Contents

ADDENDUM
NetworkAIR ACPA4000

Network Management Card Wizard

Introduction

Overview

The APC Network Management Card Wizard is a Microsoft® Windows® application that pre-configures and reconfigures single or multiple Management Cards of APC devices.

> **Note**
> You cannot use the Wizard to upgrade the firmware for a Management Card. Instead, use FTP, SCP, or XMODEM. See Upgrading Firmware.

The Wizard works locally through the serial port of your computer or remotely over your TCP/IP network. Using the Wizard to configure the Network Management Cards of your NetworkAIR PA Portable Air Conditioners, you can do the following:

- Automatically discover unconfigured Network Management Cards remotely or locally
- Initially configure multiple Network Management Cards
- Reconfigure multiple Network Management Cards after they are deployed

> **Note**
> Not all features in the user interface of the Network Management Card Wizard are supported for NetworkAIR PA Portable Air Conditioners. Use only the features documented in this addendum.

System requirements

The Wizard runs on Windows® 98, Windows NT®, Windows 2000, Windows 2003, and Windows XP Intel-based workstations.

> **Note**
>
> The Network Management Card Wizard uses FTP to transfer files. If you are using Secure CoPy (SCP) and have disabled the FTP server, you must temporarily enable it to use the Wizard to configure settings of a Network Management Card.

Configuring Network Management Card settings

Using the Wizard, you can configure basic settings locally or remotely for the Network Management Cards. The Wizard cannot configure the following settings for the Network Management Card:

- Event action settings
- Email settings
- DNS settings

Installing the Wizard

If autorun is enabled on your CD drive, a page will open automatically in your browser when the CD is inserted. Navigate to the Management Card Wizard page, and select **Install the Wizard**. Otherwise, run the **setup.exe** installation program found in the Wizard directory and follow the on-screen instructions. During installation, a shortcut link is created in the **Start** menu. Use this link to launch the Wizard application.

Online Help

To access the Wizard's online help, click **Help** at the lower left on the Wizard screen.

APC

(!) Note The Wizard is used with many APC devices, and some features described in the online help are not available with NetworkAIR PA Air Conditioners.

Quick configuration of the required settings

You can configure the required TCP/IP settings quickly using the Wizard.

See Configuring the required TCP/IP settings.

Initially configuring Management Cards of NetworkAIR PA Air Conditioners

To configure Network Management Cards initially, use the Wizard to configure the settings of each Management Card locally.

See Pre-configuring the Network Management Card.

ADDENDUM
NetworkAIR ACPA4000

APC

Reconfiguring multiple Network Management Cards

To reconfigure multiple Network Management Cards:

1. Deploy your NetworkAIR PA Portable Air Conditioners without any pre-configuration.

2. Configure the TCP/IP settings of each NetworkAIR PA Air Conditioner remotely through auto-discovery of its Management Card.

    See Configuring the required TCP/IP settings.

    See also The Network Management Cards can also use a DHCP server to assign the TCP/IP settings. See the Boot Mode description in the NetworkAIR ACPA4000 *User's Guide* (**990-1702-EN.pdf**) on the *Utility* CD.

3. Reconfigure other settings of the Management Cards of NetworkAIR PA Air Conditioners remotely.

    See Reconfiguring deployed Network Management Cards. **To perform this procedure, the FTP server must be enabled.**

ADDENDUM

NetworkAIR ACPA4000

APC

4

Using the Network Management Card Wizard

Configuring the required TCP/IP settings

To configure the Network Management Card's required TCP/IP settings remotely:

1. Contact your network administrator to obtain valid TCP/IP settings.

2. From the **Start** menu, launch the Wizard application. The Wizard automatically detects any unconfigured Network Management Cards.

3. Select the **Express (Recommended)** option from the "Installation Options" screen, and then click **Next >**.

4. Select the **Remotely (over the Network)** option from the "Express Configuration" screen, and then click **Next >**.

5. When the Wizard prompts you for the TCP/IP settings, configure the settings (**System IP**, **Subnet Mask**, and **Default Gateway** addresses).

6. Select the **Start a Web browser when finished** option to connect over the Web to the NetworkAIR PA Portable Air Conditioner. This launches the default Web browser. Click **Finish** and wait for a few seconds to let the Management Card restart, which will not interrupt power to the air conditioner.

7. After you enter the correct, IP-formatted information, click **Finish** to transmit the TCP/IP settings. The Wizard checks to see if the System IP address you entered is in use on the network. If it is discovered as an IP address in use, enter a valid IP address, click **Finish**, and follow the on-screen instructions.

ADDENDUM

NetworkAIR ACPA4000

APC

Pre-configuring the Network Management Card

To pre-configure the Network Management Card:

1. Use the link in the **Start** menu to launch the Wizard application, and then click **Next >** on the opening screen.

2. Select the **Custom (Advanced)** option from the "Installation Options" screen, and then click **Next >**.

3. Select the **Define a New Configuration File (Typical)** option from the "Custom Installation" screen, and then click **Next >**.

4. Configure your network settings. At a minimum, you must configure the TCP/IP settings (**System IP**, **Subnet Mask,** and **Default Gateway** addresses). As long as the Network Management Card's TCP/IP settings are configured before deployment, the Network Management Card can be reconfigured remotely at a later time.

> **(!) Note** If you intend to use the Wizard to reconfigure Network Management Cards, do not disable **FTP Server Access**.

5. Click **Next >** as many times as needed to cycle through the Network Management Card's settings. Bypass any setting that you do not want to configure.

6. Stop at the "Customize the settings that will be transmitted to the Management Card" screen. Choose to transmit the TCP/IP settings (**System IP**, **Subnet Mask**, **Default Gateway** addresses, and **BOOTP**) and any additional options you want to configure, then click **Next >**.

7. Verify the selections you have made on the "Configuration Summary" screen. You can save or print the settings. If you save the settings, you can load them into the Wizard at a later time. Click **Next >**.

8. Select the **Locally (via serial port)** option from the "Transmit Current Settings" screen, and then click **Next >**.

9. Follow the on-screen instructions.

   a. Click **Apply** to transmit the new settings to the Management Card of the NetworkAIR PA Portable Air Conditioner. You will be prompted when the transmission is complete or if there was a communications failure.

   b. To define the TCP/IP settings for the next Management Card that you want to configure, click **Rewind** on the "Transmit Settings Locally" screen.

Reconfiguring deployed Network Management Cards

> ⓘ **Note** **To perform this procedure, the FTP server must be enabled.**

1. Use the link in the **Start** menu to launch the Wizard application, and then click **Next >** on the opening screen.

2. Select the **Custom (Advanced)** option from the "Installation Options" screen, and then click **Next >**.

3. Select the **Define a New Configuration File (Typical)** option from the "Custom Installation" screen, and then click **Next >**.

4. Click **Next >** as many times as needed to cycle through the Network Management Card's settings. Bypass any setting that you do not want to configure.

> ⓘ **Note** Because the Wizard uses FTP to reconfigure Network Management Cards, do not disable **FTP Server Access**.

5. Stop at the "Customize the settings that will be transmitted to the Management Card" screen, and choose the settings to transmit to the Network Management Cards. (Choose only settings that are generic across multiple Network Management Cards.) Then click **Next >**.

> ⓘ **Note** Deselect the **TCP/IP** settings (**System IP**, **Subnet Mask**, **Default Gateway** addresses, and **BOOTP**) and **FTP Server Access** settings so that they will not overwrite these settings when you transfer the new settings.

6. On the "Configuration Summary" screen, verify the selections you made.

> Be sure that you select only settings that you want to reconfigure so that you do not accidentally overwrite settings of the deployed Network Management Card. All settings that have **YES** in the **Send** column of the "Configuration Summary" screen will be transmitted.
>
> **Note**

   Click the appropriate buttons to save and print the summary. If you save the settings, you can load them into the Wizard later. Click **Next >**.

7. Select the **Remotely (over network via FTP Server)** option from the "Transmit Current Settings" screen, and then click **Next >**.

8. On the "Remote File Transfer" screen, add the IP addresses of the Network Management Cards that you want to reconfigure. If the deployed Network Management Cards have different settings for the Administrator **User Name**, **Password**, and **FTP Server Port**, change the values reflected in the Wizard. If you have a saved list of Network Management Card IP addresses, you can load them by clicking **Load…**. Click **Next >** to continue.

9. Click **Apply** in the "Remote File Transfer via FTP" screen to transmit the new settings to all of the Network Management Cards specified in the preceding step. After you transmit the settings to all of the Network Management Cards, a transmission log is available. To save, print, or clear the log, click the appropriate button.

Introduction

Overview

The Network Management Card 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 Network Management Card, the program code is updated and new features become available.

This chapter describes how to transfer firmware files to Network Management Cards of NetworkAIR PA Portable Air Conditioners.

To transfer a firmware file to a Network Management Card, see Upgrading Firmware.

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

Upgrading Firmware

Firmware defined

Broadly defined, firmware is highly specialized, reliable software that resides on a memory chip within a computer or computer-related device.

The firmware allows the Management Card to manage the NetworkAIR PA Portable Air Conditioner.

Benefits of upgrading firmware

Upgrading the firmware on the Network Management Card 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 Network Management Cards support the same features in the same manner.

APC

Obtain the latest firmware version

To determine if updated firmware is available to download, go to the "Software Downloads" page, **www.apc.com/tools/download**, on the APC Web site.

The firmware upgrade consists of the two modules: An APC Operating System (AOS) module and an application module.

See Firmware files (Network Management Card).

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 firmware version 2.0.1. Then upgrade it again, this time from version 2.0.1 to the 2.*x.x* version you want.

If your APC device is running version 2.0.1 of the AOS firmware module already, you may upgrade directly to version 2.1.0 or a later version.

Firmware files (Network Management Card)

The APC Operating System (AOS) and application module files used with the Network Management Card share the same basic format:

`apc_hw0x_type_version.bin`

- `apc`: Indicates that this is an APC file.
- `hw0x`: Identifies the version of the Network Management Card that will run this binary file.
- `type`: Identifies whether the file is for the APC Operating System (AOS) or the application module (APP) for a NetworkAIR PA Portable Air Conditioner that connects to the network through the Network Management Card.
- `version`: The version number of the application file. For example, a code of 220 would indicate version 2.2.0.
- `bin`: Indicates that this is a binary file.

> **Note**
> For the most recent versions of the AOS and application modules for the Network Management Card, go to the "Software Downloads" page, **www.apc.com/tools/download**, on the APC Web site.

Firmware file transfer methods

You can use FTP or SCP to upgrade the firmware of one or more Network Management Cards over the network.

You can use XMODEM to upgrade the firmware for a Network Management Card that is not on the network.

When you use FTP, SCP, or XMODEM to upgrade the firmware for a Network Management Card, the APC Operating System (AOS) module must be transferred to the Network Management Card before you transfer the application module.

For more information about the firmware modules, see Firmware files (Network Management Card).

Use FTP or SCP to upgrade one Network Management Card

For you to be able to use FTP to upgrade a single Network Management Card over the network:

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

To use FTP to upgrade the Network Management Card:

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 Network Management Card, for example, might be the following:

- `apc_hw02_aos_228.bin`
- `apc_hw02_nairpa_106.bin`

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, use the firmware upgrade tool, a self-extracting executable file available on the NetworkAIR PA *Utility* CD or available at no cost from the support section of the APC web site (**www.apc.com/support**).

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.

If your APC device is running version 2.0.1 or later of the AOS firmware module already, you may upgrade directly to a later 2.*x.x* version 2.1.0 or a later version.

2. Open an FTP client session:

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

3. Type `open` 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 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 Network Management Card'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 Network Management Card 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_225.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 for the application module. In step 6, use the application module file instead of the AOS module.

To use Secure CoPy (SCP) to upgrade the firmware for one Network Management Card:

1. Identify and locate the firmware modules described in the preceding instructions for FTP.

    > **(!) 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, use the firmware upgrade tool, a self-extracting executable file available on the NetworkAIR PA *Utility* CD or available at no cost from the support section of the APC web site (**www.apc.com/support**).
    >
    > 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.
    >
    > If your APC device is running version 2.0.1 or later of the AOS firmware module already, you may upgrade directly to a later 2.*x.x* version 2.1.0 or a later version.

2. Use an SCP command line to transfer the AOS firmware module to the Network Management Card. The following example assumes a Network Management Card IP address of 158.205.6.185, and an AOS module of **apc_hw02_aos_225.bin**.)

    ```
    scp apc_hw02_aos_225.bin apc@158.205.6.185:apc_hw02_aos_225.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 Network Management Card.

Use FTP or SCP to upgrade multiple Network Management Cards

To upgrade multiple Network Management Cards 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 Network Management Card.

Use XMODEM to upgrade one Network Management Card

> **(!) 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 firmware version 2.0.1. Then upgrade it again, this time from version 2.0.1 to the 2.*x.x* version you want.
>
> If your APC device is running version 2.0.1 of the AOS firmware module already, you may upgrade directly to version 2.1.0 or a later version.

To use XMODEM to upgrade the firmware for a single Network Management Card that is not on the network:

1. Select a serial port at the local computer and disable any service which uses that port.
2. Connect the smart-signaling cable that came with the NetworkAIR PA Portable Air Conditioner to the selected port on your computer and to the serial port on the back of the NetworkAIR PA Portable Air Conditioner.

3. Run a terminal program (such as HyperTerminal®), and configure the selected port for 2400 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 2400. The Network Management Card 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 (Network Management Card).

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.

Updating Configuration Settings

Methods

The Management Card stores its configuration settings internally. These include TCP/IP, TFTP, SSL, SCP, FTP, Web, Device Manager, password, and system settings.

To edit or update the configuration settings for the Management Card, use Telnet, the Web interface, SNMP, or the Wizard.

Using Telnet or Web interfaces

Log on to either the Web interface or the control console of the NetworkAIR PA Portable Air Conditioner. Any setting that can be edited can be changed in these interfaces.

Using SNMP

Use SNMP to perform SETs. However, when you use SNMP, only settings which have OIDs in the MIB defined as read-write can be edited.

Using the Wizard (summary)

For a detailed description of how to update the configuration settings of one or more Management Cards, see Reconfiguring deployed Network Management Cards. The following summary does not include many of the available options.

To update the configuration settings for one or more NetworkAIR PA Portable Air Conditioners using the Wizard:

1. Install (if necessary) and run the Wizard (included on the NetworkAIR PA Portable Air Conditioner).

    See Installing the Wizard.

2. If you have a saved **.ini** file, load it and change any settings as needed. You can also create and save new settings.

3. Click **Finish**.

4. Select the settings you want to transmit to the Management Card, and then click **Next >**.

5. You can view, print, and save your new settings. When finished, click **Next >**.

6. Choose the **Network (via FTP)** option, and then click **Next >**.

7. If you have saved a list of Management Card IP addresses, load that list now. If you do not have a saved list, enter the IP addresses of the Management Cards that you want to receive the configuration settings. Enter the **FTP Server Port** and Administrator user name and password of the Management Cards to which you are transmitting the settings.

8. Save the new IP address list, and then click **Next >**.

9. Click **Apply** to transmit the configuration settings to all of the specified Management Cards. You can save, print, or clear the window containing the download results.

    To verify the update, see Verifying Upgrades and Updates.

Using the APC Security Wizard

Overview

Authentication

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

- Secure Socket 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 Network Management Card.

- Secure SHell (SSH), used for remote terminal access to the Network Management Card'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 Network Management Card, contain a set of CA root certificates from all of the commercial Certificate Authorities.

Authentication of the server (in this case, the Network Management Card) 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 Network Management Card with SSL enabled must have a server certificate on the Network Management Card itself.
- Any browser that is used to access the Network Management Card'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 Network Management Card 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 Network Management Card.)

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

ADDENDUM
NetworkAIR ACPA4000

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 Network Management Card, 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 Network Management Card when you log on to the control console interface.

> **Note**
> All public keys for SSL certificates and all host keys for SSH that are 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 Network Management Card 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 Network Management Card, 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 Network Management Cards. 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 Network Management Card so that the browser can validate the server certificate of the Network Management Card.
- 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 Network Management Card.
- For each Network Management Card that requires a server certificate, repeat the tasks that create and load the server certificate.

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 NetworkAIR PA Portable Air Conditioner *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 Network Management Card.

Load the CA root certificate to your browser. Load the **.crt** file to the browser of each user who needs to access the Network Management Card.

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 (Network Management Card). 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 Network Management Card. It displays the location and name of the Server Certificate, which has a **.p15** file extension and contains the Network Management Card private key and public root certificate.

Load the server certificate to the Network Management Card.

Perform these steps:

1. On the **Network** menu of the Web interface of the Network Management Card, 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 Secure CoPy (SCP) to transfer the server certificate to the Network Management Card. If you use FTP or SCP for the transfer, you must specify the correct location, **\sec**, on the Network Management Card. For SCP, the command to transfer a certificate named **cert.p15** to a Network Management Card 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 Network Management Card'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 Network Management Card.
- For each Network Management Card 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 NetworkAIR PA Portable Air Conditioner *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 Network Management Card'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 Network Management Card.

> **①**
> **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.

> **①**
> **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 the instructions provided by the Certificate Authority regarding the signing and issuing of server certificates.

See also

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 Network Management Card. (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 the Certificate Signing Request (CSR). This file has a **.p15** extension, contains the Network Management Card'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 Network Management Card. 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 Network Management Card. It displays the location and name of the server certificate, which has a **.p15** file extension and contains the Network Management Card's private key and the public key obtained from the **.cer** or **.crt** file.

Load the server certificate to the Network Management Card.

Perform these steps:

1. On the **Network** menu of the Web interface of the Network Management Card, 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 Secure CoPy (SCP) to transfer the server certificate to the Network Management Card. If you use FTP or SCP for the transfer, you must specify the correct location, **\sec**, on the Network Management Card. For SCP, the command to transfer a certificate named **cert.p15** to a Network Management Card 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 Network Management Card 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 onto the Network Management Card.

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 NetworkAIR PA Portable Air Conditioner *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 Network Management Card,

you can verify that the correct host key was uploaded by verifying that the fingerprints displayed here match the SSH fingerprints on the Network Management Card, 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 Network Management Card. It displays the location and name of the host key, which has a **.p15** file extension.

Load the host key to the Network Management Card. Perform these steps:

1. On the **Network** menu of the Web interface of the Network Management Card, 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 the 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 Network Management Card 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 Secure CoPy (SCP) to transfer the host key file to the Network Management Card. If you use FTP or SCP for the transfer, you must specify the correct location, **\sec**, on the Network Management Card. For SCP, the command to transfer a host key named **hostkey.p15** to a Network Management Card with an IP address of 156.205.6.185 would be:

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

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 customer support.

Copyright

990-1871   **03/2004**

ADDENDUM
NetworkAIR ACPA4000

APC