CHAPTER 11

Network Configuration

When you click the **Configure Network** button in the navigation pane, you are taken to the Configure Network Settings page. The navigation bar across the top contains links to this section's subpages.

- **Network Settings** links to Configure Network Settings
- **SNMP Syslog** links to SNMP/SYSLOG Settings
- **Date & Time** links to Configure Time and Date
- **Security** links to Security Settings
- **SSL** links to SSL Configuration
- **GUI Settings** links to GUI Settings

Configure Network Settings

Clicking **Configure Network** takes you to the Configure Network Settings page, which allows you to configure all of the settings on each network port.

The information is arranged by controller and then by port. **Current status** indicates whether the link is up or down. If the link is up, it displays the current link speed and duplex mode setting.

For each port, you can configure the following settings:

- **Port Settings**: For most networks, the default setting of **Auto Speed, Auto Duplex** is recommended. However, if your LAN switch does not support auto-negotiation, you can "force" one or both settings. The options are:

  Auto Speed, Auto Duplex
  Auto Speed, Fixed Full Duplex
  Auto Speed, Fixed Half Duplex
  Fixed to 100Mbit Full Duplex
  Fixed to 100Mbit Half Duplex
  Fixed to 10Mbit Full Duplex
  Fixed to 10Mbit Half Duplex

- **Hostname**: This defaults to the host's address. Enter a "friendly" host name for the port, if desired.
- **Assign IP Address**: You can choose whether to **Use DHCP** (Dynamic Host Configuration Protocol, the default) or **Use Static IP**.

  If you select Use DHCP, then no other configuration is needed.

Note NOTE: In order to use DHCP, your network must be configured for DHCP. If it is not, you MUST use a static IP address.

If you select **Use Static IP**, then you must fill in the **Static IP Address** and **Subnet Mask**. If you wish to use a time server (see Configure Time and Date, page 11-3), you should also fill in values for **Gateway**, **Primary DNS**, and **Secondary DNS**.

When you have selected the desired new settings, do one of the following:

- Click **Save Configuration**. The settings are saved and are applied after the system is restarted (see Reboot System, page 10-3).
- Click **Save and Apply Changes**. The settings are saved and applied immediately.

Note If at any time you wish to return the Configure Network Settings page to its initial state, click **Reset**.

SNMP/SYSLOG Settings

Clicking **Configure Network > SNMP Syslog** takes you to the SNMP/SYSLOG Settings page, which allows you to configure settings for SNMP traps and system log (SYSLOG) messages.

Caution SNMP and SYSLOG both use UDP messaging which does not have guaranteed delivery. You may miss critical messages concerning the storage unit.

Information captured by an SNMP trap or a SYSLOG message is sent to an SNMP Network Management Station or system log.

Note If you use SNMP traps, you must parse the trap MIB (Management Information Base) into your application. Use the **MIB** links in the Help section at the bottom of the page to download the MIB for SNMP v1 and v2c.

Note NOTE: Only SNMP traps are available; there is no general SNMP management capability in the unit.

To set up SNMP traps, configure the following settings:

- **SNMP server IP address *N***: Enter the IP address that SNMP traps will be sent to. One or two IP address can be specified. The default is “Not Configured”.
- **Community string**: Enter the SNMP Network Management Server password. By default, this is “public”.
- **Trap version**: Select the type of SNMP trap that is to be sent: **SNMPv1** (the default) or **SNMPv2c**.
- **When to send SNMP traps**: Using the drop-down list, select what kinds of events (see Event Log, page 5-7) will be sent as SNMP traps. There are five options: **Do not send SNMP traps** (the default), **Send SNMP traps for errors only**, **Send SNMP traps for warnings and errors**, **Send SNMP traps for information, warnings and errors**, and **Send SNMP traps for all events**.

To set up SYSLOG messages, configure the following settings:

- **SYSLOG server IP address**: Enter the IP address of the host running the SYSLOG service that will receive the SYSLOG messages.
- **SYSLOG server UDP port**: Enter the UDP port number that the management station is listening to. The default is 514.
- **SYSLOG Facility**: Using the drop-down list, select the designation for the part of the system the SYSLOG message originates from. This is defined by the SYSLOG protocol. Options will vary depending on your operating system.
- **When to send a SYSLOG message**: Using the drop-down list, select what kinds of events (see Event Log, page 5-7) will be sent in SYSLOG messages. There are five options: **Do not send SYSLOG messages** (the default), **Send SYSLOG messages for errors only**, **Send SYSLOG messages for warnings and errors**, **Send SYSLOG messages for information, warnings and errors**, and **Send SYSLOG messages for all events**.

When you have configured the SNMP and SYSLOG settings, click **Save Settings**. A message is displayed, informing you that the settings have been updated. Click the **Back** button to return to the SNMP/SYSLOG Settings page.

Note If at any time you wish to return the SNMP/SYSLOG Settings page to its initial state, click **Reset**.

To test your settings, enter a test phrase (default "test string") in the **Test String** field, then click **Test SNMP** or **Test SYSLOG**. A message is displayed, informing you that the test string has been sent, and the management station or SYSLOG file will receive the test string within a few minutes. Click the **Back** button to return to the SNMP/SYSLOG Settings page.

Configure Time and Date

Clicking **Configure Network > Date and Time** takes you to the Configure Time and Date page, which lets you set the time and date used by the unit's internal clock. This can be done manually or automatically.

To Set the Time and Date Manually

Step 1 Enter the time in the **Time entered in 'hh:mm:ss' format** field.

Note The time entered in the **Time entered in 'hh:mm:ss' format** field will be set when the **Save Settings** button is clicked. Therefore, it is suggested that you enter the time rounded to the next five minute mark, then click **Save Settings** when the entered time is reached.

Step 2 Enter the date using the **Date** drop-down lists.

Step 3 Select the **Timezone relative to GMT (GMT offset)** using the drop-down list.

Step 4 Click **Save Settings**.

To Set the Time and Date Automatically

Note For automatic time setting to work, you may have to configure the Gateway setting for your network. See Configure Network Settings, page 11-1 for more information.

Step 1 Select the **Timezone relative to GMT (GMT offset)** using the drop-down list.

Step 2 Next to **Time server IP address to use for auto time and date configure**, do one of the following:

- Select **Use IP address from list** and select a time server IP address from the drop-down list.
- Select **Use entered IP address** and enter the IP address of a known time server into the text box.

Step 3 Next to **Time server protocol**, select either **Daytime** or **SNTP**.

Step 4 If you entered a time server IP address in Step 2 and selected **Daytime** in Step 3, select the **Time server time and date format** using the drop-down list.

Note If you do not know the format of the time server data, click the **Retrieve Time Server Data** button. The data is retrieved and displayed next to **Data retrieved from contacting the daytime server**. Use this data to choose the proper format in the **Time server time and date format** dropdown list.

Step 5 If you wish the unit to contact the time server every twenty-four hours to update the time and date, select the check box next to **Set system time and date by the time server every 24 hours**.

Step 6 Click **Save Settings**.

Step 7 If you wish to update the time immediately, click the **Contact Time Server To Auto Configure Time And Date** button. The time and date are updated immediately.

Security Settings

Clicking **Configure Network > Security** takes you to the Password Configuration page, which lets you set passwords for the administrator-level (ADMIN) and user-level (USER) accounts.

Caution RESETTING TO FACTORY DEFAULTS WILL RESET THE PASSWORDS.

This page displays the following information for configuring system login:

- **Current "ADMIN"/"USER" login password requirements**: Indicates whether a password is currently required for the ADMIN or USER account, respectively.
- **Change "ADMIN"/"USER" login password requirement to**: Select **NOT Required** (the default) to disable password-protected login. Select **Required** to enable password-protected login.
- **Login user name is fixed to**: Displays the account user name: **ADMIN** or **USER**.
- **Current Password**: Enter the current account password to make changes. If password-protected login is currently disabled for this account, this item is not displayed.
- **New Password**: Enter the new account password. Passwords should be eight characters or longer and can contain both letters and numbers, but not special characters or punctuation.

- **Confirm Password**: Re-enter the password you entered for **New Password**. The two fields must match exactly.

To save the new password settings for the administrator account, click **Set ADMIN Password**. To save the new password settings for the user account, click **Set USER Password**. In either case, a message is displayed, indicating that the settings have been changed. Click the **Back** button to return to the Password Configuration page.

Note NOTE: Before you can configure security settings for the USER account, you must first configure and apply security settings for the ADMIN account.

The Connected Host Access section lets you configure the option to allow hosts that are connected to the storage area network (SAN) to provision the storage system directly, without requiring the ADMIN password. This feature requires compatible storage management software to be installed on the host. This section displays the following information:

- **Current host trust setting**: The current level at which SAN-connected hosts can access the storage system without the ADMIN password.
- **Change host trust setting to**: Select one of the four levels:
  - **None**: Host-based management access is disabled.
  - **Read-only**: Hosts can read information about the RAID storage system, but cannot provision storage.
  - **Limited** (default): Hosts can create new volumes, and expand or delete any volumes to which they have read/write access.
  - **Full**: Hosts can create new volumes, modify volume access rights, and expand or delete any volumes on the RAID system.

Click **Set Host Trust Setting** to save your changes. A message is displayed, indicating that the settings have been changed. Click the **Back** button to return to the Password Configuration page.

Caution If untrusted users have administrative access to hosts on the storage area network (SAN), we strongly recommend that you set this option to **None**.

SSL Configuration

Clicking **Configure Network > SSL** takes you to the SSL Configuration page, which allows you to set up Secure Sockets Layer (SSL) encryption between the storage system and the browser accessing the system's Management Console.

The Configure SSL section displays the following information:

- **SSL status**: The current SSL configuration. Also shows any certificate problems and a download link for the current root CA certificate (when applicable).

  Note It is recommended that you download the root CA certificate and add it to your browser's trusted certificate list to avoid certificate errors when connecting via HTTPS.

- **SSL mode**: The type of browser connection allowed by the RAID system. Select the desired option:

  - **HTTP only** (the default): Disables SSL or HTTPS connection.
  - **HTTPS only**: Enables SSL/HTTPS connection and disables unsecured (HTTP) connection.
  - **HTTPS and HTTP**: Allows both SSL/HTTPS and unsecured HTTP connections.

The Configure Certificate and Key (Advanced) section displays the following information:

- **Dynamic certificate**: This is the default mode. The SSL key and certificate are automatically generated at startup and signed with the default Cisco root CA certificate.
- **Dynamic certificate inherited from uploaded CA root**: The SSL key and certificate are automatically generated at startup and signed with the uploaded root CA certificate. To select this mode, you must provide and select files for the **Certificate** and **Key** by clicking **Browse** and navigating to the files according to the method of your operating system. CA certificate and SSL key files must be in PEM or DER format.
- **Use uploaded certificate and key**: Uses the uploaded certificate and key (PEM or DER format) as long as both files are valid. On dual-controller systems, you must provide different files for each controller.

To save SSL settings, click **Save Configuration**. A message is displayed, indicating that the settings have been changed. Click the **Back** button to return to the SSL Configuration page.

GUI Settings

Clicking **Configure Network > GUI Settings** takes you to the GUI Settings page, which allows you to configure Management Console options.

This page contains the following settings:

- **Enable GUI enhancements (requires Javascript)**: This option is enabled by default. If your browser does not support JavaScript, or if the JavaScript enhancements cause browser problems, disable this option.

  Note Sometimes, JavaScript errors can prevent user login. If this occurs, enter `http://<IPaddress>/admin/guiprefs.asp` into the browser's address bar to load this page directly. JavaScript can then be turned off and login reattempted.

- **Enable persistent tooltips (requires Javascript)**: This option is disabled by default. Enable this option to display pop-up tool tips when the mouse pointer is hovered over an icon. This option requires that the **Enable GUI enhancements** option is enabled.
- **Minimize page scrolling by using submenus where appropriate**: This option is disabled by default. Enable this option to show a summary submenu of links on certain pages. This submenu reduces the need to scroll on long pages.

  Note Enabling this option may change the way in which you are able to access certain features. In such cases, the instructions in this Administration Guide may not match your experience.

- **Minimize page scrolling by showing less information**: This option is disabled by default. Enable this option to show only essential information on each page.

Note Enabling this option may hide certain features from view or change the way in which you are able to access them. In such cases, the instructions in this Administration Guide may not match your experience.

- **Highlight array text using different colors**: This option is enabled by default. Text displayed below disk icons is color-coded by array to aid in visual identification of array members. Disable this option if you wish to display all disk text in black.
- **Select the units you wish to use for volume and free space entry**: The default setting for this option is **Gigabytes (GB)**. Select a different option, if desired. The five options are: **Megabytes (MB)**, **Gigabytes (GB)**, **Percentage of array size (%)**, **Binary Megabytes (MiB)**, and **Binary Gigabytes (GiB)**.
- **Web page auto refresh (10 to 120 secs)**: This option is enabled and set to **30** seconds by default. When no links or buttons are clicked in the Management Console for this length of time, the page is automatically refreshed with updated information from the unit. Disable this option to stop pages from automatically refreshing. Change the number in the **Auto refresh time** field to make automatic page refresh happen more or less often.

To save settings changes, click **Save Settings**. A message is displayed, indicating that the settings have been changed. Click the **Back** button to return to the GUI Settings page.