

# Security Overview

---

## Contents

<b>Introduction</b> .....	1-2
About This Guide .....	1-2
For More Information .....	1-2
<b>Access Security Features</b> .....	1-3
<b>Network Security Features</b> .....	1-7
<b>Getting Started with Access Security</b> .....	1-10
Physical Security .....	1-10
Quick Start: Using the Management Interface Wizard .....	1-11
CLI: Management Interface Wizard .....	1-12
Web: Management Interface Wizard .....	1-13
SNMP Security Guidelines .....	1-16
<b>Precedence of Security Options</b> .....	1-18
Precedence of Port-Based Security Options .....	1-18
Precedence of Client-Based Authentication:	
Dynamic Configuration Arbiter .....	1-18
Network Immunity Manager .....	1-19
Arbitrating Client-Specific Attributes .....	1-20
<b>ProCurve Identity-Driven Manager (IDM)</b> .....	1-22

## Introduction

This chapter provides an overview of the security features included on your switch. Table 1-1 on page 1-3 outlines the access security and authentication features, while Table 1-2 on page 1-7 highlights the additional features designed to help secure and protect your network. For detailed information on individual features, see the references provided.

Before you connect your switch to a network, ProCurve strongly recommends that you review the section titled “Getting Started with Access Security” on page 1-10. It outlines potential threats for unauthorized switch and network access, and provides guidelines on how to prepare the switch for secure network operation.

## About This Guide

This *Access Security Guide* describes how to configure security features on your switch.

---

### Note

For an introduction to the standard conventions used in this guide, refer to the *Getting Started* chapter in the *Management and Configuration Guide* for your switch.

---

## For More Information

For IPv6-specific security settings and features, refer to the *IPv6 Configuration Guide* for your switch.

For information on which product manual to consult for a specific software feature, refer to the “Software Feature Index” on page vi of this guide.

For the latest version of all HP ProCurve switch documentation, including Release Notes covering recently added features and other software topics, visit the HP ProCurve Networking web site at [www.procurve.com/manuals](http://www.procurve.com/manuals).

## Access Security Features

This section provides an overview of the switch's access security features, authentication protocols, and methods. Table 1-1 lists these features and provides summary configuration guidelines. For more in-depth information, see the references provided (all chapter and page references are to this *Access Security Guide* unless a different manual name is indicated).

---

### Note

Beginning with software release K.14.1xx, the Management Interface wizard provides a convenient step-by-step method to prepare the switch for secure network operation. See “Quick Start: Using the Management Interface Wizard” on page 1-11 for details.

---

**Table 1-1. Access Security and Switch Authentication Features**

Feature	Default Setting	Security Guidelines	More Information and Configuration Details
<b>Manager password</b>	no password	Configuring a local Manager password is a fundamental step in reducing the possibility of unauthorized access through the switch's Web browser and console (CLI and Menu) interfaces. The Manager password can easily be set by any one of the following methods: <ul style="list-style-type: none"> <li>• CLI: password manager command, or Management interface wizard</li> <li>• Web browser interface: the password options under the Security tab, or Management interface wizard</li> <li>• Menu interface: Console Passwords option</li> <li>• SNMP</li> </ul>	<i>“Configuring Local Password Security” on page 2-6</i> <i>“Quick Start: Using the Management Interface Wizard” on page 1-11</i> <i>“Using SNMP To View and Configure Switch Authentication Features” on page 6-21</i>

---

Feature	Default Setting	Security Guidelines	More Information and Configuration Details
<b>Telnet and Web-browser access</b>	enabled	<p>The default remote management protocols enabled on the switch are plain text protocols, which transfer passwords in open or plain text that is easily captured. To reduce the chances of unauthorized users capturing your passwords, secure and encrypted protocols such as SSH and SSL (see below for details) should be used for remote access. This enables you to employ increased access security while still retaining remote client access.</p> <p>Also, access security on the switch is incomplete without disabling Telnet and the standard Web browser access. Among the methods for blocking unauthorized access attempts using Telnet or the Web browser are the following two CLI commands:</p> <ul style="list-style-type: none"> <li>• <b>no telnet-server:</b> This command blocks inbound Telnet access.</li> <li>• <b>no web-management:</b> This command prevents use of the Web browser interface through http (port 80) server access.</li> </ul> <p>If you choose not to disable Telnet and Web browser access, you may want to consider using RADIUS accounting to maintain a record of password-protected access to the switch.</p>	<p><i>“Quick Start: Using the Management Interface Wizard” on page 1-11</i></p> <p>For more on Telnet and web browser access, refer to the chapter on <i>“Interface Access and System Information”</i> in the <i>Management and Configuration Guide</i>.</p> <p>For RADIUS accounting, refer to <i>Chapter 6, “RADIUS Authentication and Accounting”</i></p>
<b>SSH</b>	disabled	<p>SSH provides Telnet-like functions through encrypted, authenticated transactions of the following types:</p> <ul style="list-style-type: none"> <li>• 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 stored public key can gain access to the switch.</li> <li>• switch SSH and user password authentication: this option is a subset of the client public-key authentication, and is used if the switch has SSH enabled without a login access configured to authenticate the client’s key. In this case, the switch authenticates itself to clients, and users on SSH clients then authenticate themselves to the switch by providing passwords stored on a RADIUS or TACACS+ server, or locally on the switch.</li> <li>• secure copy (SC) and secure FTP (SFTP): By opening a secure, encrypted SSH session, you can take advantage of SC and SFTP to provide a secure alternative to TFTP for transferring sensitive switch information. For more on SC and SFTP, refer to the section titled <i>“Using Secure Copy and SFTP”</i> in the <i>“File Transfers”</i> appendix of the <i>Management and Configuration Guide</i> for your switch.</li> </ul>	<p><i>“Quick Start: Using the Management Interface Wizard” on page 1-11</i></p> <p><i>Chapter 8 “Configuring Secure Shell (SSH)”</i></p>

Feature	Default Setting	Security Guidelines	More Information and Configuration Details
<b>SSL</b>	disabled	Secure Socket Layer (SSL) and Transport Layer Security (TLS) provide remote Web browser access to the switch via authenticated transactions and encrypted paths between the switch and management station clients capable of SSL/TLS operation. The authenticated type includes server certificate authentication with user password authentication.	<i>“Quick Start: Using the Management Interface Wizard” on page 1-11</i> <i>Chapter 9, “Configuring Secure Socket Layer (SSL)”</i>
<b>SNMP</b>	public, unrestricted	In the default configuration, the switch is open to access by management stations running SNMP management applications capable of viewing and changing the settings and status data in the switch’s MIB (Management Information Base). Thus, controlling SNMP access to the switch and preventing unauthorized SNMP access should be a key element of your network security strategy.	<i>“SNMP Security Guidelines” on page 1-16</i> <i>“Quick Start: Using the Management Interface Wizard” on page 1-11</i> <i>Management and Configuration Guide, Chapter 14, refer to the section “Using SNMP Tools To Manage the Switch”</i>
<b>Authorized IP Managers</b>	none	This feature uses IP addresses and masks to determine whether to allow management access to the switch across the network through the following : <ul style="list-style-type: none"> <li>• Telnet and other terminal emulation applications</li> <li>• The switch’s Web browser interface</li> <li>• SNMP (with a correct community name)</li> </ul>	<i>Chapter 15, “Using Authorized IP Managers”</i>
<b>Secure Management VLAN</b>	disabled	This feature creates an isolated network for managing the ProCurve switches that offer this feature. When a secure management VLAN is enabled, CLI, Menu interface, and Web browser interface access is restricted to ports configured as members of the VLAN.	<i>Advanced Traffic Management Guide, refer to the chapter “Static Virtual LANs (VLANs)”</i>
<b>ACLs for Management Access Protection</b>	none	ACLs can also be configured to protect management access by blocking inbound IP traffic that has the switch itself as the destination IP address.	<i>“Access Control Lists (ACLs)” on page 1-8</i> <i>Chapter 10, “IPv4 Access Control Lists (ACLs)”</i>
<b>TACACS+ Authentication</b>	disabled	This application uses a central server to allow or deny access to TACACS+ aware devices in your network. TACACS+ uses username/password sets with associated privilege levels to grant or deny access through either the switch’s serial (console) port or remotely, with Telnet.  If the switch fails to connect to a TACACS+ server for the necessary authentication service, it defaults to its own locally configured passwords for authentication control. TACACS+ allows both login (read-only) and enable (read/write) privilege level access.	<i>Chapter 5, “TACACS+ Authentication”</i>

**Security Overview**  
Access Security Features

<b>Feature</b>	<b>Default Setting</b>	<b>Security Guidelines</b>	<b>More Information and Configuration Details</b>
<b>RADIUS Authentication</b>	disabled	For each authorized client, RADIUS can be used to authenticate operator or manager access privileges on the switch via the serial port (CLI and Menu interface), Telnet, SSH, and Secure FTP/Secure Copy (SFTP/SCP) access methods.	<i>Chapter 6, "RADIUS Authentication and Accounting"</i>
<b>802.1X Access Control</b>	none	<p>This feature provides port-based or user-based authentication through a RADIUS server to protect the switch from unauthorized access and to enable the use of RADIUS-based user profiles to control client access to network services. Included in the general features are the following:</p> <ul style="list-style-type: none"><li>• user-based access control supporting up to 32 authenticated clients per port</li><li>• port-based access control allowing authentication by a single client to open the port</li><li>• switch operation as a supplicant for point-to-point connections to other 802.1X-compliant ProCurve switches</li></ul>	<i>Chapter 13 "Configuring Port-Based and User-Based Access Control (802.1X)"</i>
<b>Web and MAC Authentication</b>	none	<p>These options are designed for application on the edge of a network to provide port-based security measures for protecting private networks and the switch itself from unauthorized access. Because neither method requires clients to run any special supplicant software, both are suitable for legacy systems and temporary access situations where introducing supplicant software is not an attractive option.</p> <p>Both methods rely on using a RADIUS server for authentication. This simplifies access security management by allowing you to control access from a master database in a single server. It also means the same credentials can be used for authentication, regardless of which switch or switch port is the current access point into the LAN. Web authentication uses a web page login to authenticate users for access to the network. MAC authentication grants access to a secure network by authenticating device MAC addresses for access to the network.</p>	<i>Chapter 4, "Web and MAC Authentication"</i>

# Network Security Features

This section outlines features and defence mechanisms for protecting access through the switch to the network. For more detailed information, see the indicated chapters.

**Table 1-2. Network Security—Default Settings and Security Guidelines**

Feature	Default Setting	Security Guidelines	More Information and Configuration Details
<b>Secure File Transfers</b>	not applicable	Secure Copy and SFTP provide a secure alternative to TFTP and auto-TFTP for transferring sensitive information such as configuration files and log information between the switch and other devices.	<i>Management and Configuration Guide, Appendix A “File Transfers”, refer to the section “Using Secure Copy and SFTP”</i>
<b>USB Autorun</b>	enabled (disabled once a password has been set)	Used in conjunction with ProCurve Manager Plus, this feature allows diagnosis and automated updates to the switch via the USB flash drive. When enabled in secure mode, this is done with secure credentials to prevent tampering. Note that the USB Autorun feature is disabled automatically, once a password has been set on the switch.	<i>Management and Configuration Guide, Appendix A “File Transfers”, refer to the section “USB Autorun”</i>
<b>Traffic/Security Filters</b>	none	These statically configured filters enhance in-band security (and improve control over access to network resources) by forwarding or dropping inbound network traffic according to the configured criteria. Filter options include: <ul style="list-style-type: none"> <li>• <b>source-port filters:</b> Inbound traffic from a designated, physical source-port will be forwarded or dropped on a per-port (destination) basis.</li> <li>• <b>multicast filters:</b> Inbound traffic having a specified multicast MAC address will be forwarded to outbound ports or dropped on a per-port (destination) basis.</li> <li>• <b>protocol filters:</b> Inbound traffic having the selected frame (protocol) type will be forwarded or dropped on a per-port (destination) basis.</li> </ul>	<i>Chapter 12, “Traffic/Security Filters and Monitors”</i>

Feature	Default Setting	Security Guidelines	More Information and Configuration Details
<b>Access Control Lists (ACLs)</b>	none	<p>ACLs can filter traffic to or from a host, a group of hosts, or entire subnets. Layer 3 IP filtering with Access Control Lists (ACLs) enables you to improve network performance and restrict network use by creating policies for:</p> <ul style="list-style-type: none"> <li>• <b>Switch Management Access:</b> Permits or denies in-band management access. This includes preventing the use of certain TCP or UDP applications (such as Telnet, SSH, Web browser, and SNMP) for transactions between specific source and destination IP addresses.)</li> <li>• <b>Application Access Security:</b> Eliminating unwanted IP, TCP, or UDP traffic by filtering packets where they enter or leave the switch on specific interfaces.</li> </ul> <p>Note on ACL Security Use:</p> <p>ACLs can enhance network security by blocking selected IP traffic, and can serve as one aspect of maintaining network security. However, because ACLs do not provide user or device authentication, or protection from malicious manipulation of data carried in IP packet transmissions, they should not be relied upon for a complete security solution.</p>	<i>Chapter 10, "IPv4 Access Control Lists (ACLs)"</i>
<b>Port Security, MAC Lockdown, and MAC Lockout</b>	none	<p>The features listed below provide device-based access security in the following ways:</p> <ul style="list-style-type: none"> <li>• <b>Port security:</b> Enables configuration of each switch port with a unique list of the MAC addresses of devices that are authorized to access the network through that port. This enables individual ports to detect, prevent, and log attempts by unauthorized devices to communicate through the switch. Some switch models also include eavesdrop prevention in the port security feature.</li> <li>• <b>MAC lockdown:</b> This "static addressing" feature is used as an alternative to port security to prevent station movement and MAC address "hijacking" by allowing a given MAC address to use only one assigned port on the switch. MAC lockdown also restricts the client device to a specific VLAN.</li> <li>• <b>MAC lockout:</b> This feature enables blocking of a specific MAC address so that the switch drops all traffic to or from the specified address.</li> </ul>	<p><i>Chapter 14, "Configuring and Monitoring Port Security"</i></p> <p>See also "Precedence of Port-Based Security Options" on page 1-18</p>

Feature	Default Setting	Security Guidelines	More Information and Configuration Details
<b>Key Management System (KMS)</b>	none	KMS is available in several ProCurve switch models and is designed to configure and maintain key chains for use with KMS-capable routing protocols that use time-dependent or time-independent keys. (A key chain is a set of keys with a timing mechanism for activating and deactivating individual keys.) KMS provides specific instances of routing protocols with one or more Send or Accept keys that must be active at the time of a request.	<i>Chapter 16, "Key Management System"</i>
<b>Connection-Rate Filtering based on Virus-Throttling Technology</b>	none	This feature helps protect the network from attack and is recommended for use on the network edge. It is primarily focused on the class of worm-like malicious code that tries to replicate itself by taking advantage of weaknesses in network applications behind unsecured ports. In this case, the malicious code tries to create a large number of outbound connections on an interface in a short time. Connection-Rate filtering detects hosts that are generating traffic that exhibits this behavior, and causes the switch to generate warning messages and (optionally) to throttle or drop all traffic from the offending hosts.	<i>Chapter 3, "Virus Throttling (Connection-Rate Filtering)"</i>
<b>ICMP Rate-Limiting</b>	none	This feature helps defeat ICMP denial-of-service attacks by restricting ICMP traffic to percentage levels that permit necessary ICMP functions, but throttle additional traffic that may be due to worms or viruses (reducing their spread and effect).	<i>Management and Configuration Guide, in the chapter on "Port Traffic Controls" refer to the section "ICMP Rate-Limiting"</i>
<b>Spanning Tree Protection</b>	none	These features prevent your switch from malicious attacks or configuration errors: <ul style="list-style-type: none"> <li>• <b>BPDU Filtering and BPDU Protection:</b> Protects the network from denial-of-service attacks that use spoofing BPDUs by dropping incoming BPDU frames and/or blocking traffic through a port.</li> <li>• <b>STP Root Guard:</b> Protects the STP root bridge from malicious attacks or configuration mistakes.</li> </ul>	<i>Advanced Traffic Management Guide, refer to the chapter "Multiple Instance Spanning-Tree Operation"</i>
<b>DHCP Snooping, Dynamic ARP Protection, and Dynamic IP Lockdown</b>	none	These features provide the following additional protections for your network: <ul style="list-style-type: none"> <li>• <b>DHCP Snooping:</b> Protects your network from common DHCP attacks, such as address spoofing and repeated address requests.</li> <li>• <b>Dynamic ARP Protection:</b> Protects your network from ARP cache poisoning.</li> <li>• <b>Dynamic IP Lockdown:</b> Prevents IP source address spoofing on a per-port and per-VLAN basis</li> <li>• <b>Instrumentation Monitor.</b> Helps identify a variety of malicious attacks by generating alerts for detected anomalies on the switch.</li> </ul>	<i>Chapter 11, "Configuring Advanced Threat Protection"</i>

## Getting Started with Access Security

ProCurve switches are designed as “plug and play” devices, allowing quick and easy installation in your network. In its default configuration the switch is open to unauthorized access of various types. When preparing the switch for network operation, therefore, ProCurve strongly recommends that you enforce a security policy to help ensure that the ease in getting started is not used by unauthorized persons as an opportunity for access and possible malicious actions.

Since security incidents can originate with sources inside as well as outside of an organization, your access security provisions must protect against internal and external threats while preserving the necessary network access for authorized clients and users. It is important to evaluate the level of management access vulnerability existing in your network and take steps to ensure that all reasonable security precautions are in place. This includes both configurable security options and physical access to the switch.

Switch management access is available through the following methods:

- Front panel access to the console serial port (see “Physical Security”)
- Inbound Telnet access
- Web-browser access
- SNMP access

For guidelines on locking down your switch for remote management access, see “Quick Start: Using the Management Interface Wizard” on page 1-11.

### Physical Security

Physical access to the switch allows the following:

- use of the console serial port (CLI and Menu interface) for viewing and changing the current configuration and for reading status, statistics, and log messages.
- use of the switch’s USB port for file transfers and autorun capabilities.
- use of the switch’s Clear and Reset buttons for these actions:
  - clearing (removing) local password protection
  - rebooting the switch
  - restoring the switch to the factory default configuration (and erasing any non-default configuration settings)

Keeping the switch in a locked wiring closet or other secure space helps to prevent unauthorized physical access.

As additional precautions, you can do the following:

- Disable or re-enable the password-clearing function of the Clear button.
- Configure the Clear button to reboot the switch after clearing any local usernames and passwords.
- Modify the operation of the Reset+Clear button combination so that the switch reboots, but does not restore the switch's factory default settings.
- Disable or re-enable password recovery.
- Disable USB autorun by setting a Manager password, or enable USB autorun in secure mode so that security credentials are required to use this feature.

For the commands used to configure the Clear and Reset buttons, refer to “Front-Panel Security” on page 2-23. For information on using USB Autorun, refer to the sections on “Using USB to Transfer Files to and from the Switch” and “Using USB Autorun” in the *Management and Configuration Guide, Appendix A “File Transfers”*.

## Quick Start: Using the Management Interface Wizard

The Management Interface wizard provides a convenient step-by-step method to prepare the switch for secure network operation. It guides you through the process of locking down the following switch operations or protocols:

- setting local passwords
- restricting SNMP access
- enabling/disabling Telnet
- enabling/disabling SSH
- enabling/disabling remote Web management
- restricting web access to SSL
- enabling/disabling USB autorun
- setting timeouts for SSH/Telnet sessions

The wizard can also be used to view the pre-configured defaults and see the current settings for switch access security. The wizard can be launched either via the CLI (see page 1-12) or the Web browser interface (see page 1-13).

---

**Note**

The wizard's security settings can also be configured using standard commands via the CLI, Menu or Web browser interfaces. For full details on preparing and configuring the switch for SSH and SSL operation, refer to chapters 8 and 9 respectively.

---

## CLI: Management Interface Wizard

To configure security settings using the CLI wizard, follow the steps below:

1. At the command prompt, type **setup mgmt-interfaces**.

The welcome banner appears and the first setup option is displayed (**Operator password**). As you advance through the wizard, each setup option displays the current value in brackets [ ] as shown in Figure 1-1.

The screenshot shows the Management Interface Setup Wizard. It starts with a welcome message and instructions. The main configuration screen lists various options with their current values in brackets. A summary screen follows, enclosed in a dashed box, showing the current settings. The wizard ends with a question about saving changes.

```

Welcome to the Management Interface Setup Wizard

This wizard will help you with the initial setup of the various
management interfaces. The current values are shown in brackets[ ].
Type in a new value, or press <Enter> to keep the current value.
Press CTRL-C at any time to quit the wizard without saving any
changes. Press ? for help.

Operator password [not configured]:
Confirm password:
Manager password [*****]:
Confirm password:
Restrict SNMP access to SNMPv3 only [no]:
SNMPv2 community name [notpublic]:
SNMPv2 Community access level [unrestricted]:
Telnet enabled [yes]:
SSH enabled [no]:
Web management enabled [yes]:
Restrict Web access to SSL [no]:
Timeout for ssh/telnet sessions [0]:

Operator password :
Manager password :*****
Restrict SNMP access to SNMPv3 only :no
SNMPv2 community name :notpublic
SNMPv2 Community access level :unrestricted
Telnet enabled :yes
SSH enabled :no
Web management enabled :yes
Restrict Web access to SSL :no
Timeout for ssh/telnet sessions :0

Do you want to save these changes? [yes]:

```

**Annotations:**

- Current values are shown in brackets (Password entries must be entered twice and will appear as asterisks.)**: Points to the password fields.
- Type in a new value to change a setting, or press <Enter> to keep the current value.**: Points to the right side of the configuration screen.
- Summary of current settings (displayed after last wizard option has been set)**: Points to the dashed box containing the summary.
- To save these settings, press [Enter]. To cancel any changes, type [n] (for no), then press [Enter].**: Points to the final question.

Figure 1-1. Example of Management Interface Wizard Configuration

2. When you enter the wizard, you have the following options:
  - To update a setting, type in a new value, or press **[Enter]** to keep the current value.
  - To quit the wizard without saving any changes, press **[CTRL-C]** at any time.
  - To access online Help for any option, press **[?]**.

After you have gone through each setup option, the wizard displays the summary configuration together with a prompt to save the changes (see Figure 1-1 on page 1-12 for an example).

3. When the message appears asking if you want to save these changes, you have the following options:
  - To save your changes, press **[Enter]**.
  - To cancel any changes without saving, type **[n]** and then press **[Enter]**.

After pressing **[Enter]**, the wizard exits to the command line prompt.

#### **CLI Wizard: Operating Notes and Restrictions.**

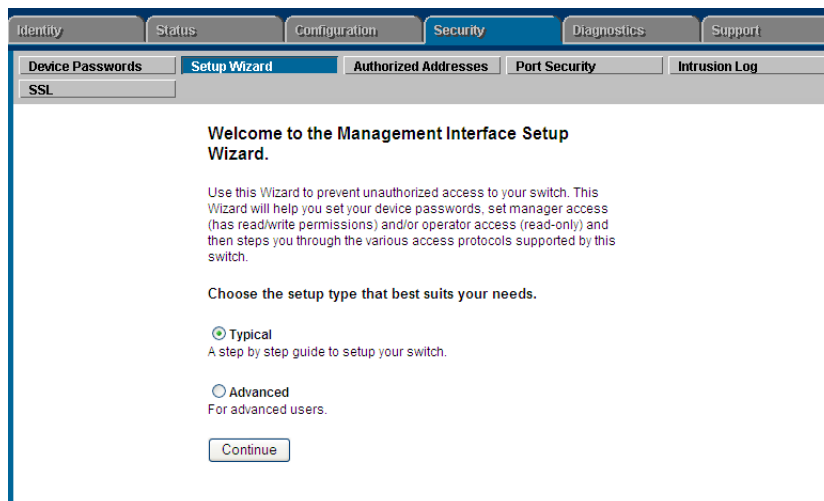
- Once a password has been configured on the switch, you cannot remove it using the CLI wizard. Passwords can be removed by executing the **no password** command directly from the CLI.
- When you restrict SNMP access to SNMPv3 only, the options SNMPv2 community name and access level will not appear.
- The wizard displays the first available SNMPv2 community and allows the user to modify the first community access parameters.
- The wizard creates a new SNMP community only when no communities have been configured on the switch.
- The USB Autorun feature is disabled as soon as an operator or manager password is set on the switch. Once a password has been set, the USB autorun option is no longer provided as part of the wizard.

#### **Web: Management Interface Wizard**

To use the Management Interface wizard from the Web browser interface, follow the steps below:

1. Click the **Security** tab.
2. Click the **Setup Wizard** button.

The Welcome window appears.



**Figure 1-2. Management Interface Wizard: Welcome Window**

This page allows you to choose between two setup types:

- **Typical**—provides a multiple page, step-by-step method to configure security settings, with on-screen instructions for each option.
  - **Advanced**—provides a single summary screen in which to configure all security settings at once.
3. To enter the wizard, choose a setup option and then click **Continue**.
- **Typical** (multi-page setup): when you select this option, you will get an alert indicating that configuration changes will be lost if you click on the Web browser's navigation tabs. Click **OK** to close the alert and then advance through the following setup pages: **Operator Password, Manager Password, SNMP, Telnet, SSH, Web Management GUI, USB Autorun, Timeout** (see pages for details and setup options).

At each page, you have the following options:

- Enter a new value and/or make a new selection, or click **Continue** to keep the current value and proceed to the next page setup. When you have gone through all configurable options, the summary setup page appears (see step 4).
  - To quit the Setup and return to the Welcome window without saving any changes, click **Exit** at any time.
  - To return to the previous screen(s), click **Back** at any time.
- **Advanced** (single page setup): when you select this option, the summary setup page appears immediately (see step 4).

- The summary setup screen displays the current configuration settings for all setup options (see Figure 1-3).

The screenshot shows the 'Management Interface Setup' screen within a 'Setup Wizard' window. The window has tabs for 'Device Passwords', 'Setup Wizard', 'Authorized Addresses', 'Port Security', and 'Intrusion Log'. The 'Setup Wizard' tab is active, and the 'SSL' sub-tab is selected. The main content area is titled 'Management Interface Setup.' and contains three sections: 'Passwords:', 'SNMP Access:', and 'Other Access:'. The 'Passwords:' section has four input fields: 'Operator password:', 'Confirm Password:', 'Manager password:', and 'Confirm Password:'. The 'SNMP Access:' section has a checkbox for 'Restrict SNMP access to SNMPv3 only', a text field for 'SNMPv2 Community Name:' with the value 'public', radio buttons for 'SNMPv2 Community Access Level:' (Restricted and Unrestricted), and radio buttons for 'SNMPv2 Operator/Manager Access:' (Operator and Manager). The 'Other Access:' section has checkboxes for 'Enable Telnet', 'Enable SSH', and 'Enable Web', and a checkbox for 'Restrict Web Access to SSL' with a note '(No Certificate Installed. To install a certificate choose the SSL tab.)'. There is also a checkbox for 'Enable USB Autorun' and a 'Session timeout:' field with the value '0'. At the bottom, there are three buttons: 'Back', 'Apply', and 'Exit'.

**Figure 1-3. Management Interface Wizard: Summary Setup**

From this screen, you have the following options:

- To change any setting that is shown, type in a new value or make a different selection.
- To apply the settings permanently, click **Apply**.
- To quit the Setup screen without saving any changes, click **Exit**.
- To return to the previous screen, click **Back**.

### **Web Wizard: Operating Notes and Restrictions.**

- If you click on the Web interface's navigation tab during setup, all configuration changes will be lost.
- If an Operator or Manager password has been configured on the switch, the enable USB Autorun option is not available.
- When you restrict SNMP access to SNMPv3 only, the SNMPv2 options are not available.
- The option to restrict Web Access to SSL is made available only if a server certificate has been previously installed on the switch.

## SNMP Security Guidelines

In the default configuration, the switch is open to access by management stations running SNMP (Simple Network Management Protocol) management applications capable of viewing and changing the settings and status data in the switch's MIB (Management Information Base). Thus, controlling SNMP access to the switch and preventing unauthorized SNMP access should be a key element of your network security strategy.

**General SNMP Access to the Switch.** The switch supports SNMP versions 1, 2c, and 3, including SNMP community and trap configuration. The default configuration supports versions 1 and 2c compatibility, which uses plain text and does not provide security options.

ProCurve recommends that you enable SNMP version 3 for improved security. SNMPv3 includes the ability to configure restricted access and to block all non-version 3 messages (which blocks version 1 and 2c unprotected operation).

SNMPv3 security options include:

- configuring device communities as a means for excluding management access by unauthorized stations
- configuring for access authentication and privacy
- reporting events to the switch CLI and to SNMP trap receivers
- restricting non-SNMPv3 agents to either read-only access or no access
- co-existing with SNMPv1 and v2c if necessary

**SNMP Access to the Authentication Configuration MIB.** Beginning with software release K.12.xxx, a management station running an SNMP networked device management application, such as ProCurve Manager Plus (PCM+) or HP OpenView, can access the switch's management information base (MIB) for read access to the switch's status and read/write access to the switch's authentication configuration (hpSwitchAuth). This means that the switch's default configuration now allows SNMP access to security settings in hpSwitchAuth.

---

**Note on SNMP  
Access to  
Authentication  
MIB**

---

Downloading and booting from the K.12.xxx or greater software version for the first time enables SNMP access to the authentication configuration MIB (the default action). If SNMPv3 and other security safeguards are not in place, the switch's authentication configuration MIB is exposed to unprotected SNMP access and you should use the command shown below to disable this access.

**If SNMP access to the hpSwitchAuth MIB is considered a security risk in your network**, then you should implement the following security precautions when downloading and booting from software release K.12.xx or greater:

- If SNMP access to the authentication configuration (hpSwitchAuth) MIB described above is not desirable for your network, then immediately after downloading and booting from the K.12.xx or greater software for the first time, use the following command to disable this feature:

**snmp-server mib hpswitchauthmib excluded**

- If you choose to leave the authentication configuration MIB accessible, then you should do the following to help ensure that unauthorized workstations cannot use SNMP tools to access the MIB:
  - a. Configure SNMP version 3 management and access security on the switch.
  - b. Disable SNMP version 2c on the switch.

For details on this feature, refer to the section titled “Using SNMP To View and Configure Switch Authentication Features” on page 6-26.

For more information on configuring SNMP, refer to the section “*Using SNMP Tools To Manage the Switch*” in the chapter “*Configuring for Network Management Applications*” in the *Management and Configuration Guide* for your switch.

## Precedence of Security Options

This section explains how port-based security options, and client-based attributes used for authentication, get prioritized on the switch.

### Precedence of Port-Based Security Options

Where the switch is running multiple security options, it implements network traffic security based on the OSI (Open Systems Interconnection model) precedence of the individual options, from the lowest to the highest. The following list shows the order in which the switch implements configured security features on traffic moving through a given port.

1. Disabled/Enabled physical port
2. MAC lockout (Applies to all ports on the switch.)
3. MAC lockdown
4. Port security
5. Authorized IP Managers
6. Application features at higher levels in the OSI model, such as SSH.  
(The above list does not address the mutually exclusive relationship that exists among some security features.)

### Precedence of Client-Based Authentication: Dynamic Configuration Arbiter

Starting in software release K.13.*xx*, the Dynamic Configuration Arbiter (DCA) is implemented to determine the client-specific parameters that are assigned in an authentication session.

A client-specific authentication configuration is bound to the MAC address of a client device and may include the following parameters:

- Untagged client VLAN ID
- Tagged VLAN IDs
- Per-port CoS (802.1p) priority
- Per-port rate-limiting on inbound traffic
- Client-based ACLs

DCA allows client-specific parameters configured in any of the following ways to be applied and removed as needed in a specified hierarchy of precedence. When multiple values for an individual configuration parameter exist, the value applied to a client session is determined in the following order (from highest to lowest priority) in which a value configured with a higher priority overrides a value configured with a lower priority:

1. Attribute profiles applied through the Network Immunity network-management application using SNMP (see “Network Immunity Manager”)
2. 802.1X authentication parameters (RADIUS-assigned)
3. Web- or MAC-authentication parameters (RADIUS-assigned)
4. Local, statically-configured parameters

Although RADIUS-assigned settings are never applied to ports for non-authenticated clients, the Dynamic Configuration Arbiter allows you to configure and assign client-specific port configurations to non-authenticated clients, provided that a client’s MAC address is known in the switch in the forwarding database. DCA arbitrates the assignment of attributes on both authenticated and non-authenticated ports.

DCA does not support the arbitration and assignment of client-specific attributes on trunk ports.

## Network Immunity Manager

Network Immunity Manager (NIM) is a plug-in to ProCurve Manager (PCM) and a key component of the ProCurve Network Immunity security solution that provides comprehensive detection and per-port-response to malicious traffic at the ProCurve network edge. NIM allows you to apply policy-based actions to minimize the negative impact of a client’s behavior on the network. For example, using NIM you can apply a client-specific profile that adds or modifies per-port rate-limiting and VLAN ID assignments.

---

**Note**

---

NIM actions only support the configuration of per-port rate-limiting and VLAN ID assignment; NIM does not support CoS (802.1p) priority assignment and ACL configuration.

NIM-applied parameters temporarily override RADIUS-configured and locally configured parameters in an authentication session. When the NIM-applied action is removed, the previously applied client-specific parameter (locally configured or RADIUS-assigned) is re-applied unless there have been other configuration changes to the parameter. In this way, NIM allows you to minimize network problems without manual intervention.

NIM also allows you to configure and apply client-specific profiles on ports that are not configured to authenticate clients (unauthorized clients), provided that a client's MAC address is known in the switch's forwarding database.

The profile of attributes applied for each client (MAC address) session is stored in the `hpicfUsrProfile` MIB, which serves as the configuration interface for Network Immunity Manager. A client profile consists of NIM-configured, RADIUS-assigned, and statically configured parameters. Using **show** commands for 802.1X, web or MAC authentication, you can verify which RADIUS-assigned and statically configured parameters are supported and if they are supported on a per-port or per-client basis.

A NIM policy accesses the `hpicfUsrProfileMIB` through SNMP to perform the following actions:

- Bind (or unbind) a profile of configured attributes to the MAC address of a client device on an authenticated or unauthenticated port.
- Configure or unconfigure an untagged VLAN for use in an authenticated or unauthenticated client session.

Note that the attribute profile assigned to a client is often a combination of NIM-configured, RADIUS-assigned, and statically configured settings. Precedence is always given to the temporarily applied NIM-configured parameters over RADIUS-assigned and locally configured parameters.

For information on Network Immunity Manager, go to the HP ProCurve Networking Web site at [www.procurve.com/solutions](http://www.procurve.com/solutions), click on **Security**, and then click on **Security Products**.

## Arbitrating Client-Specific Attributes

In previous releases, client-specific authentication parameters for 802.1X Web, and MAC authentication are assigned to a port using different criteria. A RADIUS-assigned parameter is always given highest priority and overrides statically configured local passwords. 802.1X authentication parameters override Web or MAC authentication parameters.

Starting in release `K.13.xx`, DCA stores three levels of client-specific authentication parameters and prioritizes them according to the following hierarchy of precedence:

1. NIM access policy (applied through SNMP)
2. RADIUS-assigned
  - a. 802.1X authentication
  - b. Web or MAC authentication
3. Statically (local) configured

Client-specific configurations are applied on a per-parameter basis on a port. In a client-specific profile, if DCA detects that a parameter has configured values from two or more levels in the hierarchy of precedence described above, DCA decides which parameters to add or remove, or whether to fail the authentication attempt due to an inability to apply the parameters.

For example, NIM may configure only rate-limiting for a specified client session, while RADIUS-assigned values may include both an untagged VLAN ID and a rate-limiting value to be applied. In this case, DCA applies the NIM-configured rate-limiting value and the RADIUS-assigned VLAN (if there are no other conflicts).

Also, you can assign NIM-configured parameters (for example, VLAN ID assignment or rate-limiting) to be activated in a client session when a threat to network security is detected. When the NIM-configured parameters are later removed, the parameter values in the client session return to the RADIUS-configured or locally configured settings, depending on which are next in the hierarchy of precedence.

In addition, DCA supports conflict resolution for QoS (port-based CoS priority) and rate-limiting (ingress) by determining whether to configure either strict or non-strict resolution on a switch-wide basis. For example, if multiple clients authenticate on a port and a rate-limiting assignment by a newly authenticating client conflicts with the rate-limiting values assigned to previous clients, by using Network Immunity you can configure the switch to apply any of the following attributes:

- Apply only the latest rate-limiting value assigned to all clients.
- Apply a client-specific rate-limiting configuration to the appropriate client session (overwrites any rate-limit previously configured for other client sessions on the port).

For information about how to configure RADIUS-assigned and locally configured authentication settings, refer to:

- RADIUS-assigned 802.1X authentication: *“Configuring Port-Based and User-Based Access Control (802.1X)” on page 13-1.*
- RADIUS-assigned Web or MAC authentication: *“Web and MAC Authentication” on page 4-1.*
- RADIUS-assigned CoS, rate-limiting, and ACLS: *“Configuring RADIUS Server Support for Switch Services” on page 7-1.*
- Statically (local) configured: *“Configuring Username and Password Security” on page 2-1.*

## ProCurve Identity-Driven Manager (IDM)

IDM is a plug-in to ProCurve Manager Plus (PCM+) and uses RADIUS-based technologies to create a user-centric approach to network access management and network activity tracking and monitoring. IDM enables control of access security policy from a central management server, with policy enforcement to the network edge, and protection against both external and internal threats.

Using IDM, a system administrator can configure automatic and dynamic security to operate at the network edge when a user connects to the network. This operation enables the network to:

- approve or deny access at the edge of the network instead of in the core;
- distinguish among different users and what each is authorized to do;
- configure guest access without compromising internal security.

Criteria for enforcing RADIUS-based security for IDM applications includes classifiers such as:

- authorized user identity
- authorized device identity (MAC address)
- software running on the device
- physical location in the network
- time of day

Responses can be configured to support the networking requirements, user (SNMP) community, service needs, and access security level for a given client and device.

For more information on IDM, go to the ProCurve Web site at [www.procurve.com/solutions](http://www.procurve.com/solutions), click on **Security**, and then click **Security Products**.