a new software version that supports multiple configuration files, by changing the configuration file used when you reboot the switch.

For more information about how to experiment with, upload, download, and use configuration files with different software versions, refer to the following:

- The chapter on "Switch Memory and Configuration" in the *Management and Configuration Guide*.
- "Configuring Local Password Security" on page 2-6 in this guide.

Enabling the Storage and Display of Security Credentials

To enable the security settings, enter the **include-credentials** command.

Syntax: [no] include-credentials

Enables the inclusion and display of the currently configured manager and operator usernames and passwords, RADIUS shared secret keys, SNMP and 802.1X authenticator (port-access) security credentials, and SSH client public-keys in the running configuration. (Earlier software releases store these security configuration settings only in internal flash memory and do not allow you to include and view them in the running-config file.)

To view the currently configured security settings in the running configuration, enter one of the following commands:

- **show running-config**: *Displays the configuration settings in the current running-config file.*
- **write terminal**: *Displays the configuration settings in the current running-config file.*

For more information, refer to "Switch Memory and Configuration" in the Management and Configuration Guide.

*The "***no***" form of the command disables only the display and copying of these security parameters from the running configuration, while the security settings remain active in the running configuration.*

Default: The security credentials described in "Security Settings that Can Be Saved" on page 2-11 are not stored in the running configuration.

Security Settings that Can Be Saved

The security settings that can be saved to a configuration file are:

- Local manager and operator passwords and user names

- SNMP security credentials, including SNMPv1 community names and SNMPv3 usernames, authentication, and privacy settings
- 802.1X port-access passwords and usernames
- TACACS+ encryption keys
- RADIUS shared secret (encryption) keys
- Public keys of SSH-enabled management stations that are used by the switch to authenticate SSH clients that try to connect to the switch

Local Manager and Operator Passwords

The information saved to the running-config file when the **include-credentials** command is entered includes:

```
password manager [user-name <name>] <hash-type> <pass-hash>
password operator [user-name <name>] <hash-type> <pass-hash>
```

where
<*name*> is an alphanumeric string for the user name assigned to the manager or operator.
<*hash-type*> indicates the type of hash algorithm used: SHA-1 or plain text.
<*pass-hash*> is the SHA-1 authentication protocol's hash of the password or clear ASCII text.

For example, a manager username and password may be stored in a running-config file as follows:

```
 password manager user-name George SHA1
2fd4e1c67a2d28fced849ee1bb76e7391b93eb12
```

Use the **write memory** command to save the password configurations in the startup-config file. The passwords take effect when the switch boots with the software version associated with that configuration file.

Caution

If a startup configuration file includes other security credentials, but does not contain a manager or operator password, the switch will not have password protection and can be accessed through Telnet, the serial port, or web interface with full manager privileges.

Password Command Options

The **password** command has the following options:

Syntax: [no] password <manager | operator | port-access> [user-name <*name*>] <*hash-type*> <*password*>

Set or clear a local username/password for a given access level.

manager: *configures access to the switch with manager-level privileges.*

operator: *configures access to the switch with operator-level privileges.*

port-access: *configures access to the switch through 802.1X authentication with operator-level privileges.*

user-name <*name***>***: the optional text string of the user name associated with the password.*

<*hash-type*>*: specifies the type of algorithm (if any) used to hash the password. Valid values are* **plaintext** *or* **sha-1**

<*password*>*: the clear ASCII text string or SHA-1 hash of the password.*

You can enter a manager, operator, or 802.1X port-access password in clear ASCII text or hashed format. However, manager and operator passwords are displayed and saved in a configuration file only in hashed format; port-access passwords are displayed and saved only as plain ASCII text.

After you enter the complete command syntax, the password is set. You are not prompted to enter the password a second time.

This command enhancement allows you to configure manager, operator, and 802.1X port-access passwords in only one step (instead of entering the **password** command and then being prompted twice to enter the actual password).

- For more information about configuring local manager and operator passwords, refer to “Configuring Username and Password Security” on page 2-1 in this guide.
- For more information about configuring a port-access password for 802.1X client authentication, see “802.1X Port-Access Credentials” on page 2-15 in this guide.

SNMP Security Credentials

SNMPv1 community names and write-access settings, and SNMPv3 usernames continue to be saved in the running configuration file even when you enter the **include-credentials** command.

In addition, the following SNMPv3 security parameters are also saved:

```
snmpv3 user "<name>" [auth <md5|sha> "<auth-pass>"]
[priv "<priv-pass>"]
```

where:
<*name*> is the name of an SNMPv3 management station.
[**auth** <**md5** | **sha**>] is the (optional) authentication method used for the management station.
<*auth-pass*> is the hashed authentication password used with the configured authentication method.
[**priv** <*priv-pass*>] is the (optional) hashed privacy password used by a privacy protocol to encrypt SNMPv3 messages between the switch and the station.

The following example shows the additional security credentials for SNMPv3 users that can be saved in a running-config file:

```
snmpv3 user boris \
auth md5 "9e4cfef901f21cf9d21079debeca453" \
priv "82ca4dc99e782db1a1e914f5d8f16824"

snmpv3 user alan \
auth sha "8db06202b8f293e9bc0c00ac98cf91099708ecdf" \
priv "5bc4313e9fd7c2953aaea9406764fe8bb629a538"
```

Figure 2-4. Example of Security Credentials Saved in the Running-Config

Although you can enter an SNMPv3 authentication or privacy password in either clear ASCII text or the SHA-1 hash of the password, the password is displayed and saved in a configuration file only in hashed format, as shown in the preceding example.

For more information about the configuration of SNMP security parameters, refer to the chapter on "Configuring for Network Management Applications" in the *Management and Configuration Guide* for your switch.

802.1X Port-Access Credentials

802.1X authenticator (port-access) credentials can be stored in a configuration file. 802.1X *authenticator* credentials are used by a port to authenticate supplicants requesting a point-to-point connection to the switch. 802.1X *supplicant* credentials are used by the switch to establish a point-to-point connection to a port on another 802.1X-aware switch. Only 802.1X authenticator credentials are stored in a configuration file. For information about how to use 802.1X on the switch both as an authenticator and a supplicant, see "Configuring Port-Based and Client-Based Access Control (802.1X)" in this guide.

The local password configured with the **password** command is no longer accepted as an 802.1X authenticator credential. A new configuration command (**password port-access)** is introduced to configure the local operator username and password used as 802.1X authentication credentials for access to the switch.

The **password port-access** values are now configured separately from the manager and operator passwords configured with the **password manager** and **password operator** commands and used for management access to the switch. For information on the new **password** command syntax, see "Password Command Options" on page 2-13.

After you enter the complete **password port-access** command syntax, the password is set. You are not prompted to enter the password a second time.

TACACS+ Encryption Key Authentication

You can use TACACS+ servers to authenticate users who request access to a switch through Telnet (remote) or console (local) sessions. TACACS+ uses an authentication hierarchy consisting of:

- Remote passwords assigned in a TACACS+ server
- Local manager and operator passwords configured on the switch.

When you configure TACACS+, the switch first tries to contact a designated TACACS+ server for authentication services. If the switch fails to connect to any TACACS+ server, it defaults to its own locally assigned passwords for authentication control if it has been configured to do so.

For improved security, you can configure a global or server-specific encryption key that encrypts data in TACACS+ packets transmitted between a switch and a RADIUS server during authentication sessions. The key configured on the switch must match the encryption key configured in each

TACACS+ server application. (The encryption key is sometimes referred to as "shared secret" or "secret" key.) For more information, see "TACACS+ Authentication" on page 5-1 in this guide.

TACACS+ shared secret (encryption) keys can be saved in a configuration file by entering this command:

```
ProCurve(config)# tacacs-server key <keystring>
```

The option <*keystring*> is the encryption key (in clear text) used for secure communication with all or a specific TACACS+ server.

RADIUS Shared-Secret Key Authentication

You can use RADIUS servers as the primary authentication method for users who request access to a switch through Telnet, SSH, Web interface, console, or port-access (802.1X). The shared secret key is a text string used to encrypt data in RADIUS packets transmitted between a switch and a RADIUS server during authentication sessions. Both the switch and the server have a copy of the key; the key is never transmitted across the network. For more information, refer to "3. Configure the Switch To Access a RADIUS Server" on page 6-14 in this guide.

RADIUS shared secret (encryption) keys can be saved in a configuration file by entering this command:

```
ProCurve(config)# radius-server key <keystring>
```

The option <*keystring*> is the encryption key (in clear text) used for secure communication with all or a specific RADIUS server.

SSH Client Public-Key Authentication

Secure Shell version 2 (SSHv2) is used by ProCurve switches to provide remote access to SSH-enabled management stations. Although SSH provides Telnet-like functions, unlike Telnet, SSH provides encrypted, two-way authenticated transactions. SSH client public-key authentication is one of the types of authentication used.

Client public-key authentication uses one or more public keys (from clients) that must be stored on the switch. Only a client with a private key that matches a public key stored on the switch can gain access at the manager or operator level. For more information about how to configure and use SSH public keys to authenticate SSH clients that try to connect to the switch, refer to "Configuring Secure Shell (SSH)" on page 8-1 in this guide.

The SSH security credential that is stored in the running configuration file is configured with the **ip ssh public-key** command used to authenticate SSH clients for manager or operator access, along with the hashed content of each SSH client public-key.

Syntax: ip ssh public-key <manager |operator> keystring

Set a key for public-key authentication.

manager: *allows manager-level access using SSH public-key authentication.*

operator: *allows operator-level access using SSH public-key authentication.*

"keystring":. a legal SSHv2 (RSA or DSA) public key. The text string for the public key must be a single quoted token. If the keystring contains double-quotes, it can be quoted with single quotes ('`keystring`'). The following restrictions for a keystring apply:

- *A keystring cannot contain both single and double quotes.*
- *A keystring cannot have extra characters, such as a blank space or a new line. However, to improve readability, you can add a backlash at the end of each line.*

Note

The **ip ssh public-key** command allows you to configure only one SSH client public-key at a time. The **ip ssh public-key** command behavior includes an implicit append that never overwrites existing public-key configurations on a running switch.

If you download a software configuration file that contains SSH client public-key configurations, the downloaded public-keys overwrite any existing keys, as happens with any other configured values.

To display the SSH public-key configurations (72 characters per line) stored in a configuration file, enter the **show config** or **show running-config** command. The following example shows the SSH public keys configured for manager access, along with the hashed content of each SSH client public-key, that are stored in a configuration file:

```
...
include-credentials
ip ssh public-key manager "ssh-dss \
AAAAB3NzaC1kc3MAAACBAPwJHSJmTRtpZ9BUNC+ZrsxhMuZEXQhaDME1vc/ \
EvYnTKxQ31bWvr/bT7W58NX/YJ1ZKTV2GZ2QJCicUUZVWjNFJCsa0v03XS4 \
BhkXjtHhz6gD701otgizUOO6/Xzf4/J9XkJHkOCnbHIqtB1sbRYBTxj3NzA \
K1ymvIaU09X5TDAAAAFQCPwKxnbwFfTPasXnxfvDuLSxaC7wAAAIASBwxUP \
pv2scqPPXQghgaTkdPwGGtdFW/+K4xRskAnIaxuG0qLbnekohi+ND4TkKZd \
EeidgDh7qHusBhOFXM2g73RpE2rNqQnSf/QV95kdNwWIbxuusBAzvfaJptd \
gca6cYR4xS4TuBcaKiorYj60kk144E1fkDWieQx8zABQAAAIEAu7/1kVOdS \
G0vE0eJD23TLXvu94plXhRKCUAvyv2UyK+piG+Q1el1w9zsMaxPA1XJzSY/ \
imEp4p6WXEMcl0lpXMRnkhnuMMpaPMaQUT8NJTNu6hqf/LdQ2kqZjUuIyV9 \
LWyLg5ybS1kFLeOt0oo2Jbpy+U2e4jh2Bb77sX3G5C0= spock@sfc.gov" \
ip ssh public-key manager 'ssh-rsa \
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDyO9RDD52JZP8k2F2YZXubgwRAN0R \
JRs1Eov6y1RK3XkmgVatzl+mspiEmPS4wNK7bX/IoXNdGrGkoE8tPkxlZOZ \
oqGCf5Zs50P1nkxXvAidFs55AWqOf4MhfCqvtQCe1nt6LFh4ZMig+YewgQG \
M6H1geCSLUbXXSCipdPHysakw== "TectiaClientKey [1024-bit rsa, \
nobody@testmachine, Mon Aug 15 2005 14:47:34]"'
ip ssh public-key manager "ssh-rsa \
AAAAB3NzaC1yc2EAAABIwAAAIEA1Kk9sVQ9LJOR6XO/hCMPxbiMNOK8C/ay \
+SQ10qGw+K9m3w3TmCfjh0ud9hivgbFT4F99AgnQkvm2eVsgoTtLRnfF7uw \
NmpzqOqpHjD9YzItUgSK1uPuFwXMCHKUGKa+G46A+EWxDAIypwVIZ697QmM \
qPFj1zdI4sIo5bDett2d0= joe@hp.com"
...
```

Figure 2-5. Example of SSH Public Keys

If a switch configuration contains multiple SSH client public keys, each public key is saved as a separate entry in the configuration file. You can configure up to ten SSH client public-keys on a switch.

Operating Notes

Caution

- When you first enter the **include-credentials** command to save the additional security credentials to the running configuration, these settings are moved from internal storage on the switch to the running-config file.

  You are prompted by a warning message to perform a **write memory** operation to save the security credentials to the startup configuration. The message reminds you that if you do not save the current values of these security settings from the running configuration, they will be lost the next time you boot the switch and will revert to the values stored in the startup configuration.
- When you boot a switch with a startup configuration file that contains the **include-credentials** command, any security credentials that are stored in internal flash memory are ignored and erased. The switch will load only the security settings in the startup configuration file.
- Security settings are no longer automatically saved internally in flash memory and loaded with the startup configuration when a switch boots up. The configuration of all security credentials requires that you use the **write memory** command to save them in the startup configuration in order for them to not be lost when you log off. A warning message reminds you to permanently save a security setting.

- After you enter the **include-credentials** command, the currently configured manager and operator usernames and passwords, RADIUS shared secret keys, SNMP and 802.1X authenticator (port-access) security credentials, and SSH client public-keys are saved in the running configuration.

  Use the **no include-credentials** command to disable the display and copying of these security parameters from the running configuration (using the **show running-config** and **copy running-config** commands), without disabling the configured security settings on the switch.

  After you enter the **include-credentials** command, you can toggle between the non-display and display of security credentials in **show** and **copy** command output by alternately entering the **no include-credentials** and **include-credentials** commands.
- After you permanently save security configurations to the current startup-config file using the **write memory** command, you can view and manage security settings with the following commands:
  - **show config**: Displays the configuration settings in the current startup-config file.

- **copy config** <*source-filename*> **config** <*target-filename*>: Makes a local copy of an existing startup-config file by copying the contents of the startup-config file in one memory slot to a new startup-config file in another, empty memory slot.
- **copy config tftp**: Uploads a configuration file from the switch to a TFTP server.
- **copy tftp config**: Downloads a configuration file from a TFTP server to the switch.
- **copy config xmodem**: Uploads a configuration file from the switch to an Xmodem host.
- **copy xmodem config**: Downloads a configuration file from an Xmodem host to the switch.

For more information, see "Transferring Startup-Config Files To or From a Remote Server" in the *Management and Configuration Guide*.

- The switch can store up to three configuration files. Each configuration file contains its own security credentials and these security configurations may differ. It is the responsibility of the system administrator to ensure that the appropriate security credentials are contained in the configuration file that is loaded with each software image and that all security credentials in the file are supported.
- If you have already enabled the storage of security credentials (including local manager and operator passwords) by entering the **include-credentials** command, the **Reset-on-clear** option is disabled. When you press the Clear button on the front panel, the manager and operator usernames and passwords are deleted from the running configuration. However, the switch does not reboot after the local passwords are erased. (The **reset-on-clear** option normally reboots the switch when you press the Clear button.)

  For more information about the **Reset-on-clear** option and other front-panel security features, see "Configuring Front-Panel Security" on page 2-26 in this guide.

Restrictions

The following restrictions apply when you enable security credentials to be stored in the running configuration with the **include-credentials** command:

- The private keys of an SSH host cannot be stored in the running configuration. Only the public keys used to authenticate SSH clients can be stored. An SSH host's private key is only stored internally, for example, on the switch or on an SSH client device.
- SNMPv3 security credentials saved to a configuration file on a switch cannot be used after downloading the file on a different switch. The SNMPv3 security parameters in the file are only supported when loaded on the same switch for which they were configured. This is because when SNMPv3 security credentials are saved to a configuration file, they are saved with the engine ID of the switch as shown here:

  ```
  snmpv3 engine-id 00:00:00:0b:00:00:08:00:09:01:10:01
  ```

  If you download a configuration file with saved SNMPv3 security credentials on a switch, when the switch loads the file with the current software version the SNMPv3 engine ID value in the downloaded file must match the engine ID of the switch in order for the SNMPv3 users to be configured with the authentication and privacy passwords in the file. (To display the engine ID of a switch, enter the **show snmpv3 engine-id** command. To configure authentication and privacy passwords for SNMPv3 users, enter the **snmpv3 user** command.)

  If the engine ID in the saved SNMPv3 security settings in a downloaded configuration file does not match the engine ID of the switch:

  - The SNMPv3 users are configured, but without the authentication and privacy passwords. You must manually configure these passwords on the switch before the users can have SNMPv3 access with the privileges you want.
  - Only the **snmpv3 user** <*user_name*> credentials from the SNMPv3 settings in a downloaded configuration file are loaded on the switch, for example:

    ```
    snmpv3 user boris
    snmpv3 user alan
    ```

- You can store 802.1X authenticator (port-access) credentials in a configuration file. However, 802.1X supplicant credentials cannot be stored.
- The local operator password configured with the **password** command is no longer accepted as an 802.1X authenticator credential. A new configuration command (**password port-access)** is introduced to configure

the username and password used as 802.1X authentication credentials for access to the switch. You can store the **password port-access** values in the running configuration file by using the **include-credentials** command.

Note that the **password port-access** values are configured separately from local operator username and passwords configured with the **password operator** command and used for management access to the switch. For more information about how to use the **password port-access** command to configure operator passwords and usernames for 802.1X authentication, see “Do These Steps Before You Configure 802.1X Operation” on page 13-14 in this guide.

Front-Panel Security

The front-panel security features provide the ability to independently enable or disable some of the functions of the two buttons located on the front of the switch for clearing the password (Clear button) or restoring the switch to its factory default configuration (Reset+Clear buttons together). The ability to disable Password Recovery is also provided for situations which require a higher level of switch security.

The front-panel Security features are designed to prevent malicious users from:

- Resetting the password(s) by pressing the Clear button
- Restoring the factory default configuration by using the Reset+Clear button combination.
- Gaining management access to the switch by having physical access to the switch itself

When Security Is Important

Some customers require a high level of security for information. Also, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires that systems handling and transmitting confidential medical records must be secure.

It used to be assumed that only system and network administrators would be able to get access to a network switch because switches were typically placed in secure locations under lock and key. For some customers this is no longer true. Others simply want the added assurance that even if someone did manage to get to the switch that data would still remain secure.

If you do not invoke front-panel security on the switch, user-defined passwords can be deleted by pushing the Clear button on the front panel. This function exists so that if customers forget the defined passwords they can still get back into the switch and reset the passwords. This does, however, leave the switch vulnerable when it is located in an area where non-authorized people have access to it. Passwords could easily be cleared by pressing the Clear button. Someone who has physical access to the switch may be able to erase the passwords (and possibly configure new passwords) and take control of the switch.

As a result of increased security concerns, customers now have the ability to stop someone from removing passwords by disabling the Clear and/or Reset buttons on the front of the switch.

Front-Panel Button Functions

The System Support Module (SSM) of the switch includes the System Reset button and the Clear button. When using redundant management, the System Reset button reboots the entire chassis. (See "Resetting the Management Module" in the *Management and Configuration Guide* for more information on resetting the management modules in a redundant management switch.)

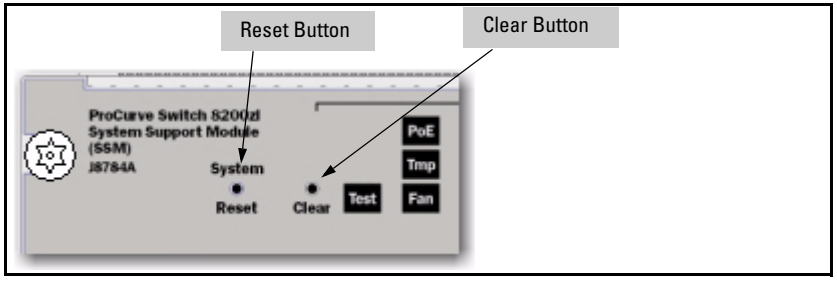


Figure 2-6. Front-Panel Button Locations on a ProCurve 8212zl Switch

Clear Button

Pressing the Clear button alone for one second resets the password(s) configured on the switch.

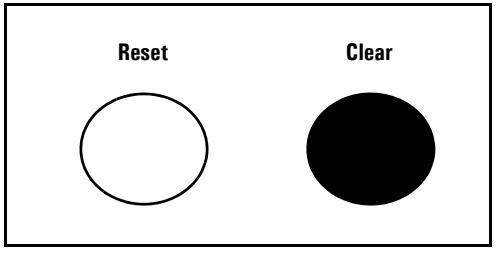


Figure 2-7. Press the Clear Button for One Second To Reset the Password(s)

Reset Button

Pressing the Reset button alone for one second causes the switch to reboot.

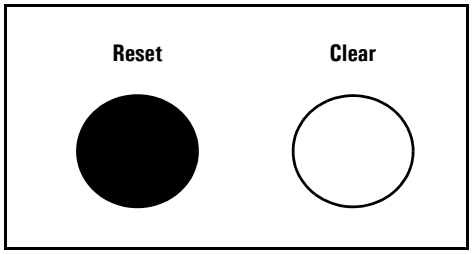
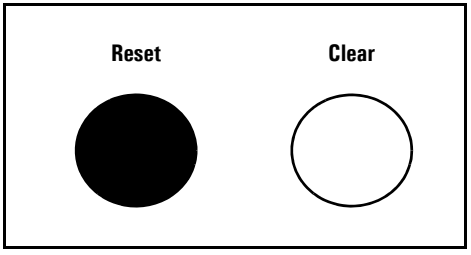


Figure 2-8. Press and hold the Reset Button for One Second To Reboot the Switch

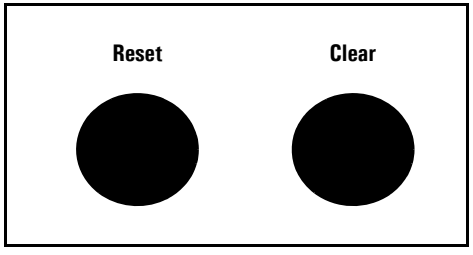
Restoring the Factory Default Configuration

You can also use the Reset button *together* with the Clear button (Reset+Clear) to **restore the factory default configuration** for the switch. To do this:

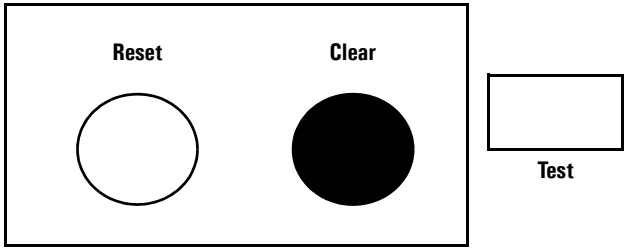
1. Press and hold the Reset button.



2. While holding the Reset button, press and hold the Clear button.

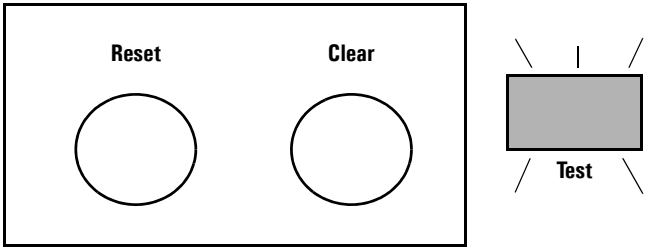


3. Release the Reset button.



4. When the Test LED to the right of the Clear button begins flashing, release the Clear button.

.



It can take approximately 20-25 seconds for the switch to reboot. This process restores the switch configuration to the factory default settings.

Configuring Front-Panel Security

Using the **front-panel-security** command from the global configuration context in the CLI you can:

- Disable or re-enable the password-clearing function of the Clear button. Disabling the Clear button means that pressing it does not remove local password protection from the switch. (This action affects the Clear button when used alone, but does not affect the operation of the Reset+Clear combination described under “Restoring the Factory Default Configuration” on page 2-25.)
- Configure the Clear button to reboot the switch after clearing any local usernames and passwords. This provides an immediate, visual means (plus an Event Log message) for verifying that any usernames and passwords in the switch have been cleared.

- Modify the operation of the Reset+Clear combination (page 2-25) so that the switch still reboots, but does *not* restore the switch's factory default configuration settings. (Use of the Reset button alone, to simply reboot the switch, is not affected.)
- Disable or re-enable Password Recovery.

Syntax: show front-panel-security

Displays the current front-panel-security settings:

Clear Password: *Shows the status of the Clear button on the front panel of the switch.* **Enabled** *means that pressing the Clear button erases the local usernames and passwords configured on the switch (and thus removes local password protection from the switch).* **Disabled** *means that pressing the Clear button does not remove the local usernames and passwords configured on the switch. (Default:* **Enabled***.)*

Reset-on-clear: *Shows the status of the reset-on-clear option (***Enabled** *or* **Disabled***). When reset-on-clear is disabled and Clear Password is enabled, then pressing the Clear button erases the local usernames and passwords from the switch. When reset-on-clear is enabled, pressing the Clear button erases the local usernames and passwords from the switch and reboots the switch. (Enabling* **reset-on-clear** *automatically enables* **clear-password***.) (Default:* **Disabled***.)*

Note: *If you have stored security credentials (including the local manager and operator usernames and passwords) to the running config file by entering the* **include-credentials** *command, the* **Reset-on-clear** *option is ignored. If you press the Clear button on the front panel, the manager and operator usernames and passwords are deleted from the startup configuration file, but the switch does not reboot. For more information about storing security credentials, see "Saving Security Credentials in a Config File" on page 2-10 in this guide.*

Factory Reset: *Shows the status of the System Reset button on the front panel of the switch. Enabled means that pressing the System Reset button reboots the switch and also enables the System Reset button to be used with the Clear button (page 2-25) to reset the switch to its factory-default configuration. (Default:* **Enabled***.)*

Password Recovery: *Shows whether the switch is configured with the ability to recover a lost password. (Refer to "Password Recovery Process" on page 2-34.) (Default:* **Enabled***.)*

> ***CAUTION:*** *Disabling this option removes the ability to recover a password on the switch. Disabling this option is an extreme measure and is not recommended unless you have the most urgent need for high security. If you disable password-recovery and then lose the password, you will have to use the Reset and Clear buttons (page 2-25) to reset the switch to its factory-default configuration and create a new password.*

For example, **show front-panel-security** produces the following output when the switch is configured with the default front-panel security settings.

```
ProCurve(config)# show front-panel-security
Clear Password          - Enabled
  Reset-on-clear        - Disabled
Factory Reset           - Enabled
Password Recovery       - Enabled
```

Figure 2-9. The Default Front-Panel Security Settings

Disabling the Clear Password Function of the Clear Button on the Switch's Front Panel

Syntax: no front-panel-security password-clear

In the factory-default configuration, pressing the Clear button on the switch's front panel erases any local usernames and passwords configured on the switch. This command disables the password clear function of the Clear button, so that pressing it has no effect on any local usernames and passwords.

For redundant management systems, this command only affects the active management module.

(Default: ***Enabled****.)*

Note: *Although the Clear button does not erase passwords when disabled, you can still use it with the Reset button (*Reset+Clear*) to restore the switch to its factory default configuration, as described under "Restoring the Factory Default Configuration" on page 2-25.*

This command displays a Caution message in the CLI. If you want to proceed with disabling the Clear button, type **[Y]**; otherwise type **[N]**. For example:

```
ProCurve(config)# no front-panel-security password-clear
                          **** CAUTION ****
Disabling the clear button prevents switch passwords from being easily reset or
recovered.  Ensure that you are familiar with the front panel security options
before proceeding.

Continue with disabling the clear button [y/n]? y

ProCurve(config)# show front-panel-security
Clear Password        - Disabled <----
Factory Reset         - Enabled
Password Recovery     - Enabled
```

Indicates the command has disabled the Clear button on the switch's front panel. In this case the Show command does not include the **reset-on-clear** status because it is inoperable while the Clear Password functionality is disabled, and must be reconfigured whenever Clear Password is re-enabled .

Figure 2-10. Example of Disabling the Clear Button and Displaying the New Configuration

Re-Enabling the Clear Button on the Switch's Front Panel and Setting or Changing the "Reset-On-Clear" Operation

Syntax: [no] front-panel-security password-clear reset-on-clear

This command does both of the following:

- *Re-enables the password-clearing function of the Clear button on the switch's front panel.*
- *Specifies whether the switch reboots if the Clear button is pressed.*

To re-enable password-clear, you must also specify whether to enable or disable the **reset-on-clear** *option.*
Defaults:

- password-clear: ***Enabled***.
- reset-on-clear: ***Disabled***.

Thus:

- *To enable password-clear with reset-on-clear disabled, use this syntax:*

  no front-panel-security password-clear reset-on-clear

- *To enable password-clear with reset-on-clear also enabled, use this syntax:*

  front-panel-security password-clear reset-on-clear

(Either form of the command enables password-clear.)
For redundant management systems, this command only affects the active management module.

Note: *If you disable* **password-clear** *and also disable the* **password-recovery** *option, you can still recover from a lost password by using the Reset+Clear button combination at reboot as described on page 2-25. Although the Clear button does not erase passwords when disabled, you can still use it with the Reset button (*Reset+Clear*) to restore the switch to its factory default configuration. You can then get access to the switch to set a new password.*

For example, suppose that **password-clear** is disabled and you want to restore it to its default configuration (enabled, with **reset-on-clear** disabled).

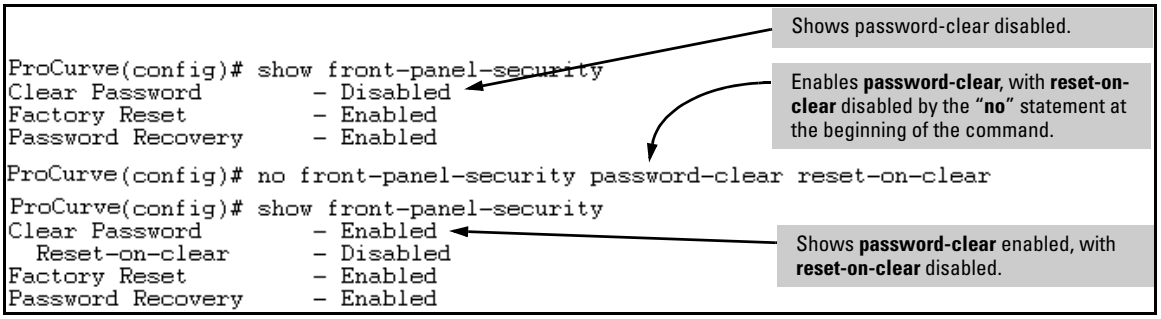


Figure 2-11. Example of Re-Enabling the Clear Button's Default Operation

Changing the Operation of the Reset+Clear Combination

In their default configuration, using the Reset+Clear buttons in the combination described under "Restoring the Factory Default Configuration" on page 2-25 replaces the switch's current startup-config file with the factory-default startup-config file, then reboots the switch, and removes local password protection. *This means that anyone who has physical access to the switch could use this button combination to replace the switch's current configuration with the factory-default configuration, and render the switch accessible without the need to input a username or password.* You can use the **factory-reset** command to prevent the Reset+Clear combination from being used for this purpose.

Syntax: [no] front-panel-security factory-reset

Disables or re-enables the following functions associated with using the Reset+Clear buttons in the combination described under "Restoring the Factory Default Configuration" on page 2-25:

- *Replacing the current startup-config file with the factory-default startup-config file*
- *Clearing any local usernames and passwords configured on the switch*

*(**Default:** Both functions enabled.)*

For redundant management systems, this command only affects the active management module.

Notes: *The Reset+Clear button combination always reboots the switch, regardless of whether the "***no***" form of the command has been used to disable the above two functions. Also, if you disable* **factory-reset**, *you cannot disable the* **password-recovery** *option, and the reverse.*

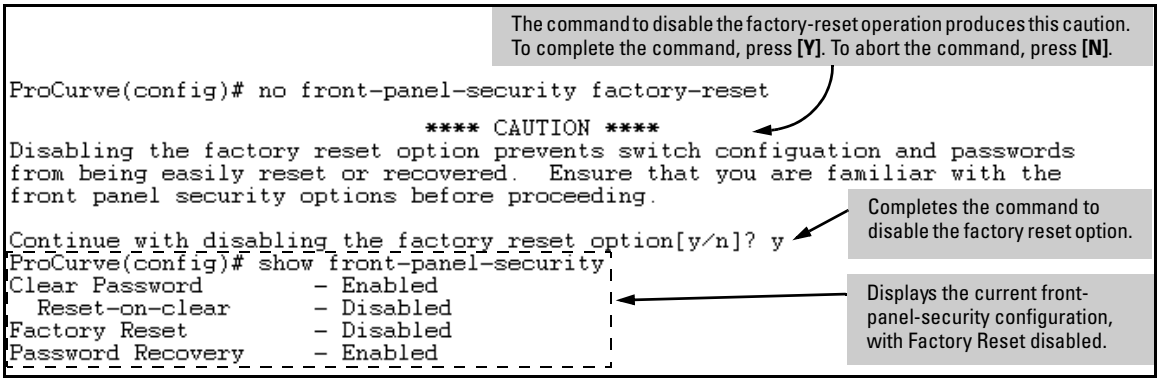


Figure 2-12. Example of Disabling the Factory Reset Option

Password Recovery

The password recovery feature is enabled by default and provides a method for regaining management access to the switch (without resetting the switch to its factory default configuration) in the event that the system administrator loses the local manager username (if configured) or password. Using Password Recovery requires:

- **password-recovery** enabled (the default) on the switch prior to an attempt to recover from a lost username/password situation
- Contacting your ProCurve Customer Care Center to acquire a one-time-use password

Disabling or Re-Enabling the Password Recovery Process

Disabling the password recovery process means that the only method for recovering from a lost manager username (if configured) and password is to reset the switch to its factory-default configuration, which removes any non-default configuration settings.

Caution

Disabling **password-recovery** requires that **factory-reset** be enabled, and locks out the ability to recover a lost manager username (if configured) and password on the switch. In this event, there is no way to recover from a lost manager username/password situation without resetting the switch to its factory-default configuration. This can disrupt network operation and make it necessary to temporarily disconnect the switch from the network to prevent unauthorized access and other problems while it is being reconfigured. Also, with **factory-reset** enabled, unauthorized users can use the Reset+Clear button combination to reset the switch to factory-default configuration and gain management access to the switch.

Syntax: [no] front-panel-security password-recovery

*Enables or (using the "***no***" form of the command) disables the ability to recover a lost password.*

When this feature is enabled, the switch allows management access through the password recovery process described below. This provides a method for recovering from a lost manager username (if configured) and password. When this feature is disabled, the password recovery process is disabled and the only way to regain management access to the switch is to use the Reset+Clear button combination (page 2-25) to restore the switch to its factory default configuration.

Note: *To disable* **password-recovery:**

- *You must have physical access to the front panel of the switch.*
- *The* **factory-reset** *parameter must be enabled (the default).*

For redundant management systems, this command only affects the active management module.

(Default: Enabled.)

Steps for Disabling Password-Recovery.

1. Set the CLI to the global interface context.
2. Use **show front-panel-security** to determine whether the factory-reset parameter is enabled. If it is disabled, use the **front-panel-security factory-reset** command to enable it.
3. Press and release the Clear button on the front panel of the switch.
4. Within 60-seconds of pressing the Clear button, enter the following command:

   no front-panel-security password-recovery

5. Do one of the following after the "**CAUTION**" message appears:
   - If you want to complete the command, press **[Y]** (for "Yes").
   - If you want to abort the command, press **[N]** (for "No")

Figure 2-13 shows an example of disabling the **password-recovery** parameter.

```
ProCurve(config)# no front-panel-security password-recovery
                              **** CAUTION ****
Disabling the clear button without password recovery prevents switch passwords
from being reset.  If the switch password is lost, restoring the default factory
configuration will be required to regain access!

Continue with disabling password recovery [y/n]? y

ProCurve(config)# _
```

Figure 2-13. Example of the Steps for Disabling Password-Recovery

Password Recovery Process

If you have lost the switch's manager username/password, but **password-recovery** is enabled, then you can use the Password Recovery Process to gain management access to the switch with an alternate password supplied by ProCurve.

Note

If you have disabled **password-recovery**, which locks out the ability to recover a manager username/password pair on the switch, then the only way to recover from a lost manager username/password pair is to use the Reset+Clear button combination described under "Restoring the Factory Default Configuration" on page 2-25. This can disrupt network operation and make it necessary to temporarily disconnect the switch from the network to prevent unauthorized access and other problems while it is being reconfigured.

To use the **password-recovery** option to recover a lost password:

1. Note the switch's base MAC address. It is shown on the label located on the upper right front corner of the switch.
2. Contact your ProCurve Customer Care Center for further assistance. Using the switch's MAC address, the ProCurve Customer Care Center will generate and provide a "one-time use" alternate password you can use with the to gain management access to the switch. Once you gain access, you can configure a new, known password.

Note

The alternate password provided by the ProCurve Customer Care Center is valid only for a single login attempt. You cannot use the *same "one-time-use" password* if you lose the password a second time. Because the password algorithm is randomized based upon your switch's MAC address, the password will change as soon as you use the *"one-time-use" password* provided to you by the ProCurve Customer Care Center.