USER'S GUIDE
AUTOMATIC TRANSFER SWITCH

Contents

Introduction

Product Description

Available interfaces

The Automatic Transfer Switch (ATS) can be managed locally with internal menus accessed through a serial connection. This connection can also be used to access the Management Card.

See Web Config for more information on accessing the Management Card using the serial connection.

The Management Card has two internal interfaces (control console and Web interface), which provide menus with options that enable you to manage the Automatic Transfer Switch and the Management Card. The Management Card's SNMP interface enables you to use an SNMP browser with the PowerNet® Management Information Base (MIB) to manage the Automatic Transfer Switch.

To manage the unit remotely, use a Web browser for the Web interface, or Telnet or Secure SHell (SSH) for the control console interface.

For more information about the Management Card's internal user interfaces, see Control Console and Web Interface.

See also

To use the PowerNet MIB with an SNMP browser, see the *PowerNet® SNMP Management Information Base (MIB) Reference Guide* (**.\doc\en\Mibguide.pdf**), which is provided on the APC Automatic Transfer Switch *Utility* CD.

Initial set-up

You must define three TCP/IP settings for the Network Management Card before it can operate on the network:

- IP address of the Management Card
- Subnet mask
- IP address of the default gateway

See also

To configure the TCP/IP settings, see the *Automatic Transfer Switch Installation and Quick Start Manual*, provided in printed form, and provided on the APC Automatic Transfer Switch *Utility* CD as a PDF file (**.\doc\en\Insguide.pdf**).

Internal Management Features

Access priority for logging on

Only one user at a time can log onto the Management Card to use its internal user interface features. The priority for access is as follows:

- Serial access has the highest priority.
- Telnet or SSH access to the control console from a remote computer has priority over Web access.
- Web access either directly or through InfraStruXure Manager has the lowest priority.

For information about how SNMP access to the Management Card is controlled, see SNMP.

Types of user accounts

The Management Card has three levels of access (Administrator, Device Manager, and Read-Only), all of which are protected by **Password** and **User Name** requirements.

- An Administrator can use all of the management menus available in the control console and the Web interface. The Administrator's default **User Name** and **Password** are both **apc**.
- A Device Manager can use only the following menus:
  - The **Status** option of the **Automatic Transfer Switch** menu.(The **Automatic Transfer Switch** menu is an option of the **Device Manager** menu in the control console.)
  - the **Log** option in the **Events** menu. (A Device Manager can also access the Event Log in the control console by pressing)
  - The **Logout** menu in both interfaces.
  - The **Help** menu in the Web interface and the help screens in the control console.
  - The **Links** menu in the Web interface.

  A Device Manager cannot access the **Network** menu or the **System** menu that are in the navigation panel in the Web interface and are sub-menus under the **Device Manager** menu in the control console.

  The Device Manager's default **User Name** is **device**, and the default **Password** is **apc**.
- A Read-Only user can only access menus using the Web interface and does not have permission to make changes to any menu.
  The Read-Only User's default User Name is **readonly**, and the default password is **apc**.

How to Recover from a Lost Password

You can use a local computer, a computer that connects to the Management Card or other device through the serial port, to access the control console.

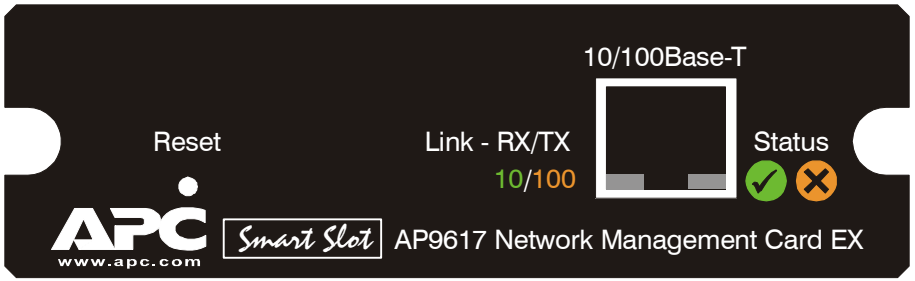
1. Select a serial port at the local computer, and disable any service that uses that port.
2. Connect the serial cable (APC part number 940-0024 or 940-1524) to the selected port on the computer and to the configuration port at the Management Card.
3. Run a terminal program (such as HyperTerminal®) and configure the selected port as follows:
   - 2400 bps
   - 8 data bits
   - no parity
   - 1 stop bit
   - no flow control
4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt. If you are unable to display the **User Name** prompt, verify the following:
   - The serial port is not in use by another application.
   - The terminal settings are correct as specified in step 3.
   - The correct cable is being used as specified in step 2.
5. Press the **Reset** button. The Status LED will flash alternately orange and green. Press the **Reset** button a second time immediately while the LED is flashing to reset the user name and password to their defaults temporarily.

6. Press ENTER as many times as necessary to redisplay the **User Name** prompt, then use the default, **apc,** for the user name and password. (If you take longer than 30 seconds to log on after the **User Name** prompt is redisplayed, you must repeat step 5 and log on again.)
7. From the **Control Console** menu, select **System**, then **User Manager**.
8. Select **Administrator**, and change the **User Name** and **Password** settings, both of which are now defined as **apc**.
9. Press CTRL-C, log off, reconnect any serial cable you disconnected, and restart any service you disabled.

Front Panel

Introduction

The front-panel features of the Network Management Card (AP9617) include Status LEDs, a Reset button, and a 10/100Base-T connector.



Features

Feature	Description
Reset button	Resets the Management Card while power remains on.
10/100 Base-T connector	Connects the Management Card to the Ethernet network.
Link-RX/TX (10/100) LED	See Link-RX/TX (10/100) LED.
Status LEDs	See Status LEDs.

Link-RX/TX (10/100) LED

This LED indicates the network status.

Condition	Description
Off	One or more of the following situations exist: • The Management Card is not receiving input power. • The cable that connects the Management Card to the network is disconnected or defective. • The device that connects the Management Card to the network is turned off or not operating correctly. • The Management Card itself is not operating properly. It may need to be repaired or replaced. Contact APC Worldwide Customer Support.
Solid **Green**	The Management Card has valid TCP/IP settings.
Solid **Orange**	A hardware failure has been detected in the Management Card. Contact APC Worldwide Customer Support.
Flashing **Green**	The Management Card is receiving or transferring data packets at 10 Megabits per second (Mbps).
Flashing **Orange**	The Management Card is receiving or transferring data packets at 100 Megabits per second (Mbps).

Status LEDs

These LEDs indicate the Management Card's status.

Condition	Description
Off	One of the following situations exists: • The Management Card is not receiving input power. • The Management Card is starting up. • The Management Card is not operating properly. It may need to be repaired or replaced. Contact APC Worldwide Customer Support.
Solid **Green**	The Management Card has valid TCP/IP settings.[1]
Flashing **Green**	The Management Card does not have valid TCP/IP settings.
Solid **Orange**	A hardware failure has been detected in the Management Card. Contact APC Worldwide Customer Support.
Flashing **Orange**	The Management Card is making BOOTP[2] requests.
Alternately flashing **Green** and **Orange**	If the LED is alternately flashing slowly, the Management Card is making DHCP requests. If the LED is alternately flashing rapidly, the Management Card is starting up.

1 If you do not use a BOOTP or DHCP server, see the Network Management Card *Installation and Quick Start Manual* provided in printed format and on the APC Automatic Transfer Switch *Utility* CD (**.\doc\en\Insguide.pdf**) to configure the Management Card's TCP/IP settings.

2 To use a DHCP server, see Boot Mode.

Watchdog Features

Overview

To detect internal problems and recover from unanticipated inputs, the Management Card uses internal, system-wide watchdog mechanisms. When it reboots itself to recover from an internal problem, a **System: Warmstart** event is recorded in the Event Log.

Network interface watchdog mechanism

The Management Card implements internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For example, if the Management Card does not receive any network traffic for 9.5 minutes (either direct traffic, such as SNMP, or broadcast traffic, such as an Address Resolution Protocol [ARP] request), it assumes that there is a problem with its network interface and reboots itself.

Resetting the network timer

To ensure that the Management Card does not reboot if the network is quiet for 9.5 minutes, the Management Card attempts to contact the Default Gateway every 4.5 minutes. If the gateway is present, it responds to the Management Card, and that response restarts the 9.5-minute timer. If your application does not require or have a gateway, specify the IP address of a computer that is running on the network most of the time and is on the same subnet. The network traffic of that computer will restart the 9.5-minute timer frequently enough to prevent the Management Card from rebooting.

Internal Interface

Introduction

Purpose

The Automatic Transfer Switch has a set of simple internal menus, which you can access locally through a serial connection, to perform basic management and configuration tasks.

Note

You can communicate with the Network Management Card through the local serial port connection. See Web Config for details.

Access the internal interface

To access the Automatic Transfer Switch internal menus, use a terminal emulation program such as HyperTerminal:

1. Select a serial port on your computer, and disable any service that uses that port.
2. Connect your computer to the Automatic Transfer Switch configuration port, using the communication cable (included).
3. Start a terminal session and configure the selected port for 19200 bps, 8 data bits, no parity, 1 stop bit, and no flow control. Save the changes.

Note Some terminal emulation programs require that a device be disconnected and then reconnected for the new serial port settings to take effect.

4. Log on to the Automatic Transfer Switch using the user name and password for the appropriate access level:

Access Level	Default User	Password
Administrator	Press ENTER.	Type **apc** (in lowercase).
User	Press ENTER.	Press ESC.

User access is as follows:

- When you log on as User, you can view information but you cannot configure settings or enter data.
- When you log on as Administrator, you can view information, configure settings, and enter data.

You can access the Network Management Card through the serial connection. See Web Config for instructions on how to configure your terminal program to connect to the card.

How to use the menus

- Enter the number corresponding to a menu selection.
- To refresh the current menu, press ENTER.
- To go to the previous menu, press ESC.
- On data entry screens an arrow (->) next to a value indicates the current selection.
- Navigation controls specific to each screen are displayed below the data or menu options, under the heading **Menu Selections.**

Internal Menus

Main menu

The main internal menu has the following options that allow you to view information, configure settings, and enter data, depending on your access level:

```
 1 - Status
 2 - Measurements
 3 - Switch Configuration
 4 - Alarms
 5 - Event Counts
 6 - Event Log
 7 - Device Data
 8 - Factory Data
 9 - Log Out
10 - System Admin (Admin Only)
11 - Web Config (Admin Only)
```

Status menu

Item	Definition
Selected Source	Source currently supplying power to the load.
Preferred Source	Power source to use when both sources are acceptable.
Switch Status	Indicates whether the alternate power source is acceptable. The load will switch to this source if the selected power source fails.
Front Panel Select	Indicates if the front panel button can be used to change sources (LOCKED or UNLOCKED).
Source A	Reports the condition of power source A (OK or FAIL).
Source B	Reports the condition of power source B (OK or FAIL).
Phase Sync	Reports if Source A and B are in phase (for 3-phase units only).The preference indicator on the front panel will flash if sources are not in phase.
24V PS	Reports the condition of the 24V power supply (OK or FAIL).
+12V PS	Reports the condition of the +12V power supply (OK or FAIL).
–12V PS	Reports the condition of the –12V power supply (OK or FAIL).
5V PS	Reports the condition of the 5V power supply (OK or FAIL).

Measurements menu

Item	Definition
Source A VRMS	Frequency and voltage of input power source A.
Source B VRMS	Frequency and voltage of input power source B.
Output Amps	Load current reading.
24 VDC PS	Voltage of the 24 VDC power supply.
+12 VDC PS	Voltage of the +12 VDC power supply.
–12 VDC PS	Voltage of the –12 VDC power supply.
5 VDC PS	Voltage of the 5 VDC power supply.

Switch configuration menu

Item	Definition
Line VRMS	Nominal source line voltage setting for this device.
Line Frequency	Nominal source frequency setting for this device.
Preferred Source	Power source that will be used when both sources are acceptable.
Sensitivity	Sensitivity of the Automatic Transfer Switch to changes in voltage. • **Low**: Causes the Automatic Transfer Switch to accept frequent, small line voltage changes without switching to the alternate power source. • **High**: Causes the Automatic Transfer Switch to switch to the alternate power source in response to small line voltage changes. Provides the best protection for sensitive equipment.
VRMS Range	Defines the range of acceptable voltage from a power source. If the voltage of the selected input source is not within this range, the Automatic Transfer Switch transfers to the alternate power source. Options are **Wide**, **Medium**, and **Narrow**.
Narrow VRMS Limit	The voltage range to use when VRMS range is set to narrow.
Medium VRMS Limit	The voltage range to use when VRMS range is set to medium.
Wide VRMS Limit	The voltage range to use when VRMS range is set to wide.
Alarm Current Threshold	The threshold, in Amps, at which an Over Current Alarm is generated.
Freq Deviation	Range of frequency fluctuation (maximum is ±3Hz).
Front Panel Select	Lock or unlock the source-switching button on the front panel of the Automatic Transfer Switch.

Alarms menu

Item	Definition
Redundancy	One or both sources have a voltage or frequency out of range.
Source Switch	The Automatic Transfer Switch is unable to switch sources.
Over Current	Power source input current is over the acceptable threshold.
Source A	Power source is out of range.
Source B	Power source is out of range.
Power Supply	The 24V, +12V, –12V, or 5V power supply is out of range.
Configuration	Configuration changes have been made.

Event Counts

The event counts screen records of the number of times each of the following events has occurred since the last time the counts were cleared.

- Redundancy loss
- Source switch
- Over current
- Source preference change
- Spike/Dropout
- Surge/Droop
- Frequency Loss
- Warm Boot
- Switch Inhibit

Event Log

The event log provides a list of the last twenty events (in the order that they occurred) since the last time the log was cleared.

See Event Counts for a listing of the possible events.

Device Data

Item	Definition
Name	Name of the contact for this device.
Location	Location of the device.
Contact Info	How to contact the person responsible for this device.
Log Time-out	Number of minutes of inactivity before you are logged off (maximum 15).
Admin Password	Change the administrator password (Administrator only).

Factory Data

The factory data screen shows the following information about the Automatic Transfer Switch:

- Model Number
- Serial Number
- Hardware Revision
- Manufacture Date
- Firmware Revision
- Date of firmware installation

System Admin

Item	Definition
Cold Start	Enable a cold start of the Automatic Transfer Switch.
Warm Start	Enable a warm start of the Automatic Transfer Switch.
Restore Defaults/ Restart	Change settings back to defaults.
Firmware Download	Update the Automatic Transfer Switch firmware.

Web Config

The **Web Config** option provides pass-through access to the Network Management Card. When you select **Web Config,** a screen will prompt you to change your terminal emulator settings to a baud rate of 2400 bps. When you are finished configuring the Network Management Card, it will also remind you to reset the Automatic Transfer Switch and change the baud rate back to 19200 .

To access Network Management Card through the serial port:

1. Disconnect your terminal program.
2. Change the baud rate to 2400 bps and reconnect the terminal program.
3. Press ENTER to display the log on prompt for the Network Management Card.

After you have finished using the menus of the Network Management Card, reset the terminal settings to return to the Automatic Transfer Switch internal menus.

4. Disconnect you terminal program.
5. Change the baud rate back to 19200 bps.
6. Press and hold the **Preference** button on the front of the Automatic Transfer Switch until all the LEDs (except the output LED) turn off (in about ten seconds).

Note The **Front Panel Select** option on the **Switch Configuration** menu must be set to **Unlocked**. Otherwise, the **Preference** button will not reset the Automatic Transfer Switch.

7. Reconnect the terminal program and log on to the internal menus.

Control Console

How To Log On

User Name and Password

Use case-sensitive **User Name** and **Password** entries (by default, **apc** and **apc**, for an Administrator, or **device** and **apc**, for a Device Manager) to log in.

If you cannot remember your **User Name** or **Password**, call APC Worldwide Customer Support for assistance.

Remote access to the control console

You can access the control console through Telnet or SSH, depending on which is enabled. (An Administrator can enable these access methods through the **Telnet/SSH** option of the **Network** menu.) By default, Telnet is enabled. Enabling SSH automatically disables Telnet.

Telnet for basic access. Telnet provides the basic security of authentication by user name and password, but not the high-security benefits of encryption. To use Telnet to access the control console from any computer on the same subnet:

1. At a command prompt, type `telnet` and the System IP address for the Network Management Card (when the Network Management Card uses the default Telnet port of 23), and press ENTER. For example, for a system with an IP address is 198.168.6.133 you would type the following:

   ```
   telnet 198.168.6.133
   ```

   Note If the Network Management Card uses a non-default port number (between 5000 and 32767), you need to include a colon or a space (depending on your Telnet client) between the IP address and the port number.

2. Enter the user name and password (by default, **apc** and **apc** for an Administrator, or **device** and **apc** for a Device Manager).

SSH for high-security access. If you use the high security of SSL for the Web interface, use SSH for access to the control console. SSH encrypts user names, passwords, and transmitted data.

The interface, user accounts, and user access rights are the same whether you access the control console through SSH or Telnet, but to use SSH, you must first configure SSH and have an SSH client program installed on your computer.

Main Screen

Example main screen

The following is an example of the screen that appears when you log on to the control console at a Network Management Card (AP917).

```
User Name: apc
Password : ***

American Power Conversion                Network Management Card AOS      v2.6.4
<c> Copyright 2001 All Rights Reserved  Automatic Transfer Switch APP      v2.6.1
-------------------------------------------------------------------------------
Name       : Switch_1                                  Date: 08/01/2004
Contact    : Tom_Adams                                 Time: 05:49:30
Location   : TestLab                                   User: Administrator
Up Time    : 1 Day 4 Hours 5 Minutes                   Stat: P+ N+ A+

Automatic Transfer Switch : Source A selected Switchover possible

-------- Control Console -------------------------------------------------------

      1- Device Manager
      2- Network
      3- System
      4- Logout

      <ESC>- Main Menu, <ENTER>- Refresh, <CTRL-L>- Event Log
>
```

Information and status fields

Main screen information fields. The main screen provides the following information:

- Two fields identifying the APC operating system (AOS) and application (APP) firmware versions. The application firmware uses a name that identifies the type of device that the Network Management Card connects to the network. In the Example main screen, the Network Management Card uses the application firmware for the Automatic Transfer Switch.

  ```
  Network Management Card AOS      v2.6.4
  Automatic Transfer Switch APP    v2.6.1
  ```

  Three fields identify the system **Name**, **Contact**, and **Location** values.

  ```
  Name      : Switch_1
  Contact   : Tom_Adams
  Location  : TestLab
  ```

To set the **Name**, **Contact**, and **Location** values, see System Menu.

- An **Up Time** field reports how long the Network Management Card has been running since it was last turned on or reset.

  ```
  Up Time   : 1 Day 4 Hours 5 Minutes
  ```

- Two fields identify when you logged on, by **Date** and **Time**.

  ```
  Date : 08/01/2004
  Time : 05:49:30
  ```

- A **User** field identifies whether you logged on as an **Administrator** or **Device Manager**.

  ```
  User : Administrator
  ```

Main screen status fields. The main screen reports status in the following fields:

- A **Stat** field that reports the Network Management Card status.

```
Stat : P+ N+ A+
```

P+	The APC operating system (AOS) is functioning properly.
N+	The network is functioning properly.
N?	A BOOTP request cycle is in progress.
N–	The Network Management Card failed to connect to the network.
N !	Another device is using the Network Management Card's IP address.
A+	The application is functioning properly.
A–	The application has a bad checksum.
A?	The application is initializing.
A !	The application is not compatible with the AOS.

Note If the AOS status is not P+, contact APC Worldwide Customer Support, even if you can still access the Network Management Card.

- An **Automatic Transfer Switch** field:
  - **Source A selected** or **Source B selected** indicates which source is currently supplying power to the load.
  - **Switchover Possible** or **Switchover Not Possible** indicates whether the load can be switched to the alternate source. The load can be switched only if the line voltage and frequency of the alternative source are in an acceptable range.

Control Console Menus

Main menu

The main **Control Console** menu has options that provide access to the control console's management features:

```
1- Device Manager
2- Network
3- System
4- Logout
```

Note

When you log on as Device Manager, you can access only the **Device Manager** menus and the **Logout** menu.

How to use the menus

Within the menu structure:

- To select a menu item, type the item number, and press ENTER.
- To save changes to configurable values, use the **Accept Changes** menu option.
- To refresh the current menu, press ENTER.
- To go to the previous menu, press ESC.
- To access brief descriptions of the current menu options if the menu has help available, type ? and then press ENTER.
- To return to the main Control Console menu, use CTRL + C.
- To access the event log, use CTRL + L.

For information about the event log, see Event-Related Menus and Options.

Device Manager menu

Use the **Device Manager** menu to select the device that you want to manage.

```
1- Automatic Transfer Switch
```

For information about the menu options to manage the Automatic Transfer Switch, see Automatic Transfer Switch Menu.

Network option

Use the **Network** menu to perform any of the following functions:

- Configure the Network Management Card's TCP/IP settings or when the Network Management Card will obtain its TCP/IP settings from a server, configure the settings for the type of server (BOOTP or DHCP) to be used.
- Define DNS Server IP addresses
- Use the Ping utility
- Define settings that affect FTP file transfers
- Configure Telnet/SSH settings
- Configure Web/SSL settings
- Define SNMP settings
- Configure e-mail settings

Note DNS settings must be defined for e-mail features to work properly.

Use the System Menu to perform the following tasks:

- Control **Administrator** and **Device Manager** access.
- Define the system **Name**, **Contact**, and **Location** values.
- Set the **Date** and **Time** used by the Network Management Card
- Through the **Tools** menu:
  - Restate the Network Management Card interface.
  - Reset parameters to their default values.
  - Delete SSH host keys and SSL certificates.
- Reset control console settings to their default values.
- Access system information about the Network Management Card.

Web Interface

Introduction

Overview

The Web interface provides options that you use to manage the Automatic Transfer Switch.

See Web/SSL for information on the menu options you use to select, enable, and disable the protocols that control access to the Web interface and to define the Web-server ports for the protocols.

Supported Web browsers

As your browser, you can use Microsoft® Internet Explorer (IE) 5.0 (and higher) or Netscape® 6.*x* (and higher) to access the Network Management Card through its Web interface. Other commonly available browsers may also work but have not been fully tested by APC.

Data verification, the Event Log, and the Data Log require that you enable the following for your Web browser:

- JavaScript
- Java
- Cookies

In addition, the Network Management Card cannot work with a proxy server. Therefore, before you can use a Web browser to access its Web interface, you must do one of the following:

- Configure the Web browser to disable the use of a proxy server for the Network Management Card.
- Configure the proxy server so that it does not proxy the specific IP address of the Network Management Card.

How to Log On

Overview

You can use the DNS name or System IP address of the Network Management Card for the URL address of the Web interface. Use your case-sensitive **User Name** and **Password** settings to log on. The default user name differs by account type:

- **apc** for an Administrator
- **device** for a Device Manager
- **readonly** for a Read-Only User

The default password is **apc** for all three account types.

Note If you are using HTTPS (SSL/TSL) as your access protocol, your login credentials are compared with information in a server certificate. If the certificate was created with the APC Security Wizard, you must use an IP address to log on to the Network Management Card if an IP address was specified as the common name in the certificate, or you must use a DNS name to log on if a DNS name was specified as the common name in the certificate.

For information about the Web page that appears when you log on to the Web interface, see Summary Page.

URL address formats

Type the DNS name or IP address of the Network Management Card in the Web browser's URL address field and press ENTER. Except as noted below, `http://` is automatically added by the browser.

Note If the error "You are not authorized to view this page" occurs (Internet Explorer only), someone is logged onto the Web interface or control console. If the error "No Response" (Netscape) or "This page cannot be displayed" (Internet Explorer) occurs, Web access may be disabled, or the Network Management Card may use a non-default Web-server port that you did not specify correctly in the address. (For Internet Explorer, you must type `http://` or `https://`as part of the address when any port other than 80 is used.)

- For a DNS name of Web1, the entry would be one of the following:
  - `http://Web1` if HTTP is your access mode
  - `https://Web1` if HTTPS (SSL) is your access mode
- For a System IP address of 198.168.6.133, when the Network Management Card uses the default port (80) at the Web server, the entry would be one of the following:
  - `http://198.168.6.133` if HTTP is your access mode
  - `https://198.168.6.133` if HTTPS (SSL) is your access mode

For a System IP address of 198.168.6.133, when the Network Management Card uses a non-default port (5000, in this example) as the Web server, the entry would be one of the following:

- `http://198.168.6.133:5000` if HTTP is your access mode
- `https://198.168.6.133:5000` if HTTPS (SSL is your access mode)

Summary Page

Example Web page

The following is an example of the navigation menu (see Navigation Menu) and Summary page that appear when you log onto the Web interface at a Network Management Card.

Summary page fields

The Summary page has two sections:

- The **Automatic Transfer Switch** section reports the status of a connected Automatic Transfer Switch.
  - **Source A selected** or **Source B selected** indicates which source is currently supplying power to the load.
  - **Switchover Possible** or **Switchover Not Possible** indicates whether the load can be switched to the alternate source. The load can be switched only if the line voltage and frequency of the alternative source are in an acceptable range.

Note This top section of the page also displays the names for **Source A** and **Source B**, which are configurable. See Configuration option.

- The **Management Card Status** section reports the following information:
  - The **Name**, **Contact**, and **Location** information for the Network Management Card
  - The login date and time
  - Type of user (**Administrator**, **Device Manager,** or **Read-Only**)
  - How long (**Up Time**) the Network Management Card has been continuously running since it was turned on or reset
  - The status of the Network Management Card

Help icon on quick status tab

Click on the question mark (**?**) in the quick status tab in the upper-right corner of any Web interface page to access the online help for that page.

Navigation Menu

Overview

When you log on to the Web interface, the navigation menu (left frame) includes the following elements:

- The Network Management Card's IP address
- **Automatic Transfer Switch** menus to manage the Automatic Transfer Switch and its components
  - **Status** menu that displays detailed status.
  - **Control** menu that lets you reset the Automatic Transfer Switch microprocessor
  - **Configuration** menu that you use to set the Automatic Transfer Switch settings and name
- **Events** menu
- **Network** menu
- **System** menu
- **Logout** option

Note When you log on as a Device Manager or Read-Only User, the **Network** and **System** menus do not appear in the navigation menu options to make any changes are not available for the Read-Only user.

- **Help** menu
- **Links** menu

Automatic Transfer Switch menu

To manage an Automatic Transfer Switch, see Automatic Transfer Switch Menu.

Selecting a menu to perform a task

- To do the following, see Event-Related Menus and Options:
  - Access the Event Log
  - Configure the actions to be taken based on an event's severity level
  - Configure SNMP Trap Receiver settings for sending event-based traps
  - Reset all event configurations to defaults
  - Define who will receive e-mail notifications of events
- To do the following, see Data Menu:
  - Access Data Log
  - Delete Data Log
  - Configure the interval at which data is logged
- To do the following, see Network Menu:
  - Configure new TCP/IP settings for the Network Management Card
  - Identify the Domain Name Service (DNS) Server and test the network connection to that server
  - Define settings for FTP, Telnet, and SSH
  - Define SNMP access control
  - Configure e-mail settings
  - Configure and test Syslog applications
  - Configure Web/SSL and view SSLcertificates

- To do the following, see System Menu.
  - Control **Administrator**, **Device Manager,** and **Read-Only** access
  - Define system settings for RADIUS
  - Define the system **Name**, **Contact**, and **Location** values
  - Set the **Date** and **Time** used by the Network Management Card
  - To do the following, see **Tools** Menu:
    - Restart the Network Management Card
    - Reset parameters to their default values
    - Delete SSH host keys and SSL certificates
    - Upload an initialization file (.ini file) that has been downloaded from another Network Management Card. The current Network Management Card then uses the values in that .ini file to configure its own settings
  - Reset control console settings to default settings
  - Select **Fahrenheit** or **Celsius** for temperature displays
  - Define the URL addresses used by the Web interface's user and APC logo links, as described in Links menu

Help menu

When you click **Help**, the **Contents** for the online help is automatically displayed to provide for navigation to a specific online help topic. However, from any of the Web interface pages, you can use the question mark (**?**) that appears in the quick status bar to link to the section of the online help that covers that page's content.

The **Help** menu also has an **About System** option you use to view information about the Network Management Card's **Model Number**, **Serial Number**, **Hardware Revision**, **Manufacture Date**, **MAC Address, Application Module** and **APC OS (AOS) Module**, including the date and time these modules were loaded.

Note In the control console, the **About System** option, which is a **System** menu option, identifies the **Flash Type** used.

Links menu

Provides three user-definable URL link options. By default, these links access the following APC Web pages:

- **APC's Web Site** accesses the APC home page.
- **Testdrive Demo** accesses a demonstration page where you can use samples of APC web-enabled products.
- **APC Monitoring** accesses the "APC Remote Monitoring Service" page where you can find more information about pay-for-monitoring services available from APC.

You can use the following procedure to redefine these links so that they point to other URL addresses.

1. Click on **Links** in the **System** menu.
2. Define any new names for the **User Links**.
3. Define any new URL addresses that you want the **User Links** to access.
4. Click **Apply**.

Automatic Transfer Switch Menu

Options and Settings

Purpose

Use the **Automatic Transfer Switch** menu to review status, control, and configuration settings for the Automatic Transfer Switch.

Status option

Brief Status.

For information on the summary status fields that are displayed when you log on:

- For the Web interface, see Summary Page.
- For the control console, see Main Screen.

Detailed status. To display detailed status:

- In the Web interface, select the **Status** option of the **Automatic Transfer Switch** menu.
- In the control console, select, in order, **Device Manager**, **Automatic Transfer Switch**, and **Detailed Status**.

Item	Definition
Status	The state of each power source: • **Selected**: This source is currently providing power. • **OK**: The alternate power source is acceptable The load will switch to this source if the selected power source fails. • **Not OK**: The alternate power source is not acceptable. The load cannot switch to the alternate power source if the selected source fails. • **Inhibited**: Although the alternate power source is acceptable, the load cannot switch to that power source because of an Over Current Condition (short-circuit).
Input Frequency	The input line frequency for each source in Hz. The control console reports this information as part of the **Input Voltage** field.
Input Voltage	The line voltage for each source. For three-phase models, the line voltage of each phase of each source within ± 4 percent per phase.
Output Current	The output current of the Automatic Transfer Switch. For three-phase models, the output current for each phase and for neutral, in amps. Neutral current is the current returning to the source after flowing through the load.
Source A Source B	The configurable names of the two power sources. See Configuration option. (In the Web interface, these names are displayed on the opening **Summary** page.)

About Automatic Transfer Switch. To obtain the model number, firmware revision, firmware date (in the Web interface only), hardware revision, manufacture date, and serial number of the Automatic Transfer Switch:

- Select the **Status** option of the **Automatic Transfer Switch** menu in the Web interface.
- Select **Device Manager**, **Automatic Transfer Switch**, and **About Automatic Transfer Switch** in the control console.

Control option

Item	Definition
Action	Choose **Reset ATS MicroProcessor** and click **Apply** to configure the Automatic Transfer Switch to reset itself when power to the unit is turned on manually or automatically. **NOTE:** The Network Management Card loses communication briefly while the Automatic Transfer Switch resets itself.

Configuration option

Item	Definition
Source A Name Source B Name	The user-defined name for each source, 32-characters maximum.
Preferred Source	The power source to which the Automatic Transfer Switch will transfer when both input power sources are acceptable. Options are **Source A**, **Source B**, and **None**.
Voltage Transfer Range	Defines the range of acceptable voltage from a power source. If the voltage of the selected input source is not within this range, the Automatic Transfer Switch transfers to the alternate power source. Options are **Wide**, **Medium**, and **Narrow**.
Sensitivity	Defines the sensitivity of the Automatic Transfer Switch to changes in voltage. • **Low**: Causes the Automatic Transfer Switch to accept frequent small line voltage changes without switching to the alternate power source. • **High**: Causes the Automatic Transfer Switch to switch to the alternate power source in response to small line voltage changes. Provides the best protection for sensitive equipment.
Current Limit	The threshold, in amps, at which an Over Current Alarm is generated.
Reset to Default Settings	Reset the Automatic Transfer Switch to its default values. **NOTE:** The Network Management Card loses communication briefly while the Automatic Transfer Switch resets itself.

Event-Related Menus and Options

Introduction

Overview

The **Events** menu provides access to the options that you use to do the following tasks:

- Access the Event Log.
- Define the actions to be taken when an event occurs, based on the severity level of that event. (You must use the Web interface to define which events will use which actions.)
  - Event logging
  - Syslog messages
  - SNMP trap notification
  - E-mail notification

Note You can use only the Web interface to define which events will use which actions, as described in Event Log and How to Configure Individual Events.

- Define up to four SNMP trap receivers, by NMS-specific IP addresses, for event notifications by SNMP traps.
- Define up to four recipients for event notifications by e-mail.

Menu options

All event-related options are accessed through the **Events** menu, except as follows:

- In the Web interface and Control Console, use the **Email** option in the **Network** menu to define the SMTP server.
- In the Control Console:
  - Use the **Email** option in the **Network** menu to define e-mail recipients.
  - Use the **SNMP** option in the **Network** menu to define the SNMP trap receivers.
  - Use CTRL + L to access the Event Log from any menu.

For information about the settings available for the **Events** menu options, and for a detailed description of the e-mail feature, see the following descriptions:

- Event Log
- Event Actions (Web Interface Only)
- Event Recipients
- E-mail Feature
- How to Configure Individual Events

Event Log

Overview

The Network Management Card supports an event-logging capability for all Automatic Transfer Switch application firmware modules. This allows you to record and view Automatic Transfer Switch and Network Management Card events. You can use any of the following to view the Event Log:

- Web interface/SSL
- Telnet/SSH
- FTP/SCP

Logged events

By default, the following events are logged:

- Any event that causes an SNMP trap, except for SNMP authentication failures.
- The Network Management Card's abnormal internal system events.

To disable the logging of events based on their assigned severity level, use the **Actions** option in the Web interface's **Events** menu.

See Event Actions (Web Interface Only).

Even if you disable the Event Log for all severity levels, some system (Network Management Card) events will still be logged because some of those events have no severity level.

To access a list of the system (Network Management Card) and Automatic Transfer Switch events, see "Event List" page.

Web interface

The **Log** option in the **Events** menu accesses the Event Log. This log displays, in reverse chronological order, all of the events that have been recorded since the log was last deleted. The **Delete Log** button clears all events from the log.

Control console

When logged on at the control console, press CTRL-L to displays, in reverse chronological order, all of the events, that have been recorded since the log was last deleted. Use the SPACE BAR to scroll through the recorded events. While viewing the log, type d and press ENTER to clear all events from the log.

Note Deleted events cannot be retrieved.

How to use FTP or SCP to retrieve log files

If you are an Administrator or Device Manager, you can use FTP or SCP to retrieve a tab-delineated event log file (*event.txt*) or data log file (*data.txt*) that you can import into a spreadsheet application.

- The file reports all of the events or data recorded since the log was last deleted.
- The file includes information that the event log or data log does not display.
  - The version of the file format (first field)
  - The date and time the file was retrieved
  - The **Name**, **Contact**, and **Location** values and IP address of the Network Management Card
  - The unique **Event Code** for each recorded event (*event.txt* file only)

Note The Network Management Card uses a four-digit year for log entries. You may need to select a four-digit date format in your spreadsheet application to display all four digits of the year.

If you are using the encryption-based security protocols for your system, use Secure CoPy (SCP) to retrieve the log file. (You should have FTP disabled.)

If you are using unencrypted authentication methods for the security of your system, use FTP to retrieve the log file.

See Security for information on the available protocols and methods for setting up the type of security appropriate for your needs.

To use SCP to retrieve the files. To use SCP to retrieve the *event.txt* file, use the following command:

```
scp username@hostname_or_ip_address:event.txt ./event.txt
```

To use SCP to retrieve the *data.txt* file, use the following command:

```
scp username@hostname_or_ip_address:data.txt ./data.txt
```

To use FTP to retrieve the files. To use FTP to retrieve the *event.txt* or *data.txt* file:

1. At a command prompt, type `ftp` and the Network Management Card's IP address, and press ENTER.

   If the **Port** setting for **FTP Server** in the **Network** menu has changed from its default value (**21**), you must use the non-default value in the FTP command. For Windows FTP clients, use the following command, including spaces. (For some FTP clients, you must use a colon instead of a space between the IP address and the port number.)

   ```
   ftp>open ip_address port_number
   ```

2. Use the case-sensitive **User Name** and **Password** for either an Administrator or a Device Manager user to log on.

   To use non-default port values to enhance security, see Port assignments.

   – For Administrator, **apc** is the default for **User Name** and **Password**.
   – For Device Manager, **device** is the default for **User Name**, and **apc** is the default for **Password**.

3. Use the **get** command to transmit the text-version of the event log or data log to your local drive.

   ```
   ftp>get event.txt
   ```

   or

   ```
   ftp>get data.txt
   ```

4. You can use the **del** command to clear the contents of the event log or data log.

   `ftp>del event.txt`

   or

   `ftp>del data.txt`

   You will not be asked to confirm the deletion.
   - If you clear the data log, the event log records a deleted-log event.
   - If you clear the event log, a new *event.txt* file is created to record the deleted-log event.
5. Type `quit` at the `ftp>` prompt to exit from FTP.

Event Actions (Web Interface Only)

Overview

Use the **Actions** option in the **Events** menu to do the following:

- Select which actions will occur for events that have a severity level.
  - **Event Log** selects which severity levels cause an event to be logged.

    See Event Log action.

  - **Syslog** selects which severity levels cause messages to be sent to Syslog servers to log events.
    - Syslog selects which severity levels cause messages to be sent to Syslog servers to log events.

    See Syslog action.

  - **SNMP Traps** selects which severity levels generate SNMP traps, and which trap receivers are notified for events of each severity level.

    See SNMP Traps action.

  - **Email** selects which severity levels cause e-mail notifications and which e-mail recipients receive e-mail for events of each severity level.

    See Email action.

  - **Paging** selects which severity levels initiate paging and which paging recipients are paged for events of each severity level.

- Click **Details** for a complete list of the Network Management Card (system), UPS, and Automatic Transfer Switch events that can occur, and then edit the actions that will occur for an individual event. Click **Hide Details** to return to the **Actions** option.

See How to Configure Individual Events.

Severity levels

Except for some system (Network Management Card) events that do not have a severity level assigned, events are assigned a default severity level.

- **Informational**: Indicates an event that requires no action, such as a notification of a return from an abnormal condition.
- **Warning**: Indicates an event that may need to be addressed should the condition continue, but does not require immediate attention.
- **Severe**: Indicates an event that requires immediate attention. Unless resolved, severe Automatic Transfer Switch and system events can cause incorrect operation of the Automatic Transfer Switch or its Network Management Card.

Event Log action

You can disable the recording of events in the Event Log. By default, all events are recorded, even events that have no severity level assigned.

Note Even if you disable the Event Log action for all severity levels, system (Network Management Card) events which have no severity level assigned will still be logged.

For more information about this log, see Event Log.

Syslog action

By default, the Syslog action is enabled for all events that have a severity level. However, before you can use this feature to send Syslog messages when events occur, you must configure it.

See Syslog.

SNMP Traps action

By default, the **SNMP Traps** action is enabled for all events that have a severity level assigned. However, before you can use SNMP traps for event notifications, you must identify the NMSs (by their IP addresses) that will receive the traps.

To define up to four NMSs as trap receivers, see Event Recipients.

Email action

By default, the **Email** action is enabled for all events that have a severity level assigned. However, before you can use e-mail for event notifications, you must define the e-mail recipients.

To define the e-mail recipients, see E-mail Feature.

Event Recipients

Overview

The Web interface and control console both have options that allow you to define up to four trap receivers and up to four e-mail addresses to be used when an event occurs that has the SNMP traps or e-mail enabled.

Trap Receiver settings

To define the **Trap Receiver** settings that allow you to define which NMSs receive traps:

- In the Web interface, use the **Recipients** option in the **Events** menu.
- In the control console, use the **SNMP** option in the **Network** menu.

Item	Definition
Community Name	The password (maximum of 15 characters) used when traps are sent to the NMS identified by the **Receiver NMS IP/Domain Name** setting.
Receiver NMS IP/Domain Name	The IP address or domain name of the NMS that will receive traps. **0.0.0.0** (the default value) causes traps not to be sent to any NMS.
Generation (Web Interface) Trap Generation (control console)	Enables (by default) or disables the sending of any traps to the NMS identified by the **Receiver NMS IP/Domain Name** setting.
Authentication Traps	Enables or disables the sending of authentication traps to the NMS identified by the **Receiver NMS IP/Domain Name** setting.

E-mail Feature

Overview

You can use the Simple Mail Transfer Protocol (SMTP) to send e-mail to a maximum of four recipients when an event occurs.

To use the e-mail feature, you must define the following settings:

- The IP addresses of the primary and secondary Domain Name Service (DNS) servers.

See DNS servers.

- The DNS name of the **SMTP Server** and the **From Address** settings for SMTP.

See SMTP settings.

- The e-mail addresses for a maximum of four recipients.

See Email Recipients.

Note You can use the **To Address** setting of the **Email Recipients** option to send e-mail to a text-based pager.

DNS servers

The Network Management Card cannot send any e-mail unless the IP address of the primary DNS server is defined.

See DNS.

The Network Management Card will wait a maximum of 15 seconds for a response from the primary or (if specified) the secondary DNS servers. If the Network Management Card does not receive a response within that time, e-mail cannot be sent. Therefore, use DNS servers that are on the same segment as the Network Management Card or on a nearby segment (but not across a wide-area network (WAN)).

Once you define the IP addresses of the DNS servers, verify that DNS is working correctly by entering the DNS name of a computer on your network to test whether you can look up the IP address for that computer.

SMTP settings

Use the **E-mail** option in the **Network** menu to define the following settings:

Setting	Description
SMTP Server	The IP address (or if DNS is configured, the DNS name) of the SMTP server. **NOTE:** This definition is required only when the **SMTP Server** option is set to **Local**. See Email Recipients.
From Address	The contents of the **From** field in the format *user@domain*.com (if an IP address is specified as **SMTP Server**) or *user@* [*IP_address*] (if DNS is configured and the DNS name is specified as **SMTP Server**) in the e-mail messages sent by the Network Management Card. **NOTE:** The SMTP server's configuration may require that you use a valid user account on the server for this setting. See the server's documentation for more information.

Email Recipients

Web interface. In the Web interface, the **Recipients** option in the **Events** menu or the **Configure the Email recipients** link in the **Email Configuration** page to identify up to four e-mail recipients.

Use the **Email Test** option to send a test message to a configured recipient.

Control console. In the control console, use the **Email** option in the **Network** menu, to identify up to four e-mail recipients.

Options (both interfaces).

Setting	Description
To Address	Defines the user and domain names of the recipient. To use e-mail for paging, use the e-mail address for that recipient's pager gateway account (for example, `myacct100@skytel.com`). The pager gateway will generate the page. You can bypass the DNS lookup of the mail server's IP address by using the IP address in brackets instead of the e-mail domain name. For example, use jsmith@[xxx.xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly. **NOTE:** The recipient's pager must be able to use text-based messaging.
Use SMTP Server	Selects one of the following methods for routing e-mail: • Through the Network Management Card's SMTP server (the recommended option, **Local**). This option ensures that the e-mail is sent before the Network Management Card's 20-second time-out, and, if necessary, is retried several times. Also do one of the following: – Enable forwarding at the Network Management Card's SMTP server so that it can route e-mail to external SMTP servers. Typically, SMTP servers are not configured to forward e-mail. Always check with the administrator of your SMTP server before changing its configuration to allow forwarding. – Set up a special e-mail account for the Network Management Card to forward e-mail to an external mail account. • Directly to the recipient's SMTP server (the **Recipient's** option). On a busy remote SMTP server, the time-out may prevent some e-mail from being sent, and with this option the Network Management Card tries to send the e-mail only once. When the recipient uses the Network Management Card's SMTP server, this setting has no effect.
Generation	Enables (by default) or disables sending e-mail to the recipient.

Setting	Description
Format	Selects the format used for e-mail messages: **Short**: Identifies only the event that occurred. For example: UPS: Communications Established **Long**: Includes information about the Network Management Card and the Automatic Transfer Switch, as well as the event. For example: Name : Switch_1 Location : TestLab Contact : Tom_Adams http://135.124.222 Serial # : JA0202006110 Date: 11/25/2004 Time: 16:09:48 Code: 0x0C01 Informational - Automatic Transfer Switch: ATS has switched to source A.

How to Configure Individual Events

"Event List" page

The **Actions** option in the **Events** menu opens the **Event Action Configuration** page. Use the **Details** button to access a complete list of configurable events of the System (Network Management Card) and Automatic Transfer Switch events that can be reported by your Network Management Card.

On the Event List page, an asterisk at the beginning of an event description indicates that the event has been configured individually and is no longer set to its default configuration. A message at the bottom of the page indicates how many events have been configured.

Each event is identified by its unique code, its description, and its assigned severity level, as shown in the following examples.

For information about severity levels and how they define the actions associated with events, see Event Actions (Web Interface Only).

Code	Description	Severity
0x0008	System: Password changed.	Informational
0x0C07	Automatic Transfer Switch: Output current has exceeded threshold.	Severe

Detailed Event Action Configuration page

The event codes provide a link to a page that allows you to do the following:

- Change the selected event's severity level
- Enable or disable whether the event uses the event log, Syslog messages, SNMP traps, or e-mail recipients
- Reset the event to its default configuration

Data Menu (Web Interface Only)

Log Option

Use this option to access a log that stores readings taken by the temperature and humidity probes at regular intervals.

The information in the data log is sampled and stored based on the log interval defined by the **Data** menu's **Configuration** option. Each entry is listed by the date and time the data was recorded, and provides the data in a column format.

See Configuration Option.

To retrieve the Data Log as a text file, see How to use FTP or SCP to retrieve log files.

See also

For descriptions of the recorded data that is specific to the Automatic Transfer Switch, see the online help for your Web interface (available from the data log page by clicking on the question mark (**?**) icon).

Configuration Option

Use this option to access the Data Log Configuration page, which reports how much data can be stored in the data log. You change the **Log Interval** setting, which defines how often data will be sampled and recorded in the data log. The report updates based on the new setting.

The minimum interval is one minute. The maximum interval is 18 hours, 12 minutes, and 15 seconds.

Network Menu

Introduction

Overview

Use the **Network** menu to do the following tasks:

- Define TCP/IP settings, including BOOTP server settings, when a BOOTP server is used to provide the needed TCP/IP values.
- Use the Ping utility.
- Define settings that affect the FTP, Telnet, SSH, Web interface, SSL, TLS, SNMP, e-mail, DNS, and Syslog features of the Automatic Transfer Switch.

Note Only an Administrator has access to the **Network** menu.

Menu options

Unless noted, the following menu options are available in the control console and Web interface:

- TCP/IP
- DNS
- Ping utility (control console)
- FTP server
- Telnet/SSH
- SNMP
- Email
- Syslog
- Web/SSL

Option Settings

TCP/IP

This option accesses the following settings:

- A Boot mode setting selects the method used to define the three TCP/IP values that the Automatic Transfer Switch needs to operate on the network:
  - **System IP**: The IP address of the Automatic Transfer Switch
  - **Subnet Mask**: The subnet mask value
  - **Default Gateway**: The IP address of the default gateway

For information about the watchdog role the default gateway plays, see Resetting the network timer.

See also

For information about how to configure the initial TCP/IP settings when you install the Automatic Transfer Switch, see the Automatic Transfer Switch *Installation and Quick Start Manual* (**.\doc\en\insguide.pdf**), provided on the APC Automatic Transfer Switch *Utility* CD and in printed form.

- Advanced settings define the Automatic Transfer Switch's host and domain names, as well as TCP/IP port, BOOTP, and DHCP settings used by the Automatic Transfer Switch.

Current TCP/IP settings fields. The current **System IP**, **Subnet Mask**, and **Default Gateway** values, along with the Automatic Transfer Switch's **MAC Address**, **Host Name**, **Domain Name**, and **Ethernet Port Speed** values are displayed above the TCP/IP settings in the control console and the Web interface.

Boot mode setting. This setting selects which method will be used to define the Automatic Transfer Switch's TCP/IP settings whenever the Automatic Transfer Switch starts, resets, or reboots:

- **Manual**: Three settings (**System IP**, **Subnet Mask**, and **Default Gateway**) are available only when **Manual** is used to define the needed TCP/IP settings.
- **BOOTP only**: A BOOTP server provides the TCP/IP settings.
- **DHCP only**: A DHCP server provides the TCP/IP settings.
- **DHCP & BOOTP**: The Automatic Transfer Switch will attempt to get its TCP/IP settings from a BOOTP server first, and then, if it cannot discover a BOOTP server, from a DHCP server.

Note

An **After IP Assignment** setting will, by default, switch **Boot mode** from its default **DHCP & BOOTP** setting to **BOOTP only** or **DHCP only**, depending on the type of server that supplied the TCP/IP settings to the Automatic Transfer Switch.

For information about the **After IP Assignment** setting, and other settings that affect how the Automatic Transfer Switch uses BOOTP and DHCP, see Advanced settings; For more information about how to use DHCP, see Boot Mode.

Advanced settings. The boot mode affects which settings are available.

- Two settings are available for all **Boot mode** selections to define the Automatic Transfer Switch's **Host Name** and **Domain Name** values.
  - **Host Name:** When an Administrator configures a host name here and a domain name in the **Domain Name** field, users can then enter a host name in any field in the Automatic Transfer Switch interface (except e-mail addresses) that accepts a domain name as input
  - **Domain Name**: An Administrator needs to configures the domain name here only. In all other fields in the Automatic Transfer Switch interface (except e-mail addresses) that accept domain names, the Automatic Transfer Switch will add this domain name when only a host name is entered.

Note

To override the expansion of a specified host name by the addition of the domain name, do one of the following:

- To override the behavior in all instances, set the domain name field in **Configure General Settings** to its default `somedomain.com` or to `0.0.0.0`.
- To override the behavior for a particular host name entry — for example when defining a trap receiver — include a trailing period. The Automatic Transfer Switch recognizes a host name with a trailing period (such as *mySnmpServer.*) as if it were a fully qualified domain name and therefore does not append the domain name.

- A **Port Speed** setting is available for all **Boot mode** selections to define the TCP/IP port's communication speed (**Auto-negotiate**, by default).

- Three settings are available for all **Boot mode** selections, except **Manual**, to identify the Automatic Transfer Switch in BOOTP or DHCP communication:
  - **Vendor Class**: Uses **APC**, by default.
  - **Client ID**: Uses the Automatic Transfer Switch's MAC address, by default.

    Caution If **Client ID** is changed from the Automatic Transfer Switch's MAC address, the new value must be unique on the LAN. Otherwise, the DHCP or BOOTP server may act incorrectly.
  - **User Class**: Uses the Automatic Transfer Switch's application module type, by default. For example, the Automatic Transfer Switch module sets the **User Class** to **ATS**.
- Two settings are available when **BOOTP only** is the Boot mode selection:
  - **Retry Then Fail**: Defines how many times the Automatic Transfer Switch will attempt to discover a BOOTP server before it stops (**4**, by default).
  - **On Retry Failure**: Defines what TCP/IP settings will be used by the Automatic Transfer Switch when it fails to discover a BOOTP server (**Use Prior Settings**, by default).

For information about the **Advanced** settings (**DHCP Cookie Is** and **Retry Then Stop**) that directly affect how DHCP is used, see Boot Mode.

DNS

Use this option to define the IP addresses of the primary and secondary DNS used by the Automatic Transfer Switch e-mail feature.)

See E-mail Feature and DNS servers.

Send DNS query (Web interface. Use this option, available only through the **DNS** menu in the Web interface, to send a DNS query that tests the setup of your DNS servers.

Use the following settings to define the parameters for the test DNS request; you view the result of the test DNS request in the **Last Query Response** field (which displays **No last query** or text describing the query result of the last test).

- Use the **Query Type** setting to select the method to use for the DNS query:
  - The URL name of the server (**Host**)
  - The IP address of the server (**IP**)
  - The fully qualified domain name (**FQDN**)
  - The Mail Exchange used by the server (**MX**)

- Use the **Query Question** text field to identify the value to be used for the selected **Query Type**:
  - For **Host**, identify the URL
  - For **IP**, identify the IP address
  - For **FQDN**, identify the fully qualified domain name, formatted as `myserver.mydomain.com`
  - For **MX**, identify the Mail Exchange address
- Enable or disable **Reverse DNS Lookup**, which is disabled by default. Enable this feature unless you do not have a DNS server configured or have poor network performance because of heavy network traffic. With **Reverse DNS Lookup** enabled, when a network-related event occurs, reverse DNS lookup logs in the event log both the IP address and the domain name for the networked device associated with the event. If the device does not have a domain name entry, only its IP address is logged with the event. Since domain names generally change much less frequently than IP addresses, enabling reverse DNS lookup can improve the ability to identify addresses of networked devices that are causing events to occur.

Ping utility (control console)

Select this option, available only in the control console, to check the network connection by testing whether a defined IP address or domain name responds to the Ping network utility.

By default, the IP address of the default gateway is used. However, you can use the IP address or domain name of any device known to be running on the network.

FTP server

Use the **Access** setting to enable or disable the FTP server. The server is enabled by default.

Note

FTP transfers files without using encryption. For higher security, use SCP for file transfers. When you select and configure SSH, SCP is enabled automatically.

See Telnet/SSH to configure SSH. If you decide to use SCP for file transfer, be sure to disable the FTP server

Use the **Port** setting to identify the TCP/IP port that the FTP server uses for communications with the Automatic Transfer Switch. The default **Port** setting is **21**.

You can change the **Port** setting to any unused port from **5000** to **32768** to enhance the protection provided by **User Name** and **Password** settings. You must then use a colon (:) in the command line to specify the non-default port. For example, for a port number of 5000 and the Automatic Transfer Switch IP address of 152.166.12.113, you would use this command:

```
ftp 152.166.12.113:5000
```

To access a text version of the Automatic Transfer Switch's event or data log, see How to use FTP or SCP to retrieve log files.

To use FTP to download configuration files:

- See File Transfer (control console only) if the files are on an FTP server of your company or agency.
- See Firmware file transfer methods if you are downloading files from the APC Web site.

Telnet/SSH

Use the **Telnet/SSH** option to perform the following tasks:

- Enable or disable Telnet or the Secure SHell (SSH) protocol for remote control console access.
  - While SSH is enabled, you cannot use Telnet to access the control console.
  - Enabling SSH enables SCP automatically.

    Note When SSH is enabled and its port and encryption ciphers are configured, no further configuration is required to use SCP. (SCP uses the same configuration as SSH.)

  - Do not enable both versions of SSH unless you require that both be activated at the same time. (Security protocols use extensive processing power.)

    Note To use SSH, you must have an SSH client installed. Most Linux and other UNIX® platforms include an SSH client as part of their installation, but Microsoft Windows operating systems do not. SSH clients are available from various vendors.

- Configure the port settings for Telnet and SSH.
- Select one or more data encryption algorithms for SSH, version 1, SSH version 2, or both.
- In the Web interface, specify a host key file previously created with the APC Security Wizard and load it to the Automatic Transfer Switch.

Note

From a command line interface, such as the command prompt on Windows operating systems, you can use FTP or SCP to transfer the host key file. You must transfer the file to location **/sec** on the Automatic Transfer Switch.

If you do not specify a host key file, the Automatic Transfer Switch generates an RSA host key of 768 bits, instead of the 1024-bit RSA host key that the Wizard creates. **The Automatic Transfer Switch can take up to 5 minutes to create this host key, and SSH is not accessible during that time.**

- Display the *fingerprint* of the SSH host key for SSH versions 1 and 2. Most SSH clients display the fingerprint at the start of a session. Compare the fingerprint displayed by the client to the fingerprint that you recorded from the Web interface or control console of the Automatic Transfer Switch.

Note

If you are using SSH version 2, expect a noticeable delay when logging on to the control console of the Automatic Transfer Switch. Although the delay is not long, it can be mistaken for a problem because there is no explanatory message.

Option	Description
Telnet/SSH Network Configuration	
Access	Enables or disables the access method selected in **Protocol Mode**. **NOTE:** Enabling SSH automatically disables Telnet. To enable SSH, change the setting and then click **Next>>** in the Web interface or choose **Accept Changes** in the control console. You must then agree to the license agreement that is displayed.
Protocol Mode	Choose one of the following: • **Telnet:** User names, passwords, and data are transmitted without encryption. • **Secure SHell (SSH), version 1:** User names, passwords, and data are transmitted in encrypted form. There is little or no delay when you are logging on. • **Secure SHell (SSH), version 2:** User names, passwords, and data are transmitted in encrypted form, but with somewhat more protection than version 1 from attempts to intercept, forge, or alter data during data transmission. There is a noticeable delay when you are logging on to the Automatic Transfer Switch. • **Secure SHell (SSH), versions 1 and 2**: Do not enable both versions of SSH unless you require that both be activated at the same time. (Security protocols use extensive processing power.)

Option	Description
Telnet/SSH Port Configuration	

Telnet Port	Identifies the TCP/IP port used for communications by Telnet with the Automatic Transfer Switch. The default is **23**.
	
	You can change the **Port** setting to the number of any unused port between **5000** and **32768** to enhance the protection provided by **User Name** and **Password** settings. Then, according to the requirements of your Telnet client program, you must use either a colon (:) or a space in the command line to specify the non-default port number. For example, for a port number of 5000 and a Automatic Transfer Switch IP address of 152.166.12.113, your Telnet client would require one or the other of the following commands:
	
	`telnet 152.166.12.113:5000`
	
	`telnet 152.166.12.113 5000`

SSH Port	Identifies the TCP/IP port used for communications by the Secure SHell (SSH) protocol with the Automatic Transfer Switch. The default is **22**. You can change the **Port** setting to the number of any unused port between **5000** and **32768** to enhance the protection provided by **User Name** and **Password** settings. See the documentation for your SSH client for information on the command line format required to specify a non-default port number when starting SSH.

Option	Description
SSH Server Configuration	
SSHv1 Encryption Algorithms	Enables or disables **DES**, and displays the status (always enabled) of **Blowfish**, two encryption algorithms (block ciphers) compatible with SSH version 1 clients. • **DES**: The key length is 56 bits. • **Blowfish**: The key length is 128 bits. You cannot disable this algorithm. **NOTE:** Not all SSH clients can use every algorithm. If your SSH client cannot use **Blowfish**, you must also enable **DES**.
SSHv2 Encryption Algorithms	Enables or disables the following encryption algorithms (block ciphers) that are compatible with SSH version 2 clients. • **3DES** (enabled by default): The key length is 168 bits. • **Blowfish** (enabled by default): The key length is 128 bits. • **AES 128**: The key length is 128 bits. • **AES 256**: The key length is 256 bits. **NOTE:** Not all SSH clients can use every algorithm. Your SSH client selects the algorithm that provides the highest security from among the enabled algorithms that it is able to use. (If your SSH client cannot use either of the default algorithms, you must enable an AES algorithm that it can use.)

Option	Description
SSH User Host Key File	
Status	The **Status** field Indicates the status of the host key (*private* key). In the control console, display the host key status by selecting **Advanced SSH Configuration**. • **SSH Disabled: No host key in use**: No host key has been transferred to the Automatic Transfer Switch or a host key has been transferred improperly. **NOTE:** A host key must be installed to the **/sec** directory of the Automatic Transfer Switch. • **Generating**: The Automatic Transfer Switch is generating a host key because no valid host key was installed in its **/sec** directory. • **Loading**: A host key is being loaded (i.e., being activated on the Automatic Transfer Switch). • **Valid**: The host key is valid. (If you install an invalid host key, the Automatic Transfer Switch discards it and generates a valid one. However, a host key that the Automatic Transfer Switch generates is only 768 bits in length. A valid host key created by the APC Security Wizard is 1024 bits.)
Filename	You can create a host key file with the APC Security Wizard and then upload it to the Automatic Transfer Switch by using the Web interface. Use the **Browse** button for the **Filename** field to locate the file, then click **Apply**. Alternatively, you can use FTP or SCP to transfer the host key file to the Automatic Transfer Switch. **NOTE:** Creating and uploading a host key in advance reduces the time required to enable SSH. If no host key is loaded when you enable SSH, the Automatic Transfer Switch creates one when it reboots. **The Automatic Transfer Switch takes up to 5 minutes to create this key, and the SSH server is not accessible during that time.**

Option	Description
SSH Host Key Fingerprint	
SSH v1:	Displays the SSH version 1 fingerprint for the host key. The fingerprint is a unique identifier to further authenticate the host key. In the control console, choose **Advanced SSH Configuration** and then **Host Key Information** to display the fingerprint.
SSH v2:	Displays the SSH version 2 fingerprint for the host key. The fingerprint is a unique identifier to further authenticate the host key. In the control console, choose **Advanced SSH Configuration** and then **Host Key Information** to display the fingerprint.

SNMP

An **Access** option (the **Settings** option in the control console) enables (by default) or disables SNMP. When SNMP is enabled, the **Access Control** settings allow you to control how each of the four available SNMP channels is used.

To define up to four NMSs to serve as trap receivers, see Trap Receiver settings.

To use SNMP to manage an Automatic Transfer Switch, see the *PowerNet® SNMP Management Information Base(MIB) Reference Guide* (**.\doc\en\mibguide.pdf**) on the APC Network Management Card *Utility* CD.

Setting	Definition
Community Name	This setting defines the password (maximum of 15 characters) which an NMS that is defined by the **NMS IP/Domain Name** setting uses to access the channel.
NMS IP/ Domain Name	Limits access to the NMS specified by a domain name or to the NMSs specified by the format used for the IP address: • A domain name allows only the NMS at that location to have access. • 159.216.12.1 allows only the NMS with that IP address to have access. • 159.216.12.255 allows access for any NMS on the 159.216.12 segment. • 159.216.255.255 allows access for any NMS on the 159.216 segment. • 156.255.255.255 allows access for any NMS on the 156 segment. • 0.0.0.0 or 255.255.255.255 allows access for any NMS.

Setting	Definition	
Access Type	Selects how the NMS defined by the **NMS IP Domain Name** setting can use the channel, when that NMS uses the correct **Community Name**.	
	Read	The NMS can use GETs at any time, but it can never use SETs.
	Write	The NMS can use GETs at any time, and can use SETs when no one is logged on to the control console or Web interface.
	Disabled	The NMS cannot use GETs or SETs.
	Write+	The NMS can use GETs and SETs at any time, even when someone is logged on to the control console or Web interface.

Email

Use this option to define two SMTP settings (**SMTP Server** and **From Address**) used by the e-mail feature of the Automatic Transfer Switch.

See SMTP settings and E-mail Feature.

Syslog

By default, the Automatic Transfer Switch can send messages to up to four syslog servers whenever Automatic Transfer Switch or embedded management card events occur. The Syslog servers, which must be specifically identified by their IP addresses or domain names, record the events in a log that provides a centralized record of events that occur at network devices.

See also

This user's guide does not describe Syslog, or the Syslog configuration values, in detail. For more information about Syslog, see RFC3164, available at **www.ietf.org/rfc/rfc3164**.

Syslog settings. Leave the Syslog settings, except the **Server IP** settings, set to their defaults unless otherwise specified by the Syslog network or system administrator.

General Settings	
Setting	**Definition**
Syslog	Enables (by default) or disables the Syslog feature.
Facility	Selects the facility code assigned to the Automatic Transfer Switch's Syslog messages (**User**, by default). **NOTE:** Although other selections are available, **User** is the selection that best defines the Syslog messages sent by a Automatic Transfer Switch.

Syslog Server Settings	
Server IP/ Domain Name	Uses specific IP addresses or domain names to identify which of up to four servers will receive Syslog messages sent by the Automatic Transfer Switch. **NOTE:** To use the Syslog feature, the **Server IP/Domain Name** setting must be defined for at least one server.
Port	Identifies the user datagram protocol (UDP) port that the Automatic Transfer Switch will use to send Syslog messages. The default is **514**, the number of the UDP port assigned to Syslog.
Local Priority (Severity Mapping)	
Map to Syslog's Priorities	Maps each of the severity levels (**Local Priority** settings) that can be assigned to embedded management card and Automatic Transfer Switch events to the available Syslog priorities. The following definitions are from RFC3164: • **Emergency**: The system is unusable • **Alert**: Action must be taken immediately • **Critical**: Critical conditions • **Error**: Error conditions • **Warning**: Warning conditions • **Notice**: Normal but significant conditions • **Informational**: Informational messages • **Debug**: Debug-level messages The following are the default settings for the four **Local Priority** settings: • **Severe** is mapped to **Critical** • **Warning** is mapped to **Warning** • **Informational** is mapped to **Info** • **None** (for events which have no severity level assigned) is mapped to **Info** **NOTE:** To disable sending Syslog messages for **Severe**, **Warning**, or **Informational** events, see Event Actions (Web Interface Only).

Syslog test (Web interface). This option allows you to send a test message to the Syslog servers configured in the **Syslog Server** section.

1. Select the priority to assign to the test message.
2. Define the test message using any text in the format described in Syslog message format. For example, `ATS: Communications Established 0x0F01` meets the required message format.
3. Click **Apply** to have the Automatic Transfer Switch send a Syslog message that uses the defined **Priority** and **Test Message** settings.

Syslog message format. A Syslog message has three parts:

- The priority (PRI) part identifies the Syslog priority assigned to the message's event and the facility code assigned to messages sent by the Automatic Transfer Switch.
- The Header includes a time stamp and the IP address of the Automatic Transfer Switch.
- The message (MSG) part has two fields:
  - A TAG field, which is followed by a colon and a space, identifies the event type (System or ATS, for example)
  - A CONTENT field provides the event text, followed by a space and the event code

Web/SSL

Use the **Web/SSL** menu to perform the following tasks.

- Enable or disable the two protocols that provide access to the Web interface of the Automatic Transfer Switch:
  - Hypertext Transfer Protocol (HTTP) provides access by user name and password, but does not encrypt user names, passwords, and data during transmission.
  - Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) encrypts user names, passwords, and data during transmission and provides authentication of the Automatic Transfer Switch by means of digital certificates.

    See Creating and Installing Digital Certificates to choose among the several methods for using digital certificates.

- Configure the ports that each of the two protocols will use.
- Select the encryption ciphers that SSL will use.

- Identify whether a server certificate is installed on the Automatic Transfer Switch. If a certificate has been created with the APC Security Wizard but is not installed:
  - In the Web interface, browse to the certificate file and upload it to the Automatic Transfer Switch.
  - Alternatively, use the SCP protocol or FTP to upload it to the location **\sec** on the Automatic Transfer Switch.

Note Creating and uploading a server certificate in advance reduces the time required to enable HTTPS (SSL/TLS). If no server certificate is loaded when you enable HTTPS (SSL/TLS), the Automatic Transfer Switch creates one when it reboots. **The Automatic Transfer Switch can take up to 5 minutes to create this certificate, and the SSL/TLS server is not available during that time.**

- Display the configured parameters of a digital server certificate, if one is installed.

Option	Description
Web/SSL Network Configuration	
Access	Enables or disables the access method selected in **Protocol Mode**.
Protocol Mode	Choose one of the following: • **HTTP:** User names, passwords, and data are transmitted without encryption. • **HTTPS (SSL):** User names, passwords, and data are transmitted in encrypted form, and digital certificates are used for authentication. **NOTE:** To enable HTTPS (SSL), change the setting and then click **Next>>** in the Web interface, or choose **Accept Changes** in the control console. You must then agree to the license agreement that is displayed. To activate the changes you must log off and log back on to the interface. When SSL is activated, your browser displays a lock icon, usually at the bottom of the screen. 

Option	Description
HTTP/HTTPS Port Configuration	
HTTP Port	Identifies the TCP/IP port used for communications by HTTP with the Automatic Transfer Switch. The default is **80**. You can change the **Port** setting to the number of any unused port between **5000** and **32768** to enhance the protection provided by **User Name** and **Password** settings. You must then use a colon (:) in the command line to specify the non-default port number. For example, for a port number of 5000 and a Automatic Transfer Switch IP address of 152.214.12.114, you would use this command: `http://152.214.12.114:5000`
HTTPS Port	Identifies the TCP/IP port used for communications by HTTPS with the Automatic Transfer Switch. The default is **443**. You can change the **Port** setting to the number of any unused port between **5000** and **32768** to enhance the protection provided by **User Name** and **Password** settings. You must then use a colon (:) in the command line to specify the non-default port number. For example, for a port number of 6502 and a Automatic Transfer Switch IP address of 156.214.12.114, you would use this command: `https://156.214.12.114:6502`

Option	Description
SSL Server Configuration	
CipherSuite	Enables or disables the following SSL encryption ciphers and hash algorithms. (To access these options in the control console, choose **Web/SSL**, then **Advanced SSL Configuration**.) **NOTE:** All of these encryption ciphers and hash algorithms use the RSA public key algorithm. • **DES (SSL_RSA_WITH_DES_CBC_SHA)**: a block cipher with a key length of 56 bits. The Secure Hash Algorithm (SHA) is used for authentication. • **3DES (SSL_RSA_WITH_3DES_EDE_CBC_SHA)**: a block cipher with a key length of 168 bits. A Secure Hash Algorithm (SHA) is used for authentication. • **RC4 (SSL_RSA_WITH_RC4_128_SHA)**: a stream cipher with a key length of 128 bits. A Secure Hash Algorithm (SHA) is used for authentication. This selection is enabled by default.
SSL Server Certificate	
Status	The **Status** field indicates whether a server certificate is installed. (To display the status in the control console, choose **Web/SSL**, then **Advanced SSL Configuration**.) • **Not installed**: No certificate is installed on the Automatic Transfer Switch. **NOTE:** If you install a certificate by using FTP or SCP, you must specify the correct location (**/sec**) on the Automatic Transfer Switch. • **Generating**: The Automatic Transfer Switch is generating a certificate because no valid certificate was installed. • **Loading**: A certificate is being loaded (activated on the Automatic Transfer Switch). • **Valid**: A valid certificate was installed to or generated by the Automatic Transfer Switch. (If you install an invalid certificate, the Automatic Transfer Switch discards it and generates a valid one. However, a certificate that the Automatic Transfer Switch generates has some limitations. See Method 1: Use the auto-generated default certificate.)

Option	Description
SSL Server Certificate	
Filename	You can create a server certificate with the APC Security Wizard and then upload it to the Automatic Transfer Switch by using the Web interface. Use the **Browse** button for the **Filename** field to locate the file, then click **Apply**. By default, the certificate is installed to the correct location. Alternatively, you can use FTP or SCP to transfer the server certificate to the Automatic Transfer Switch. However, you must specify the correct location (**/sec**) on the Automatic Transfer Switch. **NOTE:** Creating and uploading a server certificate in advance reduces the time required to enable HTTPS (SSL). If no server certificate is loaded when you enable HTTPS (SSL), the Automatic Transfer Switch creates one when it reboots. **The Automatic Transfer Switch can take up to 5 minutes to create this certificate, and the SSL server is not available during that time.**

Parameter	Description
Current Certificate Details	
Issued To	**Common Name (CN)**: The IP Address or DNS name of the Automatic Transfer Switch, except if the server certificate was generated by default by the Automatic Transfer Switch. For a default server certificate, the **Common Name (CN)** field displays the Automatic Transfer Switch's serial number. **NOTE:** If an IP address was specified as the Common Name when the certificate was created, use an IP address to log on to the Web interface of the Automatic Transfer Switch; if the DNS name was specified as the Common Name, use the DNS name to log on. When you log on, if you do not use the IP address or DNS name that was specified for the certificate, authentication fails, and you receive an error message asking if you want to continue. **Organization (O)**, **Organizational Unit (OU**), and **Locality, Country:** The name, organizational unit, and location of the organization that is using the server certificate. If the server certificate was generated by default by the Automatic Transfer Switch, the **Organizational Unit (OU)** field displays "Internally Generated Certificate." **Serial Number**: The serial number of the server certificate.
Issued By	**Common Name (CN)**: The Common Name as specified in the CA root certificate, except if the server certificate was generated by default by the Automatic Transfer Switch. For a default server certificate, the **Common Name (CN)** field displays the Automatic Transfer Switch's serial number. **Organization (O)** and **Organizational Unit (OU**): The name and organizational unit of the organization that issued the server certificate. If the server certificate was generated by default by the Automatic Transfer Switch, the **Organizational Unit (OU)** field displays "Internally Generated Certificate."
Validity	**Issued on**: The date and time at which the certificate was issued. **Expires on**: The date and time at which the certificate expires.
Current Certificate Details	

Parameter	Description
Fingerprint	Each fingerprint is a long string of alphanumeric characters punctuated by colons. A fingerprint is a unique identifier that you can use to further authenticate the server. Record the fingerprints to compare with the fingerprints contained in the certificate, as displayed in the browser. **SHA1 Fingerprint**: This fingerprint is created by a Secure Hash Algorithm (SHA).

System Menu

Introduction

Overview

Use the **System** menu to do the following tasks:

- Configure system identification, date and time settings, and access parameters for the Administrator, Device Manager, and Read-Only User accounts.
- Centrally administer remote access for each Network Management Card by using RADIUS (Remote Authentication Dial-in User Service).
- Synchronize the real-time clock for the Automatic Transfer Switch with a Network Time Protocol (NTP) server.
- Reset or restart the Automatic Transfer Switch interface.
- Define the URL links available in the Web interface.
- Set the units (Fahrenheit or Celsius) used for temperature displays.
- Access hardware and firmware information about the Automatic Transfer Switch (control console only).
- Download firmware files (control console only).
- Upload user configuration files to the Automatic Transfer Switch (Web interface only).

Note Only an Administrator has access to the **System** menu.

Menu options

Unless noted, the following menu options are available in the control console and Web interface:

- User Manager
- RADIUS
- Identification
- Date & Time
- Tools
- Preferences (Web interface)
- Links (Web interface)
- About system (control console)

Note The **About System** option is a **Help** menu option in the Web interface.

Option Settings

User Manager

Use this option to define the access values shared by the control console and the Web interface, and the authentication used to access the Web interface.

Setting	Definition
Auto Logout	The number of minutes (3, by default) before a user is automatically logged off because of inactivity.
Separate values for Administrator, Device Manager, and Read-Only User	
User Name	The case-sensitive name (maximum of 10 characters) used by Administrator and Device Manager users to log on at the control console or Web interface and by the Read-Only User to log on at the Web interface. Default values are **apc** for **Administrator** users, **device** for **Device Manager** users, and **readonly** for the **Read-Only User**.
Password	The case-sensitive password (maximum of 10 characters) always used to log on at the control console, but only used to log on to the Web interface when **Basic** is selected for the **Authentication** setting (**apc** is the default for the **Password** settings for the three account types). **NOTE:** A Read-Only User cannot log on through the control console.

RADIUS

RADIUS (Remote Authentication Dial-In User Service) is an authentication, authorization, and accounting service. Use this option to centrally administer remote access for each Automatic Transfer Switch.

When a user accesses the Automatic Transfer Switch, an authentication request is sent to the RADIUS server to determine the user's permission level.

Note RADIUS user names are limited to 32 characters.

For more information on user permission levels, see Types of user accounts.

Note RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address.

RADIUS Setting	Definition
Access	**Local Only**: RADIUS is disabled. Access to the Automatic Transfer Switch is controlled by the local user manager only.
	RADIUS then Local: RADIUS is enabled. Contact the RADIUS server first. If the RADIUS server fails to authenticate the user, the local user manager will be used to authenticate access to the Automatic Transfer Switch.
	RADIUS Only: RADIUS is enabled. Only the RADIUS server will be contacted. If the RADIUS server fails to authenticate the user, access will be denied. **NOTE:** If RADIUS only is selected, the only way to recover if the RADIUS server is unavailable, is through a serial connection to the control console.
Primary Server	The server name or IP address of the main RADIUS server.
Primary Server Secret	The shared secret between the primary RADIUS server and the Automatic Transfer Switch.
Secondary Server	The server name or IP address of the secondary RADIUS server.
Secondary Server Secret	The shared secret between the secondary RADIUS server and the Automatic Transfer Switch.
Timeout	The time in seconds that the Automatic Transfer Switch waits for a response from the RADIUS server.

Configuring the RADIUS server. You must configure your RADIUS server to work with the Automatic Transfer Switch. The following example is specific to APC's RADIUS server.

1. Define an APC vendor in your RADIUS server. APC's Private Enterprise Number, 318, is assigned by the Internet Assigned Numbers Authority (IANA).
2. Define a RADIUS vendor-specific attribute called `APC-Service-Type`. This is an integer with an attribute identifier of 1.
3. Configure RADIUS users. The `APC-Service-Type` attribute must be configured for each RADIUS user accessing the card. This attribute is set to one of the following values, which correspond to an access level on the Management Card.

```
1 - Administrator
2 - Device Manager
3 - Read-Only User
```

For more information on user permission levels, see Types of user accounts.

Identification

Use this option to define the System **Name**, **Contact**, and **Location** values used by the SNMP agent for the Automatic Transfer Switch. The option's settings provide the values used for the MIB-II **sysName**, **sysContact**, and **sysLocation** Object Identifications (OIDs).

See also

For more information about the MIB-II OIDs, see the PowerNet® *SNMP Management Information Base (MIB) Reference Guide* (**.\doc\en\mibguide.pdf**) provided on the APC Environmental Management System *Utility* CD.

Date & Time

Use this option to set the date and time used by the Automatic Transfer Switch. The option displays the current settings, and allows you to change those settings manually, or through a Network Time Protocol (NTP) Server.

Set Manually. Use this option in the Web interface, or **Manual** in the control console, to define the date and time for the Automatic Transfer Switch.

Note

An **Apply Local Computer Time to Automatic Transfer Switch** option, which is available in the Web interface only, sets these values to match the date and time settings of the computer you are using to access the Web interface.

Synchronize with Network Time Protocol (NTP) Server. Use this option, or **Network Time Protocol (NTP)** in the control console, to have an NTP Server update the date and time for the Automatic Transfer Switch automatically.

Note

In the control console, use the **NTP Client** option to enable or disable (the default) the NTP Server updates. In the Web interface, use the **Set Manually** option to disable the updates.

Setting	Definition
Primary NTP Server	Identifies the IP address or domain name of the primary NTP server.
Secondary NTP Server	Identifies the IP address or domain name of the secondary NTP server, when a secondary server is available.
GMT Offset (Time Zone)	Defines the offset from Greenwich Mean Time (GMT) based on the Automatic Transfer Switch's time zone.
Update Interval	Defines how often, in hours, the Automatic Transfer Switch accesses the NTP Server for an update. The minimum is 1 hour; the maximum is 8760 hours (1 year). Use **Update Using NTP Now** to initiate an immediate update as well.

Tools

Use this option to initiate any of the following actions:

Action	Definition
Reboot Management Interface	Restarts the user interface of the Automatic Transfer Switch.
Reset to Defaults	Resets all configuration settings. This option will reset the TCP/IP settings and enable DHCP and BOOTP.
Reset to Defaults Except TCP/IP	Resets all configuration settings except the TCP/IP settings.
Reset Only TCP/IP to Defaults	Resets the TCP/IP settings only. This option will not enable DHCP and BOOTP.
Delete SSH Host Keys and SSL Certificates	Removes any SSH host key and server certificate on the Management Card so that you can reconfigure these components of your security system.

Uploading an initialization file (Web interface only). To transfer configuration settings from a configured Automatic Transfer Switch to the current Automatic Transfer Switch, export the .ini file from the configured Automatic Transfer Switch, select the **Tools** menu on the current Automatic Transfer Switch, browse to the file, and click **Upload**. The current Automatic Transfer Switch imports the file and uses it to set its own configuration. The **Status** field reports the progress of the upload.

See How to Export Configuration Settings for information on the content of the .ini file, how to preserve comments you add to the file, and how to export settings to multiple Automatic Transfer Switchs.

File Transfer (control console only). The **File Transfer** option of the **Tools** menu provides two methods for file transfer over the network and one for file transfer through a serial connection to the Automatic Transfer Switch.

Option	Description
XMODEM	Allows you to transfer either an .ini file or a firmware upgrade file to a Automatic Transfer Switch using a terminal-emulation program. This option is available only when you use a local connection to the control console. .
FTP Client	Use one of these two options to transfer either an .ini file or a firmware upgrade file from a FTP or TFTP server of your organization (company, agency, or department) to the current Automatic Transfer Switch. These options assume that your organization has a centralized system for configuring or upgrading APC Automatic Transfer Switches. For **FTP Client**, you are prompted for a user name and password. For either option, you are then prompted for the server address and the file to transfer. After you supply that required information, the Automatic Transfer Switch transfers the file.
TFTP Client	

Preferences (Web interface)

Use this option to define whether temperature values are displayed as **Fahrenheit** or **Celsius** in the Web interface and the control console.

Links (Web interface)

Use this option to modify the links to APC Web pages.

Setting	Definition
User Links	
Name	Defines the link names that appear in the **Links** menu (by default, **APC's Web site**, **Testdrive Demo**, and **APC Monitoring**).
URL	Defines the URL addresses used by the links. By default, the following URL addresses are used: • **www.apc.com** (APC's Web site) • **http://testdrive.apc.com** (Testdrive Demo) • **http://rms.apc.com** (Remote Monitoring) **NOTE**:Only links of type http:// can be used in these fields. For information about these pages see Links menu.
Access Links	
APC Home Page	Defines the URL address used by the APC logo at the top of all Web interface pages (by default, **www.apc.com**).

About system (control console)

This option identifies the following hardware information for the Automatic Transfer Switch: **Model Number**, **Serial Number**, **Hardware Revision**, **Manufacture Date**, and **MAC Address**.

This screen also displays **Name**, **Version**, **Date**, and **Time** for the Application Module and AOS.

The **About System** menu also includes fields for system **Flash Type** and the **Type**, **Sector**, and **CRC 16** for each module.

Note In the Web interface, except for **Flash Type**, this hardware information is reported by the **About System** option in the **Help** menu.

Boot Mode

Introduction

Overview

In addition to using a BOOTP server or manual settings, the Automatic Transfer Switch can use a dynamic host configuration protocol (DHCP) server to provide the settings that it needs to operate on a TCP/IP network.

The method that is used to provide the network settings for the Automatic Transfer Switch depends on **Boot mode**, a **TCP/IP** option in the **Network** menu. To use a DHCP server to provide the network assignment for the Automatic Transfer Switch, **Boot mode** must be set to either **DHCP & BOOTP**, its default setting, or **DHCP only**.

See also

For more details on DHCP and DHCP options, see RFC2131 and RFC2132 at **www.ietf.org/rfc**.

DHCP & BOOTP boot process

When **Boot mode** is set to its default **DHCP & BOOTP** setting, the following occurs when the Automatic Transfer Switch is started or reset:

1. The Automatic Transfer Switch makes up to five requests for its network assignment from any BOOTP server. If a valid BOOTP response is received, the Automatic Transfer Switch starts the network services and sets Boot mode to **BOOTP Only**.
2. If the Automatic Transfer Switch fails to receive a valid BOOTP response after five BOOTP requests, the Automatic Transfer Switch makes up to five requests for its network assignment from any DHCP server. If a valid DHCP response is received, the Automatic Transfer Switch starts the network services and sets Boot mode to **DHCP Only**.

   Note To configure the Automatic Transfer Switch so that it always uses the **DHCP & BOOTP** setting for **Boot mode**, enable the **Remain in DHCP & BOOTP mode after accepting TCP/IP settings** option, which is disabled by default.

3. If the Automatic Transfer Switch fails to receive a valid DHCP response after five DHCP requests, it repeats BOOTP and DHCP requests until it receives a valid network assignment. First it sends a BOOTP request every 32 seconds for 12 minutes, then it sends one DHCP request with a time-out of 64 seconds, and so forth.

   Note If a DHCP server responds with an invalid offer (i.e., without the APC cookie), the Automatic Transfer Switch accepts the lease from that server on the last request of the sequence and immediately releases that lease. This prevents the DHCP server from reserving the IP Address associated with its invalid offer.

   For more information on what a valid response requires, see DHCP response options.

DHCP Configuration Settings

Automatic Transfer Switch settings

The **TCP/IP** option in the **Network** menu of the Web interface and control console accesses the network settings for the Automatic Transfer Switch.

Three settings (**Port Speed**, **Host Name**, and **Domain Name**) are available regardless of the **TCP/IP** option's **Boot mode** selection, and three settings (**Vendor Class**, **Client ID**, and **User Class**) are available for any **Boot mode** selection except **Manual**.

When **Boot mode** is set to **DHCP & BOOTP**, two options are available:

- **After IP Assignment** in the control console (or **Remain in DHCP & BOOTP mode after accepting TCP/IP settings** in the Web interface): By default, this option switches **Boot mode** to **DHCP Only** or **BOOTP Only**, based on the server that provided the TCP/IP settings.
- **DHCP Cookie Is** in the control console (or **Require vendor specific cookie to accept DHCP Address** in the Web interface): By default, this option requires that the DHCP responses include the APC cookie in order to be valid.

For more information about the APC cookie, see DHCP response options.

When **Boot mode** is set to **DHCP Only,** two options are available:

- **DHCP Cookie Is** in the control console (or **Require vendor specific cookie to accept DHCP Address** in the Web interface): By default, this option requires that the DHCP responses include the APC cookie in order to be valid.

  For more information about the APC cookie, see DHCP response options

- **Retry Then Stop** in the control console (or **Maximum # of Retries** in the Web interface): This option sets the number of times the Automatic Transfer Switch will repeat the DHCP request if it does not receive a valid response. By default, the number of retries is **0**, which sets the Automatic Transfer Switch to continue repeating the DHCP request indefinitely.

DHCP response options

Each valid DHCP response contains options that provide the TCP/IP settings that the Automatic Transfer Switch needs to operate on a network, and other information that affects the operation of the Automatic Transfer Switch.

The Automatic Transfer Switch uses the Vendor Specific Information option (option 43) in a DHCP response to determine whether the DHCP response is valid.

Vendor Specific Information (option 43). The Vendor Specific Information option contains up to two APC specific options encapsulated in a TAG/LEN/DATA format: the APC cookie and the Boot Mode Transition.

APC Cookie. Tag 1, Len 4, Data "1APC". Option 43 notifies the Automatic Transfer Switch that a DHCP server has been configured to service APC devices. By default, the APC cookie must be present in this DHCP response option before the Automatic Transfer Switch can accept the lease.

Note Use the **DHCP Cookie Is** setting described in Automatic Transfer Switch settings to disable the APC cookie requirement.

Following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the APC cookie:

```
Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43
```

Boot Mode Transition. Tag 2, Len 1, Data 1/2. This option 43 setting enables or disables the **After IP Assignment** option which, by default, causes the **Boot mode** option to use the setting that reflects the server that provided the TCP/IP settings (**DHCP Only** or **BOOTP Only**):

- For a data value of 1, the **After IP Assignment** option is disabled, and the **Boot mode** option remains in its **DHCP & BOOTP** setting after successful network assignment. Whenever the Automatic Transfer Switch restarts, it will request its network assignment first from a BOOTP server, and then, if necessary, from a DHCP server.

  See DHCP & BOOTP boot process.

- For a data value of 2, the **After IP Assignment** option is enabled and the **Boot mode** option switches to **DHCP Only** when the Automatic Transfer Switch accepts the DHCP response. Whenever the Automatic Transfer Switch restarts, it will request its network assignment (TCP/IP settings) from a DHCP server only.

  For more information about the **After IP Assignment**, see Automatic Transfer Switch settings.

Following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the APC cookie and the disable Boot Mode Transition setting:

```
Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43 0x02 0x01 0x01
```

TCP/IP options. The Automatic Transfer Switch uses the following options within a valid DHCP response to define its TCP/IP settings:

- **IP Address** (from the **yiaddr** field of the DHCP response): The IP address that the DHCP server is leasing to the Automatic Transfer Switch.
- **Subnet Mask** (option 1): The subnet mask value needed by the Automatic Transfer Switch to operate on the network.
- **Default Gateway** (option 3): The default gateway address needed by the Automatic Transfer Switch to operate on the network.
- **Address Lease Time** (option 51): The time duration for the lease associated with the identified **IP Address**.
- **Renewal Time, T1** (option 58): The Automatic Transfer Switch must wait after an IP address lease is assigned before it can request a renewal of that lease.
- **Rebinding Time, T2** (option 59): The time that the Automatic Transfer Switch must wait after an IP address lease is assigned before it can seek to rebind that lease.

Other options. The Automatic Transfer Switch uses the following options within a valid DHCP response to define NTP, DNS, hostname, and domain name settings:

- **NTP Server, Primary and Secondary** (option 42): Up to two NTP servers that can be used by the Automatic Transfer Switch.
- **NTP Time Offset** (option 2): The offset, in seconds, of the subnet for the Automatic Transfer Switch from Coordinated Universal Time (UTC).
- **DNS Server, Primary and Secondary** (option 6): One or two DNS servers that can be used by the Automatic Transfer Switch.
- **Host Name** (option 12): The hostname (maximum length of 32 characters) to be used by the Automatic Transfer Switch.
- **Domain Name** (option 15): The domain name (maximum length of 64 characters) to be used by the Automatic Transfer Switch.

Security

Security Features

Planning and implementing security features

As a network device that passes information across the network, the Automatic Transfer Switch is subject to the same exposure as other devices on the network.

Use the information in this section to plan and implement the security features appropriate for your environment.

Summary of access methods

Serial control console.

Security Access	Description
Access is by user name and password.	Always enabled.

Remote control console.

Security Access	Description
Available methods: • User name and password • Selectable server port • Server Enable/Disable • Secure SHell (SSH)	For high security, use SSH. • With Telnet, the user name and password are transmitted as plain text. • SSH disables Telnet and provides encrypted access to the control console interface to provide additional protection from attempts to intercept, forge, or alter data during data transmission.

SNMP.

Security Access	Description
Available methods: • Community Name • Domain Name • NMS IP filters • Agent Enable/Disable • 4 access communities with read/write/disable capability	The domain name restricts access only to the NMS as that location, and the NMS IP filters allow access only from designated IP addresses. • 162.245.12.1 allows only the NMS with that IP address to have access. • 162.245.12.255 allows access for any NMS on the 162.245.12 segment. • 162.245.255.255 allows access for any NMS on the 162.245 segment. • 162.255.255.255 allows access for any NMS on the 162 segment. • 0.0.0.0 or 255.255.255.255 allows access for any NMS.

File transfer protocols.

Security Access	Description
Available methods: • User name and password • Selectable server port • Server Enable/Disable • Secure CoPy (SCP)	With FTP, the user name and password are transmitted as plain text, and files are transferred without the protection of encryption. Using SCP instead of FTP encrypts the user name and password and the files being transferred, such as firmware updates, configuration files, log files, Secure Sockets Layer (SSL) certificates, and Secure SHell (SSH) host keys. If you choose SCP as your file transfer protocol, enable SSH and disable FTP.

Web server.

Security Access	Description
Available methods: • User name and password • Selectable server port • Server Enable/Disable • Secure Sockets Layer (SSL) and Transport Layer Security (TLS)	In basic HTTP authentication mode, the user name and password are transmitted base-64 encoded (with no encryption). SSL and TLS are available on Web browsers supported for the Automatic Transfer Switch and on most Web servers. The Web protocol Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) encrypts and decrypts page requests to the Web server and pages returned by the Web server to the user.

RADIUS.

Security Access	Description
Available methods: • Centralized authentication of access rights • A server secret shared between the RADIUS server and the Automatic Transfer Switch	RADIUS (Remote Authentication Dial-In User Service) is an authentication, authorization, and accounting service used to centrally administer remote access for each Automatic Transfer Switch.

Change default user names and passwords immediately

As soon as you complete the installation and initial configuration of the Automatic Transfer Switch, immediately change the default user names and passwords. Configuring unique user names and passwords is essential to establish basic security for your system.

Port assignments

If a Telnet, FTP, SSH/SCP, or Web/SSL/TLS server uses a non-standard port, a user must specify the port when using the client interface, such as a Web browser. The non-standard port address becomes an extra "password," hiding the server to provide an additional level of security. The TCP ports for which these servers listen are initially set at the standard "well known ports" for the protocols. To hide the interfaces, use any port numbers from 5000 to 32768.

Note If you are using an FTP server, use any port numbers from 5001 to 32768.

User names, passwords, community names (SNMP)

All user names, passwords, and community names for SNMP are transferred over the network as plain text. A user who is capable of monitoring the network traffic can determine the user names and passwords required to log on to the accounts of the control console or Web interface of the Automatic Transfer Switch. If your network requires the higher security of the encryption-based options available for the control console and Web interface, be sure to disable SNMP access or set its access to read-only. (Read-only access allows you to receive status information and to use SNMP traps.)

Authentication versus encryption

You can select to use security features for the Automatic Transfer Switch that control access by providing basic authentication through user names, passwords, and IP addresses, without using encryption. These basic security features are sufficient for most environments in which sensitive data is not being transferred.

To ensure that data and communication between the Automatic Transfer Switch and the client interfaces, such as the control console and the Web interface, cannot be intercepted, you can provide a greater level of security by using one or more of the following encryption-based methods:

- For the Web interface, use the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols.
- To encrypt user names and passwords for control console access, use the Secure SHell (SSH) protocol.
- To encrypt user names, passwords, and data for the secure transfer of files, use the SCP protocol.

For more information on these protocols for encryption-based security, see Secure SHell (SSH) and Secure CoPy (SCP) and Secure Sockets Layer (SSL).

Encryption

Secure SHell (SSH) and Secure CoPy (SCP)

The Secure SHell (SSH) protocol provides a secure mechanism to access computer consoles or *shells* remotely. The protocol authenticates the server (in this case, the Automatic Transfer Switch) and encrypts all transmissions between the SSH client and the server.

- SSH is an alternative to Telnet, which does not provide encryption.
- SSH protects the username and password, the credentials for authentication, from being used by anyone intercepting network traffic.
- To authenticate the SSH server (the Automatic Transfer Switch) to the SSH client, SSH uses a host key that is unique to the SSH server and that provides an identification that cannot be falsified. Therefore, an invalid server on the network cannot obtain a user name and password from a user by presenting itself as a valid server.
- The Automatic Transfer Switch supports versions 1 and 2 of SSH. The encryption mechanisms of the versions differ, and each version has advantages. Version 1 provides faster login to the Automatic Transfer Switch, and version 2 provides improved protection from attempts to intercept, forge, or change data that is transmitted.
- When you enable SSH, Telnet is automatically disabled.
- The interface, user accounts, and user access rights are the same whether you access the control console through SSH or Telnet.

For information on supported SSH client applications, see Telnet/SSH.

Secure CoPy (SCP) is a secure file transfer application that you can use instead of FTP. SCP uses the SSH protocol as the underlying transport protocol for encryption of user names, passwords, and files.

- When you enable and configure SSH, you automatically enable and configure SCP. No further configuration of SCP is needed.
- You must explicitly disable FTP. It is **not** disabled by enabling SSH.

Secure Sockets Layer (SSL)

For secure Web communication, you enable Secure Sockets Layer (SSL) by selecting HTTPS (SSL/TLS) as the protocol mode to use for access to the Web interface of the Automatic Transfer Switch. Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) is a Web protocol that encrypts and decrypts page requests from the user and pages that are returned by the Web server to the user. Originally developed by Netscape, it has become an internet standard supported by most Web browsers.

The Automatic Transfer Switch supports SSL version 3.0. Most browsers let you select the version of SSL to enable.

When SSL is enabled, your browser displays the lock icon, usually at the bottom of the screen.

SSL uses a digital certificate to enable the browser to authenticate the server (in this case, the Automatic Transfer Switch). The browser verifies the following:

- The format of the server certificate is correct.
- The server certificate's expiration date and time have not passed.
- The DNS name or IP address specified when a user logs on matches the common name in the server certificate.
- The server certificate is signed by a trusted certifying authority.

Each major browser manufacturer distributes CA root certificates of the commercial Certificate Authorities in the certificate store (cache) of its browser so that it can compare the signature on the server certificate to the signature on a CA root certificate.

You can use the APC Security Wizard, provided on the APC Automatic Transfer Switch *Utility* CD, to create a certificate signing request to an external Certificate Authority, or if you do not want to use an existing Certificate Authority, you can create an APC root certificate to upload to a browser's certificate store (cache). You can also use the Wizard to create a server certificate to upload to the Automatic Transfer Switch.

See Creating and Installing Digital Certificates for a summary of how these certificates are used.

To create certificates and certificate requests, see Create a Root Certificate & Server Certificates and Create a Server Certificate and Signing Request.

SSL also uses various algorithms and encryption ciphers to authenticate the server, encrypt data, and ensure the integrity of the data (i.e., that it has not been intercepted and sent by another server).

Note Web browsers cache (save) Web pages that you recently accessed and allow you to return to those pages without re-entering your user name and password. Always close your browser session before you leave your computer unattended.

Creating and Installing Digital Certificates

Purpose

For network communication that requires a higher level of security than password encryption, the Web interface of the Automatic Transfer Switch supports the use of digital certificates with the Secure Sockets Layer (SSL) protocol. Digital certificates can authenticate the Automatic Transfer Switch (the server) to the Web browser (the SSL client).

Choosing a method for your system

Using the Secure Socket Layer (SSL) protocol, you can choose any of the following methods for using digital certificates.

Method 1: Use the auto-generated default certificate. When you enable SSL, you must reboot the Automatic Transfer Switch. During rebooting, if no server certificate exists on the Automatic Transfer Switch, the Automatic Transfer Switch generates a default server certificate that is self-signed but that you cannot configure.

This method has the following advantages and disadvantages:

- **Advantages:**
  - Before they are transmitted, the user name and password for Automatic Transfer Switch access and all data to and from the Automatic Transfer Switch are encrypted.
  - You can use this default server certificate to provide encryption-based security while you are setting up either of the other two digital certificate options, or you can continue to use it for the benefits of encryption that SSL provides.
- **Disadvantages:**
  - The Automatic Transfer Switch takes up to 5 minutes to create this certificate, and the Web interface is not available during that time. (This delay occurs the first time you log on after you enable SSL.)
  - This method does not include the browser-based authentication provided by a CA certificate (a certificate signed by a Certificate Authority) as Methods 2 and 3 provide. There is no CA Certificate cached in the browser. Therefore, whenever you log on to the Automatic Transfer Switch, the browser generates a security alert, indicating that a certificate signed by a trusted authority is not available and asking if you want to proceed.

– The default server certificate on the Automatic Transfer Switch has the Automatic Transfer Switch's serial number in place of a valid *common name* (the DNS name or the IP address of the Automatic Transfer Switch). Therefore, although the Automatic Transfer Switch can control access to its Web interface by user name, password, and account type (e.g., **Administrator**, **Device Manager**, or **Read-Only User**), the browser cannot authenticate what Automatic Transfer Switch is sending or receiving data.

– The length of the *public key* (RSA key) that is used for encryption when setting up an SSL session is only 768 bits. (The public key used in Methods 2 and 3 is 1024 bits, providing more complex encryption and consequently a higher level of security.)

Method 2: Use the APC Security Wizard to create a CA certificate and a server certificate. Use the APC Security Wizard to create two digital certificates:

- A *CA root certificate* (Certificate Authority root certificate) that the APC Security Wizard uses to sign all server certificates and which you then install into the certificate store (cache) of the browser of each user who needs access to the Automatic Transfer Switch.
- A *server certificate* that you upload to the Automatic Transfer Switch. When the APC Security Wizard creates a server certificate, it uses the CA root certificate to sign the server certificate.

The Web browser authenticates the Automatic Transfer Switch sending or requesting data:

- To identify the Automatic Transfer Switch, the browser uses the *common name* (IP address or DNS name of the Automatic Transfer Switch) that was specified in the server certificate's *distinguished name* when the certificate was created.
- To confirm that the server certificate is signed by a "trusted" signing authority, the browser compares the signature of the server certificate with the signature in the root certificate cached in the browser. An expiration date confirms whether the server certificate is current.

This method has the following advantages and disadvantages.

- **Advantages:**
  - Before they are transmitted, the user name and password for Automatic Transfer Switch access and all data to and from the Automatic Transfer Switch are encrypted.
  - The length of the *public key* (RSA key) that is used for encryption when setting up an SSL session is 1024 bits, providing more complex encryption and consequently a higher level of security than the public key used in Method 1. (This longer encryption key is also used in Method 3.)
  - The server certificate that you upload to the Automatic Transfer Switch enables SSL to authenticate that data are being received from and sent to the correct Automatic Transfer Switch. This provides an extra level of security beyond the encryption of the user name, password, and transmitted data.
  - The root certificate that you install to the browser enables the browser to authenticate the Automatic Transfer Switch's server certificate to provide additional protection from unauthorized access.
- **Disadvantage:**

  Because the certificates do not have the digital signature of a commercial Certificate Authority, you must load a root certificate individually into the certificate store (cache) of each user's browser. (Browser manufacturers already provide root certificates for commercial Certificate Authorities in the certificate store within the browser.)

Method 3: Use the APC Security Wizard to create a certificate-signing request to be signed by the root certificate of an external Certificate Authority and to create a server certificate. You use the APC Security Wizard to create a request (a **.csr** file) to send to a Certificate Authority. The Certificate Authority returns a signed certificate (a **.crt** file) based on information you submitted in your request. You then use the APC Security Wizard to create a server certificate (a .**p15** file) that includes the signature from the root certificate returned by the Certificate Authority. You upload the server certificate to the Automatic Transfer Switch.

Note You can also use Method 3 if your company or agency operates its own Certificate Authority, Use the APC Security Wizard in the same way, but use your own Certificate Authority in place of a commercial Certificate Authority.

This method has the following advantages and disadvantages.

- **Advantages:**
  - Before they are transmitted, the user name and password for Automatic Transfer Switch access and all data to and from the Automatic Transfer Switch are encrypted.
  - You have the benefit of authentication by a Certificate Authority that already has a signed root certificate in the certificate cache of the browser. (The CA certificates of commercial Certificate Authorities are distributed as part of the browser software, and a Certificate Authority of your own company or agency has probably already loaded its CA certificate to the browser store of each user's browser.) Therefore, you do not have to upload a root certificate to the browser of each user who needs access to the Automatic Transfer Switch.

- The length of the *public key* (RSA key) that is used for setting up an SSL session is 1024 bits, providing more complex encryption and consequently a higher level of security than the public key used in Method 1. (This longer encryption key is also used in Method 2.)
- The server certificate that you upload to the Automatic Transfer Switch enables SSL to authenticate that data are being received from and sent to the correct Automatic Transfer Switch. This provides an extra level of security beyond the encryption of the user name, password, and transmitted data.
- The browser matches the digital signature on the server certificate that you uploaded to the Automatic Transfer Switch with the signature on the CA root certificate that is already in the browser's certificate cache to provide additional protection from unauthorized access.

• **Disadvantages:**

- Setup requires the extra step of requesting a signed root certificate from a Certificate Authority.
- An external Certificate Authority may charge a fee for providing signed certificates.

Firewalls

Although some methods of authentication provide a higher level of security than others, complete protection from security breaches is almost impossible to achieve. Well-configured firewalls are an essential element in an overall security scheme.

Using the APC Security Wizard

Overview

Authentication

Authentication verifies the identity of a user or a network device (such as an APC Automatic Transfer Switch). Passwords typically identify computer users. However, for transactions or communications requiring more stringent security methods on the Internet, the Automatic Transfer Switch supports more secure methods of authentication.

- Secure Sockets Layer (SSL), used for secure Web access, uses digital certificates for authentication. A digital *CA root* certificate is issued by a Certificate Authority (CA) as part of a public key infrastructure, and its digital signature must match the digital signature on a server certificate on the Automatic Transfer Switch.
- Secure SHell (SSH), used for remote terminal access to the Automatic Transfer Switch's control console, uses a public *host key* for authentication rather than a digital certificate.

How certificates are used. Most Web browsers, including all browsers supported by the Automatic Transfer Switch, contain a set of CA root certificates from all of the commercial Certificate Authorities.

Authentication of the server (in this case, the Automatic Transfer Switch) occurs each time a connection is made from the browser to the server. The browser checks to be sure that the server's certificate is signed by a Certificate Authority known to the browser. For this authentication to occur:

- Each Automatic Transfer Switch with SSL enabled must have a server certificate on the Automatic Transfer Switch.
- Any browser that is used to access the Automatic Transfer Switch's Web interface must contain the CA root certificate that signed the server certificate.

If authentication fails, the browser prompts you on whether to continue despite the fact that it cannot authenticate the server.

If your network does not require the authentication provided by digital certificates, you can use the default certificate that the Automatic Transfer Switch generates automatically. The default certificate's digital signature will not be recognized by browsers, but a default certificate enables you to use SSL for the encryption of transmitted user names, passwords, and data. (If you use the default certificate, the browser prompts you to agree to unauthenticated access before it logs you on to the Web interface of the Automatic Transfer Switch.)

How SSH host keys are used. An SSH *host key* authenticates the identity of the server (the Automatic Transfer Switch) each time an SSH client contacts the Automatic Transfer Switch. Each Automatic Transfer Switch with SSH enabled must have an SSH host key on the Automatic Transfer Switch itself.

Files you create for SSL and SSH security

Use the APC Security Wizard to create the following components of an SSL and SSH security system:

- The server certificate for the Automatic Transfer Switch, if you want the benefits of authentication that such a certificate provides.You can create either of the following types of server certificate:
  - A server certificate signed by a custom CA root certificate also created with the APC Security Wizard. Use this method if your company or agency does not have its own Certificate Authority and you do not want to use an external Certificate Authority to sign the server certificate.
  - A server certificate signed by an external Certificate Authority. This Certificate Authority can be one that is managed by your own company or agency or can be one of the commercial Certificate Authorities whose CA root certificates are distributed as part of a browser's software.
- A certificate signing request containing all the information required for a server certificate except the digital signature. You need this request if you are using an external Certificate Authority.
- A CA root certificate.
- An SSH host key that your SSH client program uses to authenticate the Automatic Transfer Switch when you log on to the control console interface.

Note All public keys for SSL certificates and all host keys for SSH created with the APC Security Wizard are 1024-bit RSA keys. If you do not create and use SSL server certificates and SSH host keys with the APC Security Wizard, the Automatic Transfer Switch generates 768-bit RSA keys.

Only APC server management and key management products can use server certificates, host keys, and CA root certificates created by the APC Security Wizard. These files will not work with products such as OpenSSL® and Microsoft IIS.

Create a Root Certificate & Server Certificates

Summary

Use this procedure if your company or agency does not have its own Certificate Authority and you do not want to use a commercial Certificate Authority to sign your server certificates.

Note

The public RSA key that is part of a certificate generated by the APC Security Wizard is 1024 bits. (The default key generated by the Automatic Transfer Switch, if you do not use the Wizard, is 768 bits.)

- Create a CA root certificate that will be used to sign all server certificates to be used with Automatic Transfer Switchs. During this task, two files are created.
  - The file with the **.p15** extension is an encrypted file which contains the Certificate Authority's private key and public root certificate. This file signs the server certificates.
  - The file with the **.crt** extension, which contains only the Certificate Authority's public root certificate. You load this file into each Web browser that will be used to access the Automatic Transfer Switch so that the browser can validate the server certificate of the Automatic Transfer Switch.
- Create a server certificate, which is stored in a file with a **.p15** extension. During this task, you are prompted for the CA root certificate that signs the server certificate.
- Load the server certificate onto the Automatic Transfer Switch.
- For each Automatic Transfer Switch that requires a server certificate, repeat the tasks that create and load the server certificate.

The procedure

Create the CA root certificate. Perform these steps. (Click **Next** to move from screen to screen.)

1. If the APC Security Wizard is not already installed on your computer, install it by running the installation program **APC Security Wizard.exe** from the APC Automatic Transfer Switch *Utility* CD.
2. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
3. On the screen labeled Step 1, select **CA Root Certificate** as the type of file to create.
4. Enter a name for the file that will contain the Certificate Authority's public root certificate and private key. The file name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. On the screen labeled Step 2, provide the information to configure the CA root certificate. The **Country** and **Common Name** fields are required; the other fields are optional. For the **Common Name** field, enter an identifying name of your company or agency; use only alphanumeric characters, with no spaces.

Note By default, a CA root certificate is valid for 10 years from the current date and time, but you can edit the **Validity Period Start** and **Validity Period End** fields.

6. On the next screen, review the summary of the certificate. Scroll downward to view the certificate's unique serial number and fingerprints. To make any changes to the information you provided, click **Back**, and revise the information.

Note

The certificate's subject information and the certificate's issuer information should be identical.

7. The last screen verifies that the certificate has been created and instructs you on the next tasks.
   – This screen displays the location and name of the **.p15** file that you will use to sign the server certificates.
   – This screen also displays the location and name of the **.crt** file, which is the CA root certificate that you will load into the browser of each user who needs to access the Automatic Transfer Switch.

Load the CA root certificate to your browser. Load the **.crt** file to the browser of each user who needs to access the Automatic Transfer Switch.

See also

See the help system of the browser for information on how to load the **.crt** file into the browser's certificate store (cache). Following is a summary of the procedure for Microsoft Internet Explorer.

1. Select **Tools**, then **Internet Options** from the menu bar.
2. On the **Content** tab in the **Internet Options** dialog box, click **Certificates** and then **Import**.
3. The Certificate Import Wizard will guide you through the rest of the procedure. The file type to select is X.509, and the CA Public Root Certificate is the **.crt** file created in the procedure Create a Root Certificate & Server Certificates.

Create an SSL Server User Certificate. Perform these steps. (Click **Next** to move from screen to screen.)

1. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
2. On the screen labeled Step 1, select **SSL Server Certificate** as the type of file to create.
3. Enter a name for the file that will contain the server certificate and the private key. The file name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
4. Click the **Browse** button, and select the CA root certificate created in the procedure Create a Root Certificate & Server Certificates. The CA Root Certificate is used to sign the Server User Certificate being generated.
5. On the screen labeled Step 2, provide the information to configure the server certificate. The **Country** and **Common Name** fields are required; the other fields are optional. For the **Common Name** field, enter the IP address or DNS name of the server (Automatic Transfer Switch). Because the configuration information is part of the signature, it cannot be exactly the same as the information you provided when creating the CA root certificate; the information you provide in some of the fields must be different.

Note By default, a server certificate is valid for 10 years from the current date and time, but you can edit the **Validity Period Start** and **Validity Period End** fields.

6. On the next screen, review the summary of the certificate. Scroll downward to view the certificate's unique serial number and fingerprints. To make any changes to the information you provided, click **Back**, and revise the information.

   Note The information for every certificate must be unique. The configuration of a server certificate cannot be the same as the configuration of the CA root certificate. (The expiration date is not considered part of the unique configuration; some other configuration information must also differ.)

7. The last screen verifies that the certificate has been created and instructs you on the next task, to load the server certificate to the Automatic Transfer Switch. It displays the location and name of the Server Certificate, which has a **.p15** file extension and contains the Automatic Transfer Switch private key and public root certificate.

Load the server certificate to the Automatic Transfer Switch.

Perform these steps:

1. On the **Network** menu of the Web interface of the Automatic Transfer Switch, select the **Web/SSL** option.
2. In the **SSL/TLS Server Certificate** section of the page, browse to the server certificate, the **.p15** file you created in the procedure Create a Root Certificate & Server Certificates. (The default is **C:\Program Files\American Power Conversion\APC Security Wizard**.)

Note

Alternatively, you can use FTP or SCP to transfer the server certificate to the Automatic Transfer Switch. If you use FTP or SCP for the transfer, you must specify the correct location, **\sec**, on the Automatic Transfer Switch. For SCP, the command to transfer a certificate named **cert.p15** to a Automatic Transfer Switch with an IP address of 156.205.6.185 would be:

```
scp cert.p15 apc@156.205.6.185:\sec\cert.p15
```

Create a Server Certificate and Signing Request

Summary

Use this procedure if your company or agency has its own Certificate Authority or if you plan to use a commercial Certificate Authority to sign your server certificates.

- Create a Certificate Signing Request (CSR).The CSR contains all the information for a server certificate except the digital signature. This process creates two output files:
  - The file with the **.p15** extension contains the Automatic Transfer Switch's private key.
  - The file with the **.csr** extension contains the certificate signing request, which you send to an external Certificate Authority.
- When you receive the signed certificate from the Certificate Authority, import that certificate. Importing the certificate combines the **.p15** file containing the private key and the file containing the signed certificate from the external Certificate Authority. The output file is a new encrypted server certificate file with a **.p15** extension.
- Load the server certificate onto the Automatic Transfer Switch.
- For each Automatic Transfer Switch that requires a server certificate, repeat the tasks that create and load the server certificate.

The procedure

Create the Certificate Signing Request (CSR). Perform these steps. (Click **Next** to move from screen to screen.)

1. If the APC Security Wizard is not already installed on your computer, install it by running the installation program **APC Security Wizard.exe** from the APC Automatic Transfer Switch *Utility* CD.
2. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
3. On the screen labeled Step 1, select **Certificate Request** as the type of file to create.
4. Enter a name for the file that will contain the Automatic Transfer Switch's private key. The file name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. On the screen labeled Step 2, provide the information to configure the certificate signing request (CSR) with the information that you want the signed server certificate to contain. The **Country** and **Common Name** fields are required; the other fields are optional. For the **Common Name** field, enter the IP Address or DNS name of the Automatic Transfer Switch.

Note By default, a server certificate is valid for 10 years from the current date and time, but you can edit the **Validity Period Start** and **Validity Period End** fields.

6. On the next screen, review the summary of the certificate. Scroll downward to view the certificate's unique serial number and fingerprints. To make any changes to the information you provided, click **Back**, and revise the information.

Note

The certificate's subject information and the certificate's issuer information should be identical.

7. The last screen verifies that the certificate signing request has been created and displays the location and name of the file, which has a **.csr** extension.
8. Send the certificate signing request to an external Certificate Authority, either a commercial Certificate Authority or, if applicable, a Certificate Authority managed by your own company or agency.

See also

See the instructions provided by the Certificate Authority regarding the signing and issuing of server certificates.

Import the signed certificate. When the external Certificate Authority returns the signed certificate, perform these steps to import the certificate. This procedure combines the signed certificate and the private key into an SSL server certificate that you then upload to the Automatic Transfer Switch. (Click **Next** to move from screen to screen.)

1. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
2. On the screen labeled Step 1, select **Import Signed Certificate**.
3. Browse to and select the signed server certificate that you received from the external Certificate Authority. The file has a **.cer** or **.crt** extension.
4. Browse to and select the file you created in step 4 of the task, Create a Server Certificate and Signing Request. This file has a **.p15** extension, contains the Automatic Transfer Switch's private key, and, by default, is located in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. Specify a name for the output file that will be the signed server certificate that you upload to the Automatic Transfer Switch. The file must have a **.p15** extension.
6. Click **Next** to generate the server certificate. The certificate's **Issuer Information** on the summary screen confirms that the external Certificate Authority signed the certificate.
7. The last screen verifies that the certificate has been created and instructs you on the next task, to load the server certificate to the Automatic Transfer Switch. It displays the location and name of the server certificate, which has a **.p15** file extension and contains the Automatic Transfer Switch's private key and the public key obtained from the **.cer** or **.crt** file.

Load the server certificate to the Automatic Transfer Switch.

Perform these steps:

1. On the **Network** menu of the Web interface of the Automatic Transfer Switch, select the **Web/SSL** option.
2. In the **SSL/TLS Server Certificate** section of the page, browse to the server certificate, the **.p15** file you created in the procedure Import the signed certificate. (The default location is **C:\Program Files\American Power Conversion\APC Security Wizard**.)

Note

Alternatively, you can use FTP or SCP to transfer the server certificate to the Automatic Transfer Switch. If you use FTP or SCP for the transfer, you must specify the correct location, **\sec**, on the Automatic Transfer Switch. For SCP, the command to transfer a certificate named **cert.p15** to a Automatic Transfer Switch with an IP address of 156.205.6.185 would be:

```
scp cert.p15 apc@156.205.6.185:\sec\cert.p15
```

Create an SSH Host Key

Summary

This procedure is optional. If you select SSH encryption, but do not create a host key, the Automatic Transfer Switch generates a 768-bit RSA key when it reboots. Host keys for SSH that are created with the APC Security Wizard are 1024-bit RSA keys.

- Use the APC Security Wizard to create a host key, which is encrypted and stored in a file with **.p15** extension.
- Load the host key on to the Automatic Transfer Switch.

The procedure

Create the host key. Perform these steps. (Click **Next** to move from screen to screen.)

1. If the APC Security Wizard is not already installed on your computer, install it by running the installation program **APC Security Wizard.exe** from the APC Automatic Transfer Switch *Utility* CD.
2. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
3. On the screen labeled Step 1, select **SSH Server Host Key** as the type of file to create.
4. Enter a name for the file that will contain the host key. The file name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. Click **Next** to generate the Host Key.

6. The summary screen displays the SSH version 1 and version 2 fingerprints, which are unique for each host key and identify the host key. After you load the host key onto the Automatic Transfer Switch, you can verify that the correct host key was uploaded by verifying that the fingerprints displayed here match the SSH fingerprints on the Automatic Transfer Switch, as displayed by your SSH client program.
7. The last screen verifies that the host key has been created and instructs you on the next task, to load the host key to the Automatic Transfer Switch. It displays the location and name of the host key, which has a **.p15** file extension.

Load the host key to the Automatic Transfer Switch. Perform these steps:

1. On the **Network** menu of the Web interface of the Automatic Transfer Switch, select the **Telnet/SSH** option.
2. In the **SSH User Host Key File** section of the page, browse to the host key, the **.p15** file you created in the procedure Create an SSH Host Key. (The default location is **C:\Program Files\American Power Conversion\APC Security Wizard**.)
3. On the **SSH Host Key Fingerprint** section of the page, note the fingerprint for the version (or versions) of SSH you are using. Then log on to the Automatic Transfer Switch through your SSH client program, and verify that the correct host key was uploaded by verifying that these fingerprints match the fingerprints that the client program displays.

Note

Alternatively, you can use FTP or SCP to transfer the host key file to the Automatic Transfer Switch. If you use FTP or SCP for the transfer, you must specify the correct location, **\sec**, on the Automatic Transfer Switch. For SCP, the command to transfer a host key named **hostkey.p15** to a Automatic Transfer Switch with an IP address of 156.205.6.185 would be:

```
scp cert.p15 apc@156.205.6.185:\sec\hostkey.p15
```

APC Device IP Configuration Wizard

Purpose and Requirements

Purpose: configure basic TCP/IP settings

You can use the APC Device IP Configuration Wizard to configure the basic TCP/IP settings (IP address, subnet mask, and default gateway) of the following:

- Network Management Cards
- Devices that contain embedded Network Management Cards

Using the Wizard, you can configure the basic TCP/IP settings of installed or embedded Network Management Cards in either of the following ways:

- Automatically discover and configure unconfigured Network Management Cards remotely over your TCP/IP network.
- Configure or reconfigure a Network Management Card through a direct connection from the serial port of your computer to the device that contains the card.

Note The Wizard can discover and configure Network Management Cards only if they are on the same network segment as the computer that is running the Wizard.

System requirements

The Wizard runs on Windows NT®, Windows 2000, Windows 2003, and Windows XP Intel-based workstations.

Install the Wizard

Automated installation

If autorun is enabled on your CD-ROM drive, the installation program starts automatically when you insert the CD.

Manual installation

If autorun is not enabled on your CD-ROM drive, run **setup.exe** in the Wizard directory on the CD, and follow the on-screen instructions

You can download the latest version of the APC Device IP Configuration Wizard from the APC Web site, **www.apc.com** and run **setup.exe** from the folder to which you downloaded it.

Use the Wizard

Launch the Wizard

The installation creates a shortcut link in the **Start** menu that you can use to launch the Wizard.

Configure the basic TCP/IP settings remotely

Prepare to configure the settings. Before you run the Wizard, be sure that you have the information you will need during the configuration procedure:

1. Contact your network administrator to obtain valid TCP/IP settings to use.
2. If you are configuring multiple unconfigured Network Management Cards, obtain the MAC address of each one so that you can identify each Network Management Card that the Wizard discovers. (The Wizard displays the MAC address for a discovered card on the same screen on which you then enter the TCP/IP settings.)

- For Network Management Cards that you install, the MAC address is on a label on the bottom of the card.
- For embedded Network Management Cards, the MAC address is on a label on the device containing the card — for example, usually on the side of a device that you mount in a rack.

Note You can also obtain the MAC address from the Quality Assurance slip that came with the Network Management Card or with the device containing an embedded Network Management Card.

Run the Wizard to perform the configuration. To discover and configure, over the network, installed or embedded Network Management Cards that are not configured:

1. From the **Start** menu, launch the Wizard. The Wizard automatically detects the first Network Management Card that is not configured.
2. Select **Remotely (over the network)**, and click **Next >**.
3. Enter the TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway**) for the unconfigured Network Management Card identified by the MAC address at the top of the screen. Then click **Next >**.
4. On the **Transmit Current Settings Remotely** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the device that contains the Network Management Card after you transmit the card's settings.
5. Click **Finish** to transmit the TCP/IP settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.
6. The Wizard searches for another installed or embedded but unconfigured Network Management Card. If it finds one, it displays the screen with data entry boxes for the TCP/IP settings of that card.
   - To skip configuring the card whose MAC address is currently displayed, click **Cancel**.
   - To configure the TCP/IP settings of the next card, repeat this procedure beginning at step 4.

Configure or reconfigure the TCP/IP settings locally

To configure a single Network Management Card through a serial connection:

1. Contact your network administrator to obtain valid TCP/IP settings.
2. Connect the serial configuration cable that came with the Network Management Card or with the device that contains an embedded Network Management Card.
   a. Connect one end to an available communications port on your computer. Make sure no other application is using the port.
   b. Connect the other end to the serial port of the card or device.
3. From the **Start** menu, launch the Wizard application.
   – If the Network Management Card is not configured, wait for the Wizard to detect it.
   – If you are assigning basic TCP/IP settings serially to a Network Management Card, click **Next>** to move to the next screen.
4. Select **Locally (through the serial port)**, and click **Next >**.
5. Enter the TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway**) for the Network Management Card. Then click **Next >**.
6. On the **Transmit Current Settings Remotely** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the device that contains the Network Management Card after you transmit the card's settings.
7. Click **Finish** to transmit the TCP/IP settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.
8. If you selected **Start a Web browser when finished** in step 6, you can now configure other parameters through the Web interface of the card or device.

How to Export Configuration Settings

Retrieving and Exporting the .ini file

Summary of the procedure

As an Administrator, you can retrieve a dynamically generated .ini file of an Automatic Transfer Switch's current configuration and export that file to another Automatic Transfer Switch or to multiple Automatic Transfer Switchs.

1. Configure an Automatic Transfer Switch to have the settings you want to export.
2. Retrieve the .ini file from that Automatic Transfer Switch.
3. Customize the .ini file (to change at least the TCP/IP settings) and make a copy to export.
4. Use any of the file transfer protocols supported by the Automatic Transfer Switch to transfer the copied file to one or more additional Automatic Transfer Switches. (To transfer the file to multiple Automatic Transfer Switches simultaneously, write an FTP script that repeats the steps for transferring the file to a single Automatic Transfer Switch.)
5. Each receiving Automatic Transfer Switch stores the file temporarily in its flash memory, uses it to reconfigure its own Automatic Transfer Switch settings, and then deletes the file.

Contents of the .ini file

The config.ini file that you retrieve from an Automatic Transfer Switch contains the following:

- *section headings*, which are category names enclosed in brackets ([ ]), and under each section heading, *keywords,* which are labels describing specific Automatic Transfer Switch settings.

  Note Only section headings and keywords supported for the specific device associated with the Automatic Transfer Switch from which you retrieve the file are included.

- Each keyword is followed by an equals sign and the current *value* for that parameter's setting, either the default value (if the value has not been specifically configured) or the configured value.
  - The `Override` keyword, with its default value, prevents one or more keywords and their device-specific values from being exported.
    - In the `[NetworkTCP/IP]` section, the default value for `Override` (the MAC address of the Automatic Transfer Switch) blocks the exporting of the values for the keywords `SystemIP`, `SubnetMask`, `DefaultGateway`, and `BootMode`.
    - In the UPS section, the default value for `Override` (the UPS serial number) blocks the exporting of the value for the `RatedOutputVoltage` keyword. (`RatedOutputVoltage` and its value are included only in the .ini file only if the output voltage of the UPS is configurable.)
  - You must edit the section `[SystemDate/Time]` if you want to set the system date and time of a receiving Automatic Transfer Switch or cause that Automatic Transfer Switch to use an NTP Server to set its date and time.

    See Customizing for configuration guidelines for date and time settings.

Detailed procedures

Use the following procedures to retrieve the settings of one Automatic Transfer Switch and export them to one or more other Automatic Transfer Switches.

Retrieving. To set up and retrieve an .ini file to export:

1. Configure an Automatic Transfer Switch with the settings you want to export.

   Note To avoid errors, configure the Automatic Transfer Switch by using its Web interface or control console whenever possible. Directly editing the .ini file risks introducing errors.

2. Use FTP to retrieve the file config.ini from the Automatic Transfer Switch you configured:
   a. Open a connection to the Automatic Transfer Switch, using its IP Address. For example:
      ```
      ftp> open 158.165.2.132
      ```
   b. Log on, using the Administrator user name and password configured for the Automatic Transfer Switch.
   c. Retrieve the config.ini file containing the Automatic Transfer Switch's current settings:
      ```
      ftp> get config.ini
      ```
      The file is written to the folder from which you launched FTP.

See also To create batch files and use an APC utility to retrieve configuration settings from multiple Automatic Transfer Switches and export them to other Automatic Transfer Switches, see *Release Notes: ini File Utility, version 1.0* (**.\doc\en\ininotes.pdf**) on the APC Automatic Transfer Switch *Utility* CD.

Customizing. You must customize the file to change at least the TCP/IP settings before you export it.

1. Use a text editor to customize the file.
   - Section headings, keywords, and pre-defined values are not case-sensitive, but string values that you define are case-sensitive.
   - Use adjacent quotation marks to indicate no value. For example, `LinkURL1=""` indicates that the URL is intentionally undefined.
   - To define values, opening and closing quotation marks are optional, except to enclose values that contain leading or trailing spaces or values which are already enclosed in quotation marks. (Leading or trailing spaces not within the opening and closing quotation marks are ignored.)
   - To export a specific system date and time or any scheduled events, you must configure the values directly in the .ini file.
     - To export a specific system time, export only the configured `[SystemDate/Time]` section as a separate .ini file. (The time necessary to export a large file would cause the configured time to be significantly inaccurate.)
     - For greater accuracy, if the Automatic Transfer Switch receiving the file can access a Network Time Protocol (NTP) Server, set the value for the `NTPEnable` keyword as follows:

       ```
       NTPEnable=enabled
       ```
   - Add comments about changes that you made. The first printable character of a comment line must be a semicolon (`;`).

2. Copy the customized file to another file name in the same folder:
   – The copy, which you will export to other Automatic Transfer Switches, can have any file name up to 64 characters and must have the .ini file suffix.
   – Retain the original customized file for future use. **The file that you retain is the only record of your comments.** They are removed automatically from the file that you export.

Exporting the file to a single Automatic Transfer Switch. To export the .ini file to another Automatic Transfer Switch, use any of the file transfer protocols supported by Automatic Transfer Switch (including FTP, FTP Client, SCP, and TFTP). The following example uses FTP:

1. From the folder containing the customized .ini file and its copy, use FTP to log in to the Automatic Transfer Switch to which you are exporting the .ini file. For example:

   ```
   ftp> open 158.165.4.135
   ```

2. Export the copy of the customized .ini file. The receiving Automatic Transfer Switch accepts any file name that has the .ini suffix, is no more than 64 characters in length, and is exported to its root directory.

   ```
   ftp> put filename.ini
   ```

Exporting the file to multiple Automatic Transfer Switches. To export the .ini file to multiple Automatic Transfer Switches:

- Use FTP or SCP, but write a script that incorporates and repeats the steps used for exporting the file to a single Management Card.
- Use a batch processing file and the APC .ini file utility.

See also

To create the batch file and use the utility, see *Release Notes: ini File Utility, version 1.0* (**.\doc\en\ininotes.pdf**) on the APC Automatic Transfer Switch *Utility* CD.

The Upload Event and its Error Messages

The event and its error messages

The following system event occurs when the receiving Automatic Transfer Switch completes using the .ini file to update its settings.

```
Configuration file upload complete, with number valid values
```

This event has no default severity level.

If a keyword, section name, or value is invalid, the event text is extended to include notification of the following errors.

Note The export to and the subsequent upload by the receiving Automatic Transfer Switch succeeds even if there are errors.

Event text	Description
Configuration file warning: Invalid keyword on line *number*. Configuration file warning: Invalid value on line *number*.	A line with an invalid keyword or value is ignored.
Configuration file warning: Invalid section on line *number*.	If a section name is invalid, all keyword/value pairs in that section are ignored.
Configuration file warning: Keyword found outside of a section on line *number*.	A keyword entered at the beginning of the file (i.e., before any section headings) is ignored.
Configuration file warning: Configuration file exceeds maximum size.	If the file is too large, the Automatic Transfer Switch stores and processes what it can, but ignores what it cannot. Reduce the size of the file, or divide it into two files, and try uploading again.

Messages in config.ini

A feature might not be supported for the device from which you retrieve the configuration settings or might not be supported for the device to which you export the configuration settings. In this case, the user configuration file contains, under the section name for that feature, a message stating that the feature is not supported. No keywords and values are listed, and that feature will not be configured on any device to which you export the user configuration file.

Errors generated by overridden values

The `Override` keyword and its value will generate error messages in the event log when it blocks the exporting of values.

See Contents of the .ini file for information about which values are overridden.

The overridden values are device-specific and not appropriate to export to other Automatic Transfer Switches. Therefore, you can ignore these error messages. To prevent these error messages from occurring, you can delete the lines that contain the `Override` keyword and the lines that contain the values that they override. Do not delete or change the line containing the section heading.

Using the Device IP Configuration Wizard

On Windows operating systems, instead of using the preceding procedure for exporting .ini files, you can choose to update Automatic Transfer Switch settings by using the Device IP Configuration Wizard.

For a detailed description of how to update the configuration settings of one or more Automatic Transfer Switches using the Device IP Configuration Wizard, see APC Device IP Configuration Wizard.

File Transfers

Introduction

Overview

The Automatic Transfer Switch automatically recognizes binary firmware files. Each of these files contains a header and one or more Cyclical Redundancy Checks (CRCs) to ensure that the data contained in the file is not corrupted before or during the transfer operation.

When new firmware is transmitted to the Automatic Transfer Switch, the program code is updated and new features become available.

This chapter describes how to transfer firmware files to Automatic Transfer Switches.

Note

To transfer a firmware file to a Automatic Transfer Switch, see Upgrading Firmware.

To verify a file transfer, see Verifying Upgrades and Updates.

Upgrading Firmware

Benefits of upgrading firmware

Upgrading the firmware on the Automatic Transfer Switch has the following benefits:

- New firmware has the latest bug fixes and performance improvements.
- New features become available for immediate use.
- Keeping the firmware versions consistent across your network ensures that all Automatic Transfer Switches support the same features in the same manner.

Firmware files (Automatic Transfer Switch)

A firmware version consists of two modules: An APC Operating System (AOS) module and an application module.

The APC Operating System (AOS) and application module files used with the Automatic Transfer Switch share the same basic format:

`apc_hw0x_type_version.bin`

- `apc`: Indicates that this is an APC file.
- `hw0x`: Identifies the version of the Automatic Transfer Switch that will run this binary file.
- *`type`*: Identifies whether the file is for the APC Operating System (AOS) or the application module (APP) for the Automatic Transfer Switch.
- *`version`*: The version number of the application file. For example, a code of 261 would indicate version 2.6.1.
- `bin`: Indicates that this is a binary file.

Obtain the latest firmware version

Automated upgrade tool for Microsoft Windows systems. An automated self-extracting executable tool combines the firmware modules that you need to automate your upgrades on any supported Windows operating system

- The version of the tool on the APC Automatic Transfer Switch *Utility* CD will upgrade your device to the latest AOS and application modules available when the CD was released.
- If a later firmware upgrade is available, you can obtain an updated version of the tool at no cost from the support section of the APC Web site **www.apc.com/tools/download**. At this Web page, find the latest firmware release for your APC product (in this case, the Automatic Transfer Switch) and download the automated tool, not the individual firmware modules.

If the AOS firmware module you already have is a 1.*x.x* version, the executable tool must perform two consecutive upgrades:

- The first upgrade is from version 1.*x.x* to the latest available 2.0.*x* version of the AOS firmware module.
- The second upgrade is from the 2.0.*x* version to the most recently released version of the AOS module.

The tool therefore contains firmware modules for both upgrades.

Each upgrade tool is specific to an APC product type. Do not use the tool from one product CD to upgrade firmware of a different APC product. If you use a version of the tool from the APC Web site, make sure that you use the upgrade tool that corresponds with your APC product type.

Manual upgrades, primarily for Linux systems. If all computers on your network are running Linux, you must upgrade the firmware of your Automatic Transfer Switches manually, i.e., by using the separate APC firmware modules (AOS module and application module).

If you have a networked computer running a supported Microsoft Windows operating system on your network, you can use the tool described in Automated upgrade tool for Microsoft Windows systems to upgrade the firmware of a Automatic Transfer Switch automatically over the network. This tool automates the entire upgrade process, even if your current firmware is a 1.*x.x* version.

Note

When performing a manual upgrade, not using the automated tool, you cannot upgrade the AOS firmware module of any APC device directly from firmware version 1.*x.x* to firmware version 2.1.0 or later. The upgrade attempt will fail. You must first upgrade to the latest available 2.0.*x* version of the AOS module and then to the later version.

You can obtain the individual firmware modules you need for a manual firmware upgrade from the support section of the APC Web site **www.apc.com/tools/download**.

Firmware file transfer methods

To upgrade the firmware of a Automatic Transfer Switch:

- From a networked computer running a Microsoft Windows operating system, you can use the automated firmware upgrade tool on your CD or downloaded from the APC Web site.
- From a networked computer on any supported operating system, you can use FTP or SCP to transfer the individual AOS and application firmware modules.
- For a Automatic Transfer Switch that is not on your network, you can use XMODEM through a serial connection to transfer the individual AOS and application firmware modules from your computer to the Automatic Transfer Switch.

Note

When you transfer individual firmware modules and do not use the automated firmware upgrade tool to upgrade the firmware for a Automatic Transfer Switch, you must transfer the APC Operating System (AOS) module to the Automatic Transfer Switch before you transfer the application module.

For more information about the firmware modules, see Firmware files (Automatic Transfer Switch).

Use FTP or SCP to upgrade one Automatic Transfer Switch

Instructions for using FTP. For you to be able to use FTP to upgrade a single Automatic Transfer Switch over the network:

- The Automatic Transfer Switch must be connected to the network.
- The FTP server must be enabled at the Automatic Transfer Switch.
- The Automatic Transfer Switch must have its TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway** addresses) configured.

To use FTP to upgrade the Automatic Transfer Switch:

1. Open an MS-DOS command prompt window on a computer that is connected to the network. Go to the directory that contains the firmware upgrade files, and list the files. For the directory `C:\apc`, the commands would be those shown in **bold**:

   ```
   C:\>cd\apc
   C:\apc>dir
   ```

   Files listed for a Automatic Transfer Switch, for example, might be the following:

   – `apc_hw02_aos_264.bin`

   – `apc_hw02_ats_261.bin`

2. Open an FTP client session:

   ```
   C:\apc>ftp
   ```

3. Type `open` and the Automatic Transfer Switch's IP address, and press ENTER. If the **Port** setting for **FTP Server** in the **Network** menu has changed from its default of **21**, you must use the non-default value in the FTP command.
   a. For some FTP clients, use a colon to add the port number to the end of the IP address.
   b. For Windows FTP clients, separate the port number from the IP address by a space. For example, if the Automatic Transfer Switch's **FTP Server Port** setting has been changed from its default of **21**, such as to **21000**, you would use the following command for a Windows FTP client transferring a file to a Automatic Transfer Switch with an IP address of 150.250.6.10.
   ```
   ftp> open 150.250.6.10 21000
   ```
4. Log on using the Administrator user name and password. (**apc** is the default for both.)
5. Upgrade the AOS. For example:
   ```
   ftp> bin
   ftp> put apc_hw02_aos_264.bin
   ```
6. When FTP confirms the transfer, type **quit** to close the session.
7. Wait 20 seconds, and then repeat step 2 through step 6, but in step 6, use the application module file name instead of the AOS module.

Instructions for using SCP. To use SCP to upgrade the firmware for one Automatic Transfer Switch:

1. Identify and locate the firmware modules described in the preceding instructions for FTP.
2. Use an SCP command line to transfer the AOS firmware module to the Automatic Transfer Switch. The following example assumes a Automatic Transfer Switch IP address of 158.205.6.185, and an AOS module of **apc_hw02_aos_264.bin**.)

   ```
   scp apc_hw02_aos_264.bin apc@158.205.6.185:apc_hw02_aos_264.bin
   ```
3. Use a similar SCP command line, with the name of the application module instead of the AOS module, to transfer the application module to the Automatic Transfer Switch.

How to upgrade multiple Automatic Transfer Switches

Export configuration settings. You can create batch files and use an APC utility to retrieve configuration settings from multiple Automatic Transfer Switchs and export them to other Automatic Transfer Switches.

See also

See *Release Notes: ini File Utility, version 1.0* (**.\doc\en\ininotes.pdf**) on the APC Automatic Transfer Switch *Utility* CD.

Use FTP or SCP to upgrade multiple Automatic Transfer Switches. To upgrade multiple Automatic Transfer Switches using an FTP client or using SCP, write a script which automatically performs the procedure. For FTP, use the steps in Use FTP or SCP to upgrade one Automatic Transfer Switch.

Use XMODEM to upgrade one Automatic Transfer Switch

Note

You cannot upgrade the AOS firmware module of any APC device directly from firmware version 1.*x.x* to 2.1.0 or later. The upgrade attempt will fail.

To upgrade the AOS firmware module of an APC device from version 1.*x.x* to 2.1.0 or later, first upgrade the module to the latest available version 2.0.*x* AOS firmware module. Then upgrade it again, this time from version 2.0.*x* to the 2.*x.x* version you want.

If your APC device is running a 2.0.*x* of the AOS firmware module already, you can upgrade directly to version 2.1.0 or a later version.

To use XMODEM to upgrade the firmware for a single Automatic Transfer Switch that is not on the network:

1. Obtain the individual firmware modules (the AOS module and the application module) from the support section of the APC Web site **www.apc.com/tools/download**.
2. Select a serial port at the local computer, disable any service which uses that port, and connect the smart-signaling cable that came with the Automatic Transfer Switch to the selected port and to the serial port at the Automatic Transfer Switch.
3. Run a terminal program (such as HyperTerminal), and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control, and save the changes.
4. Press ENTER to display the **User Name** prompt.
5. Enter your Administrator user name and password. The default for both is **apc**.
6. Start an XMODEM transfer:

a. Select option 3—**System**

b. Select option 4—**File Transfer**

c. Select option 2—**XMODEM**

d. Type `Yes` at the prompt to continue with the transfer.

7. Select the appropriate baud rate. A higher baud rate causes faster firmware upgrades. Also, change the terminal program's baud rate to match the one you selected, and press ENTER.
8. From the terminal program's menu, select the binary AOS file to transfer via XMODEM-CRC. After the XMODEM transfer is complete, set the baud rate to 9600. The Automatic Transfer Switch will automatically restart.
9. Repeat step 3 through step 8 to install the application module. In step 8, substitute the application module file name for the AOS module file name.

For information about the format used for application modules, see Firmware files (Automatic Transfer Switch).

Verifying Upgrades and Updates

Overview

To verify that the firmware upgrade was successful, see the **Last Transfer Result** message, available through the **FTP Server** option of the **Network** menu (in the control console only), or use an SNMP GET to the **mfiletransferStatusLastTransferResult** OID.

Last transfer result codes

Code	Description
Successful	The file transfer was successful.
Result not available	There are no recorded file transfers.
Failure unknown	The last file transfer failed for an unknown reason.
Server inaccessible	The TFTP or FTP server could not be found on the network.
Server access denied	The TFTP or FTP server denied access.
File not found	The TFTP or FTP server could not locate the requested file.
File type unknown	The file was downloaded but the contents were not recognized.
File corrupt	The file was downloaded but at least one CRC was bad.

You can also verify the versions of the upgraded APC Operating System (AOS) and application modules by using the **About System** option in the **System** menu of the control console or in the **Help** menu of the Web interface, or by using an SNMP GET to the MIB II **sysDescr** OID.

Troubleshooting

Management Card

Management Card access problems

For problems that are not described in the following table, see SNMP problems. If you still cannot resolve the problem, see Obtaining service.

Problem	Solution
Unable to ping the Management Card	If the Management Card's Status LED is green, try to ping another node on the same network segment as the Management Card. If that fails, it is not a Management Card problem. If the Status LED is not green, or if the ping test succeeds, perform the following checks: • Verify all network connections. • Verify the IP addresses of the Management Card and the NMS. • If the NMS is on a different physical network (or subnetwork) from the Management Card, verify the IP address of the default gateway (or router). • Verify the number of subnet bits for the Management Card's subnet mask.
The terminal program cannot allocate the communications port when you try to configure the Management Card	Before you can use a terminal to configure the Management Card, you must shut down any application, service, or program using the communications port.

Problem	Solution
Cannot access the control console through a serial connection	Make sure that you did not change the baud rate. Try 2400, 9600, 19200, or 38400.
Cannot access the control console remotely	• Make sure you are using the correct access method (Telnet or SSH). An Administrator can enable these access methods through the **Telnet/SSH** option of the **Network** menu. By default, Telnet is enabled. Enabling SSH automatically disables Telnet. • For Secure SHell (SSH), the Management Card may be creating a host key. The Management Card can take up to 5 minutes to create this host key, and SSH is not accessible during that time.
Cannot access the Web interface	• Verify that HTTP or HTTPS access is enabled. • Make sure you are specifying the correct URL — one that is consistent with the security system used by the Management Card. SSL requires https, not http, at the beginning of the URL. • Verify that you can ping the adapter. • Verify that you are using a Web browser that is supported for the Network Management Card. See Supported Web browsers. • If the Network Management Card has just restarted and SSL security is being set up, the Management Card may be generating a server certificate. The Management Card can take up to 5 minutes to create this certificate, and the SSL/TLS server is not available during that time.

SNMP problems

Problem	Solution
Unable to perform a GET	• Verify the read (GET) community name. • Use the control console or Web interface to ensure that the NMS has access. See SNMP.
Unable to perform a SET	• Verify the read/write (SET) community name. • Use the control console or Web interface to ensure that the NMS has write (SET) access. See SNMP.
Unable to receive traps at the NMS	Query the **mconfigTrapReceiverTable** PowerNet MIB OID to check whether the NMS IP address is listed correctly and whether the community name defined for the NMS matches the community name in the table. Use SETs to the **mconfigTrapReceiverTable** OIDs, or use the control console or Web interface to make any necessary corrections. See SNMP.
Traps received at an NMS are not identified	See your NMS documentation to verify that the traps are properly integrated in the alarm/trap database.

Product Information

Warranty and Service

Limited warranty

APC warrants the Automatic Transfer Switch and Network Management Card to be free from defects in materials and workmanship for a period of two years from the date of purchase. Its obligation under this warranty is limited to repairing or replacing, at its own sole option, any such defective products. This warranty does not apply to equipment that has been damaged by accident, negligence, or misapplication or has been altered or modified in any way. This warranty applies only to the original purchaser.

Warranty limitations

Except as provided herein, APC makes no warranties, expressed or implied, including warranties of merchantability and fitness for a particular purpose. Some jurisdictions do not permit limitation or exclusion of implied warranties; therefore, the aforesaid limitation(s) or exclusion(s) may not apply to the purchaser.

Except as provided above, in no event will APC be liable for direct, indirect, special, incidental, or consequential damages arising out of the use of this product, even if advised of the possibility of such damage.

Specifically, APC is not liable for any costs, such as lost profits or revenue, loss of equipment, loss of use of equipment, loss of software, loss of data, costs of substitutes, claims by third parties, or otherwise. This warranty gives you specific legal rights and you may also have other rights, which vary according to jurisdiction.

Obtaining service

To obtain support for problems with your Automatic Transfer Switch and Network Management Card :

1. Note the serial number and date of purchase. In the Web interface, see the **Status** option of the **Automatic Transfer Switch** menu and the **About System** option of the **Help** menu for serial numbers.
2. Contact Customer Support at a phone number located at the end of this manual. A technician will try to help you solve the problem by phone.
3. If you must return the product, the technician will give you a return material authorization (RMA) number. If the warranty expired, you will be charged for repair or replacement.
4. Pack the unit carefully. The warranty does not cover damage sustained in transit. Enclose a letter with your name, address, RMA number and daytime phone number; a copy of the sales receipt; and a check as payment, if applicable.
5. Mark the RMA number clearly on the outside of the shipping carton.
6. Ship by insured, prepaid carrier to the address provided by the Customer Support technician.

Warning Do not attempt to remove the Management Card. The terms of your warranty require that service be performed by an authorized APC technician only.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

T

U

V

W

X

APC Worldwide Customer Support

Customer support for this or any other APC product is available at no charge in any of the following ways:

- Visit the APC Web site to access documents in the APC Knowledge Base and to submit customer support requests.
  - **www.apc.com** (Corporate Headquarters)

    Connect to localized APC Web sites for specific countries, each of which provides customer support information.
  - **www.apc.com/support/**

    Global support searching APC Knowledge Base and using e-support.
- Contact an APC Customer Support center by telephone or e-mail.
  - Regional centers:

Direct InfraStruXure Customer Support Line	(1)(877)537-0607 (toll free)
APC headquarters U.S., Canada	(1)(800)800-4272 (toll free)
Latin America	(1)(401)789-5735 (USA)
Europe, Middle East, Africa	(353)(91)702000 (Ireland)
Japan	(0) 35434-2021
Australia, New Zealand, South Pacific area	(61) (2) 9955 9366 (Australia)

  - Local, country-specific centers: go to **www.apc.com/support/contact** for contact information.

Contact the APC representative or other distributor from whom you purchased your APC product for information on how to obtain local

Copyright

990-1240B-001 **12/2004**