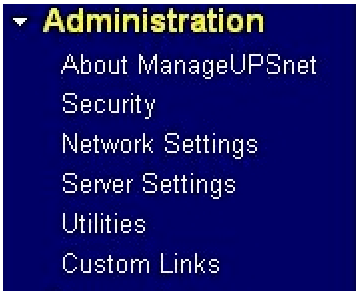
SECTION IV:

ADMINISTRATIVE SETTINGS

OVERVIEW OF ADMINISTRATION

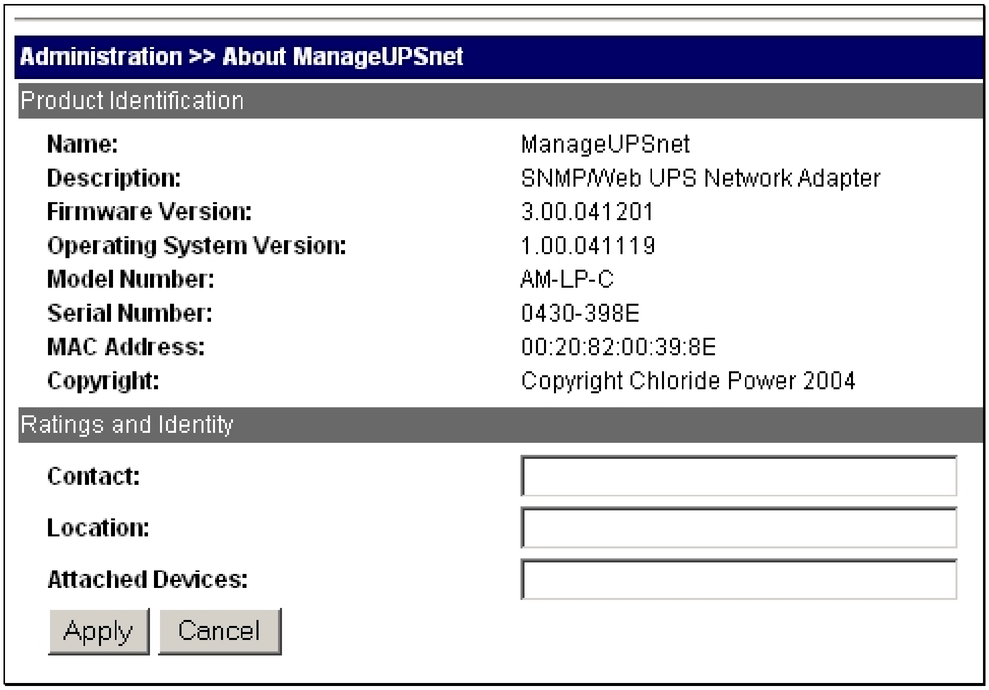
The *Administration* area contains menus and utilities for setting identity information, network parameters (covered in Section II), security and firmware maintenance.



About ManageUPS

The *Product Identification* area contains information that is useful when contacting your vendor for technical support.

Ratings and Identity contains standard variables required in most SNMP applications.



Administration >> About ManageUPSnet

Product Identification

Name:	ManageUPSnet
Description:	SNMP/Web UPS Network Adapter
Firmware Version:	3.00.041201
Operating System Version:	1.00.041119
Model Number:	AM-LP-C
Serial Number:	0430-398E
MAC Address:	00:20:82:00:39:8E
Copyright:	Copyright Chloride Power 2004

Ratings and Identity

Contact:	
Location:	
Attached Devices:	

PRODUCT IDENTIFICATION

Name : Product Model Name.

Firmware Version: Version of the ManageUPS *services* package that contains the device monitoring agent(s) along with related services and clients.

Operating System Version: Version of the ManageUPSNET Operating System.

Model Number: Adapter Model Number / Part Number.

Serial Number: Adapter Serial Number is a 4 digit date code followed by the last 4 digits of the MAC ID.

MAC Address: Adapter MAC Address

RATINGS AND IDENTITY

Contact: The system Contact name for this UPS.
(This value is returned as the `sysContact` object in SNMP MIB-II)

Location: Location of the UPS.
(This value is returned as the `sysLocation` object in SNMP MIB-II).

Attached Devices: Brief description of devices attached to the UPS.
(This value is returned as the `upsIdentAttachedDevices` object in the UPS MIB - RFC1628)

Security Settings

The security provided by ManageUPS is generally adequate for most applications that operate within a protected intranet environment.

However, you should be aware that **usernames, passwords and SNMP community names are transmitted over the network in plain text.**

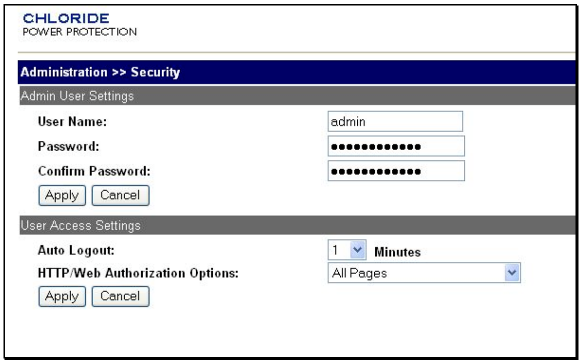
Authentication and User Access control options are explained below.

For further security, you may want to disable services that you are not using. You may also want to change the "well-known ports" assignments used for enabled services to "hide" these services from casual users on the network.
(See *Server Settings* on the following page for more information)

USER SETTINGS

UserName and password required for authentication when accessing the adapter via Web, Telnet, FTP or serial communication methods.

SNMP security is controlled using SNMP Communities. (See Messaging, SNMP Communities)



CHLORIDE
POWER PROTECTION

Administration >> Security

Admin User Settings

User Name: admin

Password: ••••••••••••

Confirm Password: ••••••••••••

User Access Settings

Auto Logout: 1 Minutes

HTTP/Web Authorization Options: All Pages

USER ACCESS SETTINGS

Controls the duration authentication lasts when there is no session activity and determines what can be viewed or changed by non-authenticated users accessing the adapter via WEB Browser.

AUTO LOGOUT:

This security feature will automatically log a user off of HTTP, Telnet or FTP when the session is idle for the specified amount of minutes.

HTTP/WEB AUTHORIZATION OPTIONS:

The following options are available:

All Pages: Use this option if each page requires authentication.

Only Posts: This option allows anyone to view all pages (except the **Security** page) but requires authentication for posting information to the adapter (i.e. pressing the Apply button).

Disable All Authorization: Use this option to allow anyone to view or save information to the adapter without authentication. This is option is not recommended in most cases.

NOTE: ManageUPS allows three successive authentication attempts. If the username and password combination is not entered correctly after three attempts, the card will refuse further attempts and you will see the message:

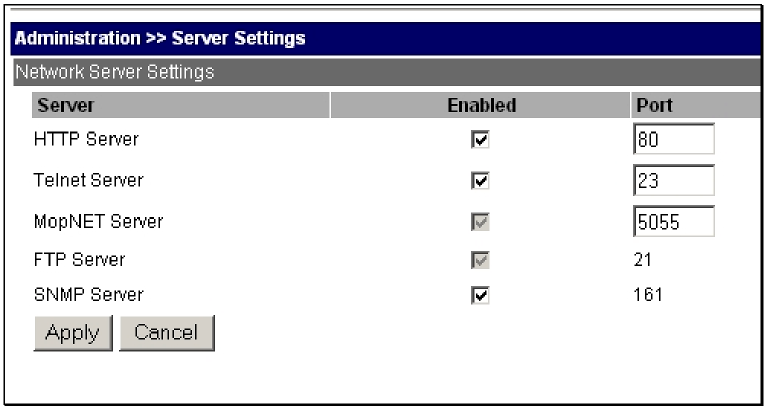
```
HTTP/1.1 401

Unauthorized
```

You will need to restart your WEB, FTP or Telnet session to try again with the correct combination.

Server Settings

Settings of the network *servers* hosted by the adapter.

For greater security, use these controls to change port settings or disable any servers you are not using.



Administration >> Server Settings

Network Server Settings

Server	Enabled	Port
HTTP Server	☑	80
Telnet Server	☑	23
MopNET Server	☑	5055
FTP Server	☑	21
SNMP Server	☑	161

Server: Name of the server/service on the adapter..

Enable: Enables/Disables server.

If you disable the SNMP server -- all SNMP services will be disabled. The adapter will no longer accept SNMP get or set requests and will no longer send SNMP traps.

If you disable the http server, the adapter will no longer respond to browser access requests.

If you disable the telnet server, the adapter will no longer accept incoming connections via telnet.

Port: The default port settings for these servers are the "well-known" ports for a specific protocol. If an arbitrary port is used (between 5000 and 65535), you can effectively "hide" the server on the network. This provides an additional level of security since the port must be known by the user when attempting to connect to the server with client software.

(NOTE: If you change the port setting in a server, you will also need to use the new port setting when accessing the server with a client. For example, if you change the http server port to "8080", then, the syntax you use in your browser address bar would need to identify the non-standard port:

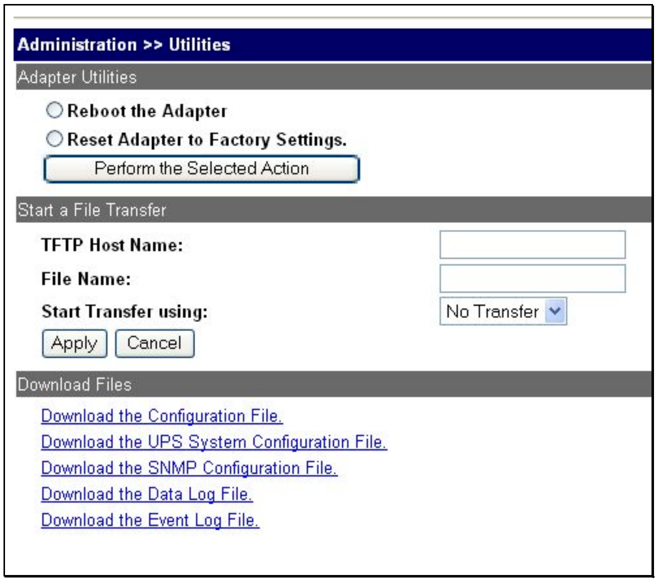
```
http://[manageupsDNSName]:8080
```

Changing ports can have unexpected consequences. Some ports have standard assignments for use with specific network services. And, depending on your network security policies, some ports may be blocked at routers or firewalls. If you feel the need to change ports from the default values, you should consult with your network administrator.

The *FTP* and the *mopnet* servers cannot be disabled.

Utilities

The *Utilities* menus offer mechanisms for setting certain configuration parameters in the adapter and for managing various files in the adapter.



Administration >> Utilities

Adapter Utilities

○ Reboot the Adapter

○ Reset Adapter to Factory Settings.

Perform the Selected Action

Start a File Transfer

TFTP Host Name:

File Name:

Start Transfer using: No Transfer

Apply Cancel

Download Files

Download the Configuration File.

Download the UPS System Configuration File.

Download the SNMP Configuration File.

Download the Data Log File.

Download the Event Log File.

REBOOT / RESET UTILITIES

Reboot the Adapter:

This will cause the adapter to perform a reboot. This is required to cause system changes such as a change to the IP Address to take effect. (See also, *Hardware Reset* -- below)

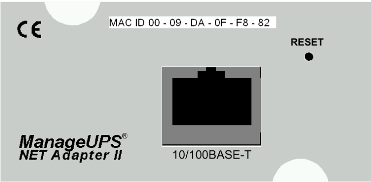
Reset the Adapter:

This will cause all settings on the adapter to be reset to their factory default values.

Note that this will reset all passwords and other user-specific settings. If you want to save some settings, download and save the configuration files before resetting the card. You may be able to edit the saved configuration files to upload specific settings you want to retain.

HARDWARE RESET

There is a hardware RESET switch on front panel of the adapter. The RESET switch provides the same function as *rebooting* the adapter. If the agent services firmware appears to be locked up, or non-responsive, the RESET switch can be reached through the access hole by using a paperclip or similar object.



Note: Resetting the adapter with the RESET switch will clear all volatile object values in the SNMP agent. This includes MIB-2 management objects:

`upsUpTime, snmpInPackets, upsInputLineBads, upsAlarmsPresent,`

etc.

If trap destinations (receivers) are configured, a `Cold Start` trap will be sent when hardware reset is initiated.

FILE MAINTENANCE

ManageUPS allows for firmware, configuration and graphics files to be uploaded to the card over the network via TFTP or FTP.

The *File Transfer* and *Downloads* utilities can be used to update adapter firmware or to simplify configuration of multiple adapters on your network.

KEY FILES

sys	**[pkgName]**`yymmdd.tar`	ManageUPS agent and services package.
	`mosk-ver.yymmdd.pkg`	ManageUPS OS kernel
conf	`snmp.conf`	Contains snmp trap and community settings
cfg	`System1.cfg`	Contains communication settings, device driver information and any user-entered UPS identity parameters that are held by the ManageUPS agent as a proxy for information not supplied by a particular UPS model..
	`mopups.cfg`	Contains settings for network timeserver, email messaging, SNMP wellKnownAlarms, security, servers, remote server shutdown and logging.

The "sys" type files contain the agent firmware and operating system files. If you register your product on the connectivity support web site, you will be notified by email if an update for either of these files is available for download.

The "cfg" type files store the results of user-specific settings entered during the configuration steps covered in sections II and III.

<u>**To simplify configuration of multiple adapters on your network:**</u>

After you have configured the first adapter, download the mopups and/or snmp configuration file(s) and save to a directory on your workstation hard drive. The files should be named as in the table above before uploading to the adapter.

If there are some settings that you would like to make globally throughout your adapter population, these *global settings* sections can be saved as a special subset of the configuration file. Rename the extension of partial "`.cfg`" files to "`.merge`".

When a "`.merge`" file is uploaded to the adapter, its contents are *merged* with the existing file of the same name. When a "`.cfg`" file is uploaded, it replaces the existing file completely.

You can use TFTP or FTP to upload these configuration files to other adapters on your network.

Or, use ManageUPS DCU application (Windows) to simplify file maintenance activities. (See *Quick Start Guide* for more information on DCU and file maintenance)

USING TFTP

To use the WEB interface for TFTP uploads you will need access to the TFTP server on your network. Place the files to be uploaded onto the TFTP server. Enter the address and file name (path) in the controls offered in the ManageUPS WEB interface:

TFTP Host Name:

IP address or hostname of the TFTP server containing the file to be transferred.

File Name:

The name of the file to be transferred.

Start Transfer:

Select the method of transfer to be used, this must be set prior to clicking the **Apply** button.

USING FTP

Place the file you want to upload on a workstation.

Open a command prompt and change to the directory that contains the file you want to upload.

Open an FTP session by typing:

```
ftp [manageupsDNSname] or [manageupsIPaddress]
```

You will be prompted for the username and password: (*Default is* `admin, admin`).

If the file to be uploaded is a type `.cfg` or type `.merge` , simply enter:

```
ftp> put mopups.cfg   or  put mopups.merge
```

If the file to be uploaded is an agent or system update, then enter the word "bin" at the FTP prompt an press [enter].

```
ftp> bin
```

then enter the put file command:

```
ftp> put pkgnameyymmdd.tar        or     put mkernyymmdd.pkg
```

DOWNLOADS

The *Download*s menu offers links to configuration and log files associated with this adapter. Select a link to start the download.

Custom Links

ManageUPS allows for four types of user-definable links that let you link from one ManageUPS adapter to a variety of other resources on your network.

There is *help* available from the adapter web page if you need more information on custom links.