
Configuring Security for Network Devices

White Paper

You can configure security for HP networking devices through the device console, the device's Web browser-based agent, and/or the management application—HP TopTools for Hubs & Switches. The methods for configuring the level of security that you want while still being able to manage your devices are discussed in this paper.

Device Security

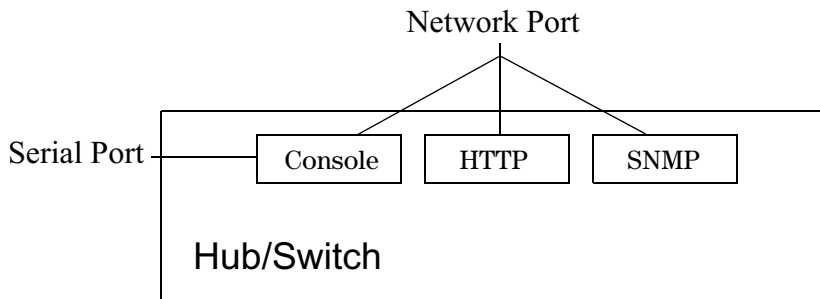
Configuring security for a networking device without using a management application can be accomplished in three ways:

- Device Console/Telnet Security
- Web (HTTP) Security
- SNMP Security

Device Console/Telnet Security

The console is a text-based interface for monitoring and configuring a device from a terminal or terminal emulator. You can access the console through the serial port or over the network via telnet. A password must be supplied to access the console interface. Newer devices such as switches and 100Base-T hubs may offer two levels of password and may require a user name as well.

Passwords are configured through the console interface. You can disable telnet access to the device by using the console interface. See the device's User Guide for specific instructions.



Note

When you use telnet to access a device, the password is sent over the network without any encryption.

Web (HTTP) Security

Newer HP hubs and switches support a Web browser-based interface. The HTTP protocol is used for monitoring or configuring the device from the browser. You can configure user names and passwords from the browser.

There are two categories of passwords:

- **Operator (Read only):** The Operator can view all pages except the Security pages. For switches, this password is the same as the console password.
- **Manager (Full Read and Write permissions):** The Manager can view all pages and make any changes in any page. The Manager name and password are the same as the name and password used in accessing the device through the console or a telnet session. If you change the password in this page, the console password is overwritten and becomes this password.

The minimum recommended setup is to have one Manager password. You can also configure the Manager name and password from the console, providing security for console access as well.

Manager/Operator Password Combinations

The level of protection and the access granted to the device depends on what passwords are set at what levels. The table below describes the settings and their consequences.

Table 1. Manager/Operator Password Combinations

Passwords	Read Protected	Write Protected	Results
Manager password set Operator password not set	N/A	Yes	Anyone can get Read Access, but only the Manager can read and write to the device. Recommended minimum setting.
Manager password set Operator password set	Yes	Yes	Both the Manager and the Operator have Read Access, but only the Manager has Write Access. Everyone else is shut out of the device. Recommended setting.
Manager password not set Operator password set	Yes	Yes	The Operator has both Read and Write Access because Write Access has not been reserved for the Manager.
Manager password not set Operator password not set	N/A	N/A	Anyone can get Read and Write Access to the device. Not recommended.

Access to the browser interface can be disabled using the console.

A challenge-response mechanism is used for verifying the user name and password. The password is modestly encrypted before it is sent over the *network*.

SNMP Security with Community Names

The Function of Community Names

A community defines authentication and access control between an SNMP agent and a management station. The community name functions as a password in that management stations must use the community name for all Get and Set operations. This is different and separate from the Operator and Manager passwords, which protect access to the browser interface and console settings.

You can configure HP devices with multiple community names and various levels of access. To use HP TopTools for Hubs & Switches, you should configure two community names, one with “read” level access, and one with “write” level access.

SNMP community names are not encrypted (IETF standards). For greater security accessing HP hubs and switches, use the Authorized Managers list to specify the addresses of the workstations from which SNMP requests are allowed. Be sure to include the address of any workstation on which HP TopTools for Hubs & Switches is running.

Note

In the following sections, there are reference marks (^{Note x}) on device types. These notes refer to Table 2 which lists the HP product numbers for the devices described.

Configuring Community Names

Older hubs^{Note 1} There is only one community name, referred to by the console as the “password”. This is the “write” community name. Use the name “public” as the “read” community name.

Newer hubs^{Note 2} Starting from the main menu of the device console:

1. Select “2. Management Access Configuration...” [or “5. Managers/Password change...”]
2. Select “2. Community Name” [or “2. Configure community name”] and add two new names.
3. For the “read” Community, set Read View = User; Write View = Discovery
4. For the “write” Community, set Read View = Full; Write View = Full

Most switches^{Note 3} Starting from the main menu of the device console:

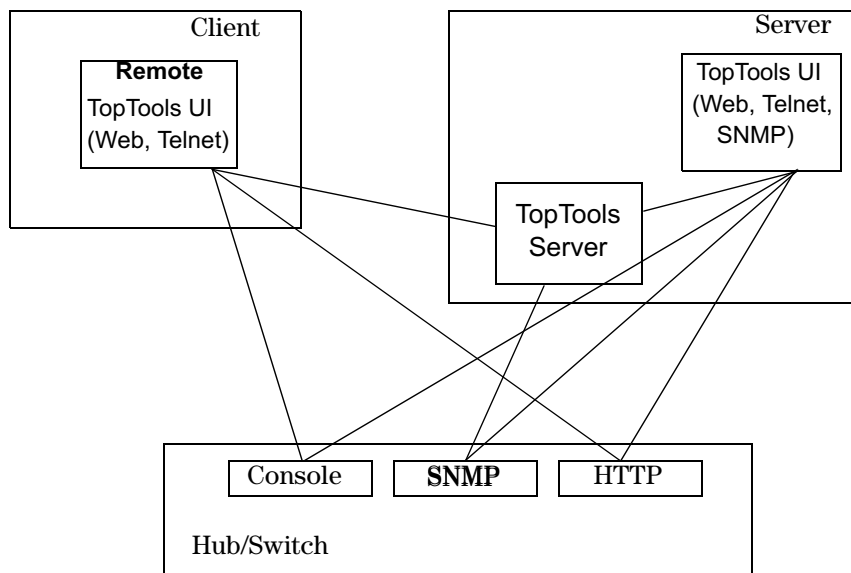
1. Select “Configuration...”
2. Select “SNMP Communities...” and add two new community names
3. For the “read” Community, set MIB View = Operator; Write Access = Restricted
4. For the “write” Community, set MIB View = Manager; Write Access = Unrestricted

The procedure for a few devices^{Note 4} is different. See your device’s User Guide.

TopTools Security

There are several additional security issues if you have installed HP TopTools. This section will address:

- How is access to the TopTools server secured?
- How can TopTools use the device security already configured?
- Problems with the TopTools security strategy.



TopTools Server Access

The security mechanism for TopTools is built on Windows NT and the Internet Information Server (IIS) or the Personal Web Server (PWS) security. The TopTools installation process prompts for a password, which is applied to the user “TopTools User” in the NT security group called “TopTools Group”.

The TopTools Group has full access to the subdirectories under /inetpub/wwwroot/hphtt. The installation for TopTools for Hubs & Switches also gives this group full access to the subdirectories under \TopTools. This is the default security setup. A user with NT Administrator privileges can modify this with NT’s extensive security options.

The “challenge-response” mechanism is used by IIS or PWS when prompting for the user name and password. The password is modestly encrypted before being sent over the *network*. By default “anonymous” access allows any user to read any web page. HP TopTools recommends using the IIS application to modify the “anonymous” access.

When you first access a TopTools web page, the NT security mechanism will cause the web server to prompt for a user name and password. The name and password supplied must permit access to the directories that contain the files for that page. With the default security, the you have access to all the pages in TopTools, or none of the pages.

If you are using TopTools and want to access a page that is provided directly from a device, the web security for the device becomes active. You will be prompted for a user name and password to access the web interface of the device.

If you telnet from TopTools to a device, you must supply the password for the device console.

Using Device Community Names with HP TopTools

If Discovery has not already run, run Discovery for all desired networks. Be sure to check Ping Discovery and Web Server Discovery (see the online help). If all your devices are not discovered, you can add them manually as follows:

1. In the TopTools home page, select the **Settings** button and select **Discovery** from the menu.
2. In the Discovery page, select the **Additional Devices** tab.
3. Type in the address of the device and click the **Add Device** button.

To inform TopTools of the community names for each device, do these steps:

1. In the TopTools home page, select **Devices** and select **Device Types** from the menu.
2. Select the **All Devices** tab.
3. Select the device from the list at the right. You can select multiple devices if they have the same community name.
4. Click the right mouse button on one of the devices.
5. Select the **Security** menu item, then select **Set SNMP Passwords** (Communities).
6. Type in the “read” community (twice) for the selected devices and click **Set Read Password**.

7. Type in the “write” community (twice) for the selected devices and click **Set Write Password**.
8. Run Discovery again.

All the features of HP TopTools for Hubs & Switches will now work correctly for all HP devices, except as noted in the section “TopTools Known Problems”.

Note

You may want to add routers manually as well, and define their community names. This improves the discovery process.

TopTools Known Problems

The following problems exist for devices that have been configured with both a “read” and “write” community name other than “public”:

1. For new devices,^{Note 2, 3} the **Update Firmware** option on the Devices page does not work.
2. For newer devices,^{Note 2, 3} The **SNMP Trap Configuration** option in the Devices page does not work.
3. For a few device models,^{Note 5} the Closeup View cannot be launched from the Devices page or the Topology map.
4. Automatic Management does not launch automatically for these devices after discovery.
5. The topology of some older devices may not display correctly.

Workarounds for Problems

For the first three problems, you can use “public” as the “read” community name for those devices. You can increase security for all the devices (except J3233A) by specifying the workstation with TopTools as the only Authorized Manager for “public” on each device.

For the fourth problem, you can apply the Automatic Management settings manually. Use the procedure in the *readme.htm* file titled “Using Auto Management to get your devices in sync”.

Recommended Security Procedures

The following suggestions will allow you to provide maximum security for your devices while maintaining the ability to manage them.

On the console:

1. Configure a community with “write” capability. Do not use “public”.
2. Configure a community name of “public” with read-only capability. You do not need to do this on older devices^{Note 1}.
3. Add the TopTools server to the list of authorized managers for the “write” level community name. this prevents any other address from using that community name to change values on that device. This feature is not available on older devices^{Note 1} and on model HP J3233A.

4. Add the TopTools server to the list of authorized managers for the “public” community name. This prevents any other addresses from using “public” to read values from that device. This feature is not available on older devices^{Note 1} and the HP J3233A.
5. Define a password for the console. Use at least a Manager or “write” level password for those devices that support two passwords.
6. Disable telnet access. See the User Guide for each device.

From HP TopTools:

1. When you are installing TopTools, assign a password to control access to the TopTools web pages.
2. On the TopTools server, user the Internet Service Manager to disable “anonymous” access to the web server.
3. On the Devices page, inform TopTools of the read and write community names assigned to each device.

Results of Recommendations

If you follow the above recommendations, you can expect the following results:

1. Because there is no telnet access, the console requires physical access to the device, unless there is a modem and phone line attached to the device. You will need a serial cable and terminal or PC in order to access the device console. You must know the console password.
2. Web access to devices is secured by the same password, which is modestly encrypted by the browser before being sent over the network.
3. SNMP access to devices is only available from the TopTools server. It is further secured by the defined read and write community names.
4. Web access to the HP TopTools web pages is secured by the password entered during TopTools installation, and involves going through the Microsoft account security system. The password is modestly encrypted by the browser.
5. You can manage from anywhere inside the Intranet.

Reference List of HP Devices

Table 2. HP Product Numbers

Note 1 Devices (Hubs & Bridges)	Note 2 Devices (Hubs)	Note 3 Devices (Switches)	Note 4 Devices (Hub & Switches)	Note 5 Devices (Switches)
28673A	J3200A	J3100A/B	J3125A	J3100A
28674A/B	J3202A	J3175A	J3126A	J3125A
28688A/B	J3204A	J3177A	J3233A	J3126A
28682A	J3301A	J3245A		J3175A
28692A	J3303A	J3298A		J3177A
28699A		J3299A		
J2355A		J4110A		
J2410A		J4120A		
J2413A		J4121A		
J2415A		J4122A		
J2601A/B				
J2602A/B				
JJ2610A				
J2611A/B				
J2612A				
J2630A				
J2631A				
J2632A				

Technical information subject to change without notice.
 © Copyright 1998, Hewlett-Packard Company

August 1998