



# Management Protocols

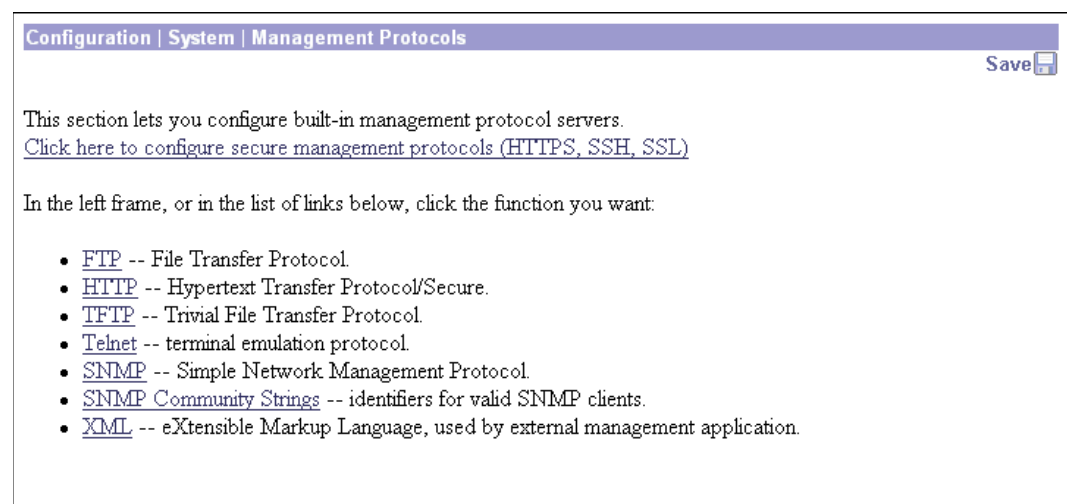
The VPN 3000 Concentrator Series includes various built-in servers, using various protocols, that let you perform typical network and system management functions. This section explains how you configure and enable those servers.

## Configuration | System | Management Protocols

This section of the Manager lets you configure and enable built-in VPN Concentrator servers that provide management functions using:

- [FTP](#)
- [HTTP](#)
- [TFTP](#) (Trivial File Transfer Protocol)
- [Telnet](#), and Telnet over SSL
- [SNMP](#) (Simple Network Management Protocol)
- [SNMP Communities](#): Identifiers for valid SNMP clients
- [XML](#) (Extensible Markup Language)

**Figure 8-1** Configuration | System | Management Protocols Screen



104855

# FTP

This screen lets you configure and enable the VPN Concentrator's FTP server. When the server is enabled, you can use an FTP client to upload and download files in VPN Concentrator Flash memory.

FTP server login usernames and passwords are the same as those enabled and configured on the Administration | Access Rights | Administrators screens. To protect security, the VPN Concentrator does not allow anonymous FTP login.

The settings here have no effect on FTP backup of event log files. (See System | Events | [General](#) and System | Events | [FTP Backup](#).) For those operations, the VPN Concentrator acts as an FTP client.

**Figure 8-2** Configuration | System | Management Protocols | FTP Screen

## Screen Elements

- **Enable** — Check this box to enable the FTP server. The box is checked by default. Disabling the FTP server provides additional security.
- **Port** — Enter the port number that the FTP server uses. The default value is 21.
- **Maximum Connections** — Enter the maximum number of concurrent control connections (sessions) that the FTP server allows. (FTP uses separate connections for control and data transfer during a session.) The minimum number is 1. The default is 5. The maximum is 20.

### Reminder:

After you apply changes, the Manager returns to the [Configuration | System | Management Protocols](#) screen. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

# HTTP

This screen lets you configure and enable the VPN Concentrator's HTTP server. When the server is enabled, you can use a web browser to communicate with the VPN Concentrator.



## Note

The VPN Concentrator Manager requires either the HTTP or HTTPS server. *Clicking Apply, even if you have made no changes on this screen, breaks your HTTP/HTTPS connection and you must restart the Manager session from the login screen.*

If you disable *either* HTTP or HTTPS, and that is the protocol you are currently using, you can reconnect with the other protocol if it is enabled and configured.

If you disable *both* HTTP and HTTPS, you cannot use a web browser to connect to the VPN Concentrator. Use the Cisco Command Line Interface from the console or a Telnet session.

If you disable HTTPS, you cannot use WebVPN.

Related information:

- For information on installing the SSL digital certificate in your browser and connecting via HTTPS, see “[Chapter 1, “Using the VPN Concentrator Manager.”](#)”
- To configure SSL and HTTPS parameters, see the Tunneling and Security | [SSL](#) screen.
- To install, generate, view, or delete the SSL certificate on the VPN Concentrator, see the Administration | Certificate Management screens.

**Figure 8-3** Configuration | System | Management Protocols | HTTP Screen

Configuration | System | Management Protocols | HTTP

Configure the HTTP server. Configuration for HTTPS can be found at [Configuration | Tunneling and Security | SSL | HTTPS](#).

If you click **Apply**, you will break your HTTP connection to this device, and you will have to restart from the login screen.

**Enable HTTP**  Disabling will provide additional security.

**HTTP Port**  The default port is 80. Changing the port will provide additional security.

**Maximum Sessions**  Enter the maximum number of concurrent HTTP/HTTPS management sessions.

104971

## Screen Elements

- **Enable HTTP** — Check this box to enable the HTTP server. The box is checked by default. You must enable HTTP to install the SSL certificate in the browser initially, so you can thereafter use HTTPS. Disabling the HTTP server provides additional security, but makes system management less convenient. See the preceding notes.

- **HTTP Port** — Enter the port number that the HTTP server uses. The default value is 80.
- **Maximum Sessions** — Enter the maximum number of concurrent, combined HTTP management sessions that the server allows. The minimum number of sessions is 1. The default number is 4. The maximum number is 10.
- **Apply / Cancel** — To apply your HTTP server settings, to include your settings in the active configuration, *and to break the current HTTP connection*, click **Apply**. If HTTP is still enabled, the Manager returns to the main login screen. If both HTTP and HTTPS are disabled, you can no longer use the Manager.

### Reminder:

After you apply changes, the Manager returns to the [Configuration | System | Management Protocols](#) screen. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

## TFTP

This screen lets you configure and enable the VPN Concentrator's TFTP server. When the server is enabled, you can use a TFTP client to upload and download files in VPN Concentrator Flash memory.

TFTP is similar to FTP, but it has no login procedure and no user interface commands. It allows only file transfers. The lack of a login procedure makes it relatively insecure.

The settings here have no effect on TFTP file transfer from the Administration | File Management | TFTP Transfer screen. For those operations, the VPN Concentrator acts as a TFTP client.

**Figure 8-4** Configuration | System | Management Protocols | TFTP Screen

### Screen Elements

- **Enable** — Check this box to enable the TFTP server. The box is unchecked by default. Disabling the TFTP server provides additional security.
- **Port** — Enter the port number that the TFTP server uses. The default port number is 69.
- **Maximum Connections** — Enter the maximum number of simultaneous connections that the TFTP server allows. The minimum number is 1. The default number is 5. The maximum number is 20.
- **Timeout** — Enter the timeout in seconds for inactive TFTP connections. The minimum timeout is 1 second. The default is 10 seconds. The maximum is 30 seconds. Change the default value only if you have problems with TFTP transfers.

# Telnet

This screen lets you configure and enable the VPN Concentrator's Telnet terminal emulation server. When the server is enabled, you can use a Telnet client to communicate with the VPN Concentrator. You can fully manage and administer the VPN Concentrator using the Cisco VPN Concentrator Command Line Interface via Telnet.

Telnet server login usernames and passwords are the same as those enabled and configured on the Administration | Access Rights | Administrators screens.

To configure SSL parameters, see the Tunneling and Security | [SSL](#) screen. To manage the SSL digital certificate, see the Administration | Certificate Management screens.

**Figure 8-5** Configuration | System | Management Protocols | Telnet Screen

Configuration | System | Management Protocols | Telnet

Configure the Telnet server.

**Enable Telnet**  Disabling will provide additional security.

**Telnet Port**  The default port is 23. Changing the port will provide additional security.

**Maximum Connections**  Enter the maximum number of concurrent connections. *This limit also applies to SSH.*

Apply Cancel

104879

## Screen Elements

- **Enable Telnet** — Check this box to enable the Telnet server. The box is checked by default. Disabling the Telnet server provides additional security, but doing so prevents using the Cisco VPN Concentrator Command-Line Interface via Telnet.
- **Telnet Port** — Enter the port number that the Telnet server uses. The default value is 23.
- **Maximum Connections** — Enter the maximum number of concurrent Telnet connections that the server allows. The minimum number is 1. The default number is 5. The maximum number is 10.

### Reminder:

After you apply changes, the Manager returns to the [Configuration | System | Management Protocols](#) screen. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

# SNMP

This screen lets you configure and enable the VPN Concentrator's SNMP server. When the server is enabled, you can use an SNMP client to collect information from the VPN Concentrator but not to configure it.

To use the SNMP server, you must also configure an SNMP Community on the System | Management Protocols | [SNMP Communities](#) screen.

The settings on this screen have no effect on sending system events to SNMP trap destinations (see System | Events | [General](#) and System | Events | [Trap Destinations](#)). For those functions, the VPN Concentrator acts as an SNMP client.

**Figure 8-6** Configuration | System | Management Protocols | SNMP Screen

Configuration | System | Management Protocols | SNMP

Configure the SNMP server.

**Enable**  Disabling will provide additional security. You can use third-party SNMP managers only for viewing statistics, not for configuring this device.

**Port**  The default port is 161. Changing the port will provide additional security.

**Maximum Queued Requests**  Enter the maximum number of outstanding queued requests.

Apply Cancel

67249

## Screen Elements

- **Enable** — Check this box to enable the SNMP server. The box is checked by default. Disabling the SNMP server provides additional security.
- **Port** — Enter the port number that the SNMP server uses. The default value is 161.
- **Maximum Queued Requests** — Enter the maximum number of outstanding queued requests that the SNMP server allows. The minimum number is 1. The default number is 4. The maximum number is 200.

### Reminder:

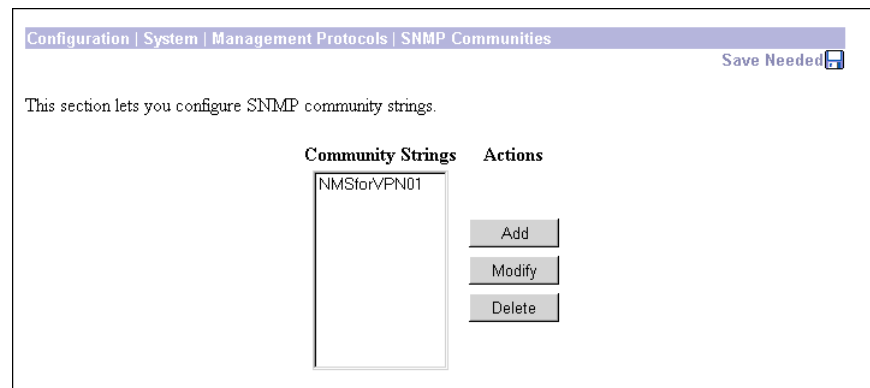
After you apply changes, the Manager returns to the [Configuration | System | Management Protocols](#) screen. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

# SNMP Communities

This section of the Manager lets you configure and manage SNMP community strings, which identify valid communities from which the SNMP server will accept requests. A community string is like a password: it validates messages between an SNMP client and the server.

To use the VPN Concentrator SNMP server, you must configure and add at least one community string. You can configure a maximum of 10 community strings. To protect security, the SNMP server does *not* include the usual default public community string, and we recommend that you not configure it.

**Figure 8-7** Configuration | System | Management Protocols | SNMP Communities Screen



## Screen Elements

- **Community Strings** — The Community Strings list shows SNMP community strings that have been configured. If no strings have been configured, the list shows --Empty--.
- **Add** — Click to configure and add a new community string. The Manager opens the System | Management Protocols | [SNMP Communities | Add or Modify](#) screen.
- **Modify** — To modify a configured community string, select the string from the list and click **Modify**. The Manager opens the System | Management Protocols | [SNMP Communities | Add or Modify](#) screen.
- **Delete** — To delete a configured community string, select the string from the list and click **Delete**. *There is no confirmation or undo.* The Manager refreshes the screen and shows the remaining entries in the list.

### Reminder:

After you apply changes, the Manager returns to the [Configuration | System | Management Protocols](#) screen. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

# SNMP Communities | Add or Modify

These Manager screens let you:

- Add: Configure and add a new SNMP community string.
- Modify: Modify a configured SNMP community string.

**Figure 8-8** Configuration | System | Management Protocols | SNMP Communities | Add or Modify Screen

Configuration | System | Management Protocols | SNMP Communities | Add

Add an SNMP Community string.

Community String  Enter the community string.

Add Cancel

67244

## Screen Elements

- **Community String** — Enter the SNMP community string. Maximum 31 characters, case-sensitive.
- **Add or Apply** — To add this entry to the list of configured community strings, click **Add**. Or to apply your changes to this community string, click **Apply**. Both actions include your entry in the active configuration. The Manager returns to the System | Management Protocols | [SNMP Communities](#) screen; a new entry appears at the bottom of the Community Strings list.
- **Cancel** — To discard your entry or changes, click **Cancel**. The Manager returns to the System | Management Protocols | [SNMP Communities](#) screen, and the Community Strings list is unchanged.

## Reminder:

After you apply changes, the Manager returns to the System | Management Protocols | [SNMP Communities](#) screen. To save the active configuration and make it the boot configuration, click the **Save Needed** icon at the top of the Manager window.

# XML

This screen lets you configure the VPN Concentrator to support an XML-based management interface. Enabling XML management allows VPN 3000 Concentrators to be more easily managed by a centralized management system. XML is enabled by default. To disable the XML option, clear the check box. To re-enable the XML option, click the check box.

On this screen, you can also configure the VPN Concentrator to enable HTTPS or SSH (or both) on the Concentrator's Public interface and to lock the XML interface to a specific HTTPS or SSH IP address.

**Figure 8-9** Configuration | System | Management Protocols | XML Screen

Configuration | System | Management Protocols | XML

Configure XML management.

**Enable**  Check to enable XML management. Note that HTTPS or SSH must be enabled.

**Enable HTTPS on Public**  Check to enable HTTPS on the Public interface. This will allow XML over HTTPS through the Public interface.

**HTTPS IP Address**  Enter the IP address and wildcard from which to allow HTTPS access on on the Public interface. **Note: Enter a *wildcard* mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. Entering 0.0.0.0 will match the specified address; entering 255.255.255.255 will match *all* addresses.

**HTTPS Wildcard-mask**

**Enable SSH on Public**  Check to enable SSH on the Public interface. This will allow XML over SSH through the Public interface.

**SSH IP Address**  Enter the IP address and wildcard from which to allow SSH access on on the Public interface. **Note: Enter a *wildcard* mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. Entering 0.0.0.0 will match the specified address; entering 255.255.255.255 will match *all* addresses.

**SSH Wildcard-mask**

68224

## Screen Elements

- **Enable** — Check this box, the default, to enable the XML management capability. You must also enable HTTPS or SSH on the VPN 3000 Concentrator's Public interface. Because enabling the XML management capability facilitates managing the VPN 3000 Concentrator by an external management application, do not disable the XML management capability unless you have a specific reason for doing so.
- **Enable HTTPS on Public** — Check this box to allow HTML or XML management over HTTPS on the VPN Concentrator's Public interface. If this field is already checked, and is unselectable, WebVPN and/or HTTPS management (Tunneling and Security | [SSL](#) | [HTTPS](#)) is already enabled on the public interface.

- **HTTPS IP Address** — Enter the IP address from which to allow HTTPS access on the VPN Concentrator's Public interface.
- **HTTPS Wildcard-mask** — Enter the wildcard mask for the HTTPS IP address.

**Note**

---

Enter a *wildcard* mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, and 0s in bit positions to match. For example, entering 0.0.0.0 matches the *specified* address; entering 255.255.255.255 matches *all* addresses.

---

- **Enable SSH on Public** — Check this box to allow command-line or XML management over Secure Shell (SSH) on the VPN Concentrator's Public interface.
- **SSH IP Address** — Enter the IP address from which to allow SSH access on the VPN Concentrator's Public interface.
- **SSH Wildcard-mask** — Enter the wildcard mask for the SSH IP address.

**Note**

---

Enter a *wildcard* mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, and 0s in bit positions to match. For example, entering 0.0.0.0 matches the *specified* address; entering 255.255.255.255 matches *all* addresses.

---