Schneider Electric

User Manual

KVM ACCESS Management Software

American Power Conversion Legal Disclaimer

The information presented in this manual is not warranted by the American Power Conversion Corporation to be authoritative, error free, or complete. This publication is not meant to be a substitute for a detailed operational and site specific development plan. Therefore, American Power Conversion Corporation assumes no liability for damages, violations of codes, improper installation, system failures, or any other problems that could arise based on the use of this Publication.

The information contained in this Publication is provided as is and has been prepared solely for the purpose of evaluating data center design and construction. This Publication has been compiled in good faith by American Power Conversion Corporation. However, no representation is made or warranty given, either express or implied, as to the completeness or accuracy of the information this Publication contains.

IN NO EVENT SHALL AMERICAN POWER CONVERSION CORPORATION BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL, OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, CONTRACT, REVENUE, DATA, INFORMATION, OR BUSINESS INTERRUPTION) RESULTING FROM, ARISING OUT, OR IN CONNECTION WITH THE USE OF, OR INABILITY TO USE THIS PUBLICATION OR THE CONTENT, EVEN IF AMERICAN POWER CONVERSION CORPORATION HAS BEEN EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. AMERICAN POWER CONVERSION CORPORATION RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES WITH RESPECT TO OR IN THE CONTENT OF THE PUBLICATION OR THE FORMAT THEREOF AT ANY TIME WITHOUT NOTICE.

Contents

General Information

Overview

Introduction

KVM ACCESS provides single portal, single login, secure, centralized access, administration and management of your entire network - local and worldwide - anywhere, anytime. KVM ACCESS offers a single, integrated browser-based interface to manage all your devices. Users no longer need to learn the interface for each individual device, making system management easier and more efficient.

By consolidating the management of your IT devices, KVM ACCESS software allows every device to be securely accessed and controlled by means of a single IP address. Servers and network equipment are integrated into a single tree view, making KVM ACCESS software ideal for enterprises with data centers and branch offices, located in several remote locations.

Recognizing the broad spectrum of computing environments, KVM ACCESS Java software implementation allows it to work with Sun Java Runtime Environment (JRE) enabled operating systems, ensuring multi-platform integration and mutual operability.

Features

- Complete control of your enterprise - consolidates the management of all APC IT devices.
- Single portal, single sign on, single IP address to securely access every device on the installation.
- Port association allows the creation of logical devices consisting of ports selected from KVM switches, Blade Servers and Power Distribution Units (PDUs). Instead of accessing these devices through different user interfaces, only one integrated user interface does the job.
- Multiplatform customer support (Windows, Mac OS-X, Linux, and Sun).
- APC device auto-discovery with device-availability status, and alarms.
- All devices are integrated into a single tree view for centralized access, administration, and management of a worldwide network from anywhere at anytime.
- Automated database backup of KVM ACCESS server, devices, and real-time database updating.
- Backup and restore of device configuration and account information.
- Comprehensive reporting capabilities - logging and auditing of system events for KVM ACCESS software and managed devices.
- Critical system event notification via SMTP email, SNMP trap notification, SMS, and Syslog auditing.
- Export of device logs and session history in .csv, .txt, or zip format.
- Automatic scheduling of system, configuration, and maintenance tasks.
- View, manage, and terminate active user sessions in real time.
- Role-Based Access and Control (RBAC).
- Multilanguage interface to minimize user training time and increase productivity.
- Direct Web Access - users can be redirected to 3rd party data center devices from KVM ACCESS.

Security

Security features include internal and external authentication. External authentication support includes LDAP, Active Directory, RADIUS, TACACS+, and NT Domain. Only after being authenticated can users gain access to the devices.

Option to force users of all KVM ACCESS managed devices to be authenticated through KVM ACCESS. Users cannot log in to the devices directly.

Compliant with the X.509 Digital Certificate Standard.

128-bit SSL encryption of all data on the web.

Flexible session time-outs.

Role based access and control, configurable user and group permissions for server access and control.

Supports strong password protection - SAS 70 compliance for configurable number of failed login attempts and user ID lock out parameters.

Devices can identify themselves by Name, MAC address, or IP in the browser. The IP addresses of KVM/PDU devices can be hidden.

IP and MAC filtering.

Local and remote access logged and authenticated.

Private CA support.

Server Management Features

- BIOS level support.
- Flexible encryption design allows users to choose any combination of 56- bit DES, 168-bit 3DES, 256-bit AES, 128-bit RC4, or Random for independent KB/Mouse, video, and virtual media data encryption.
- Virtual Media - supports CAC/Smart Card readers, fingerprint readers, DVD/CD drives, USB mass storage devices, PC hard drives and ISO images.
- Panel DynaArray.
- Virtual Remote Desktop.
- Exit Macro support.
- Mouse DynaSync.
- Message Board.

Requirements

Server Requirements

Systems that KVM ACCESS will be installed on should meet the following requirements:

- Hardware Requirements
  - CPU: Pentium 4, 2.60 GHz or higher
  - Memory: At least 512MB (1GB or more recommended)
  - Hard drive: 500MB or more free space
  - Ethernet: At least 1 Ethernet adapter (100Mbps or higher) - Giga LAN recommended
- Operating System Requirements
  - Windows: 2000, XP, 2000 Server, Server 2003, Server 2008, or Windows Vista with Java Runtime Environment (JRE) 6, Update 11, or higher (with the latest service package for each installed)
  - Linux (with Java Runtime Environment (JRE) 6, Update 11, or higher)
    - Red Hat Enterprise Linux V. 4
    - Novell SUSE Enterprise Server 9 and 10

Client Requirements

Hardware Requirements.

- CPU: For best results, computers used to access the switch should have at least a P III 1 GHz processor, with the screen resolution set to 1024 x 768.
- Memory: At least 512MB (1GB or more recommended).
- Ethernet: At least 1 Ethernet adapter - 10Mbps or higher - 100Mbps recommended.
- Browsers must support 128 bit SSL encryption.
- For the browser-based Java Applet Viewer the latest version of the Java Runtime Environment (JRE) must be installed.
- At least 205MB of memory must be available for the first viewer after logging in from the browser and 100MB for each additional viewer that is opened, thereafter.

Operating Systems. Supported operating systems for client workstations that connect to KVM ACCESS are shown below:

OS		Version
Windows		2000 and higher
Linux	RedHat	7.1 and higher
	Fedora	Core 2 and higher
	SuSE	9.0 and higher
	Mandriva (Mandrake)	9.0 and higher
UNIX	AIX	4.3 and higher
	FreeBSD	4.2 and higher
	Sun	Solaris 8 and higher

Supported operating systems for users that log into KVM ACCESS include Windows 2000 and higher, and those capable of running the Java Runtime Environment (JRE) 6, Update 11, or higher. The Windows 2000 Client does not support the WinClient Viewer.

Browsers:
Supported browsers for users that log into KVM ACCESS include:

Browser		Version
IE		6 and higher
Chrome		8.0 and higher
Firefox	Windows	3.5 and higher
	Linux	3.0 and higher
Safari	Windows	4.0 and higher
	Mac	3.1 and higher
Opera		10.0 and higher
Mozilla	Windows	1.7 and higher
	Sun	1.7 and higher
Netscape		9.0 and higher

Device Requirements

All APC IP KVM products must be at a firmware level that contains the KVM ACCESS Management function and the KVM ACCESS Management function must be enabled.

Download and install the latest version of the relevant firmware from **www.apc.com**, if necessary. For details on upgrading the firmware see “Upgrade Selected Appliance Firmware” on page 88.

Note: Devices must be configured to communicate on the same port that you configure for the KVM ACCESS's Device Port (see “Device port” on page 8).
For a list of supported devices see “Compatible Products” on page 103.

Licenses

The KVM ACCESS license controls the number of nodes permitted on the KVM ACCESS server installation. License information is contained on the USB License Key that came with your KVM ACCESS purchase.

Upon completion of the KVM ACCESS software installation, a default license (one master and 80 nodes) is automatically provided. To add more nodes you must upgrade the license. See “Upgrading the License” on page 82 for detailed information.

Nodes.

- A node can either be a physical port, or an aggregate device. Each node requires a license.
- Aggregate devices can be created when a device (router, server, ethernet switch, etc.,) managed through KVM ACCESS is capable of being accessed through several devices’ ports. By consolidating those ports into a single Aggregate Device, the Aggregate Device counts as a single node, and only requires a single license.
- Ports on devices, when not part of an aggregate device, must be unlocked (see “Locking / Unlocking Ports” on page 60) in order to be used. Each unlocked port counts as one node.
- Generic devices (routers, switches, etc.) are not counted.
- Direct Web Access devices are not counted.
- Folders do not count as nodes, however each physical port within a folder counts as a node. In addition, each Aggregate Device contained in a folder counts as one node. See “Devices Menu” on page 49 for detailed information on each of the device categories.

Installation

Windows Version Installation

Before you begin

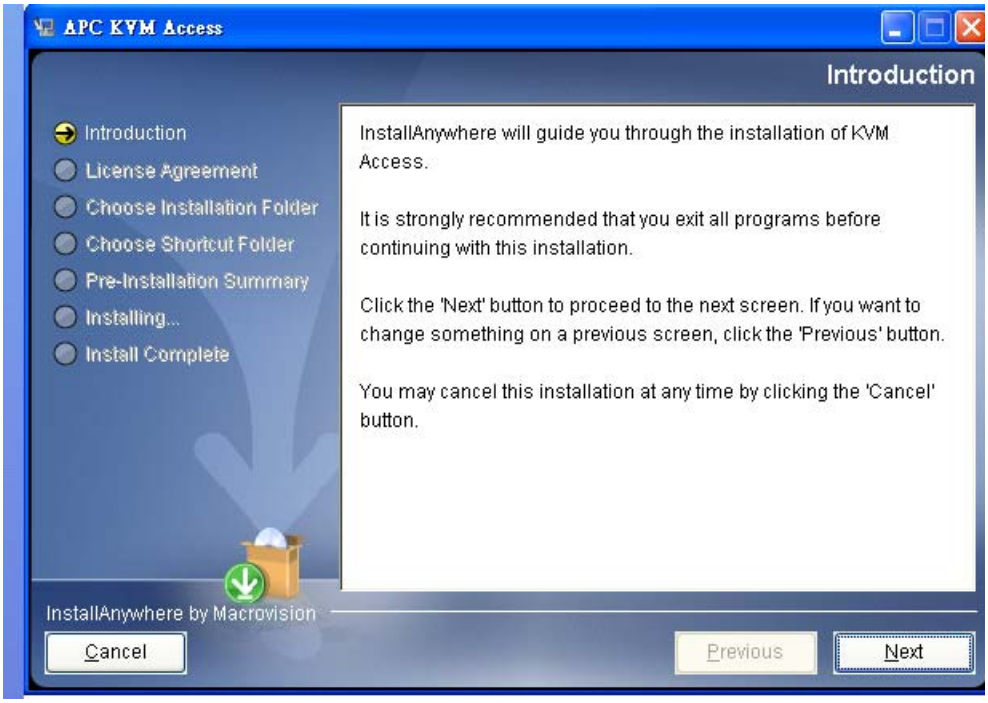
Before running the installation program make sure of that the Sun's Java Runtime Environment (JRE) 6, Update 11, or higher has been installed on your system. If not, you need to download and install it. You can get the latest version from the Java web site:

`http://java.com`

After the JRE has been installed on your system, you are ready to install the KVM ACCESS program.

Starting the installation

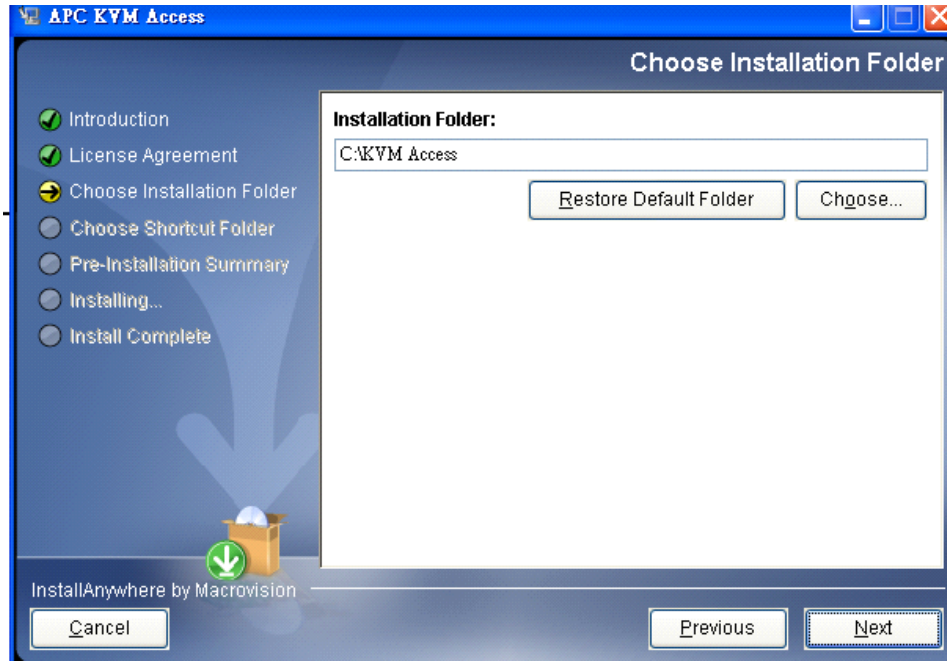
1. Put the software CD into the computer's CD or DVD drive.
2. Go to the folder where **KVM ACCESS Setup_Win.exe** is located, and execute it. The **Introduction** window, will open. Click the **Next** button to continue.



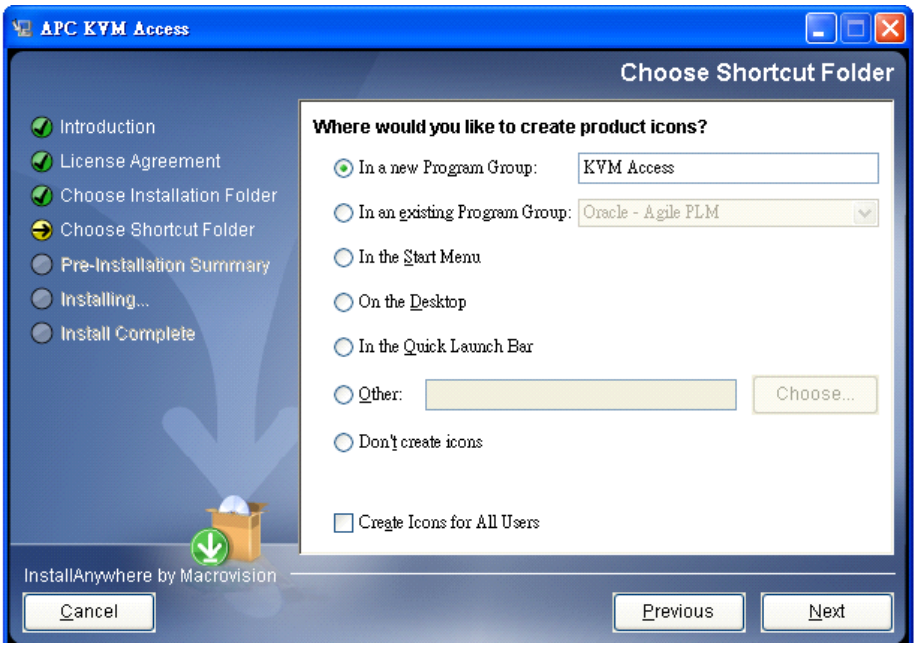
3. Read the **License Agreement** that opens, then click the "**I accept...**" radio button.
4. Click the **Next** button to continue.
5. In the dialog box that opens, enter the software serial number (the serial number can be found on the CD case), then click **Next** to continue.

Note: Save your software serial number in a safe place in case you need it for reinstallation.

6. In the **Choose Installation Folder** dialog box, specify the KVM ACCESS' installation folder. If you don't want to use the default entry, click **Choose...** to browse to the location you want, then click **Next** to continue.



7. In the **Choose Shortcut Folder** dialog box, click one of the radio buttons to specify where you would like to create product icons, then click **Next** to continue.



8. Fill in the fields in the **Config & Setup** dialog box, according to the information in the table.

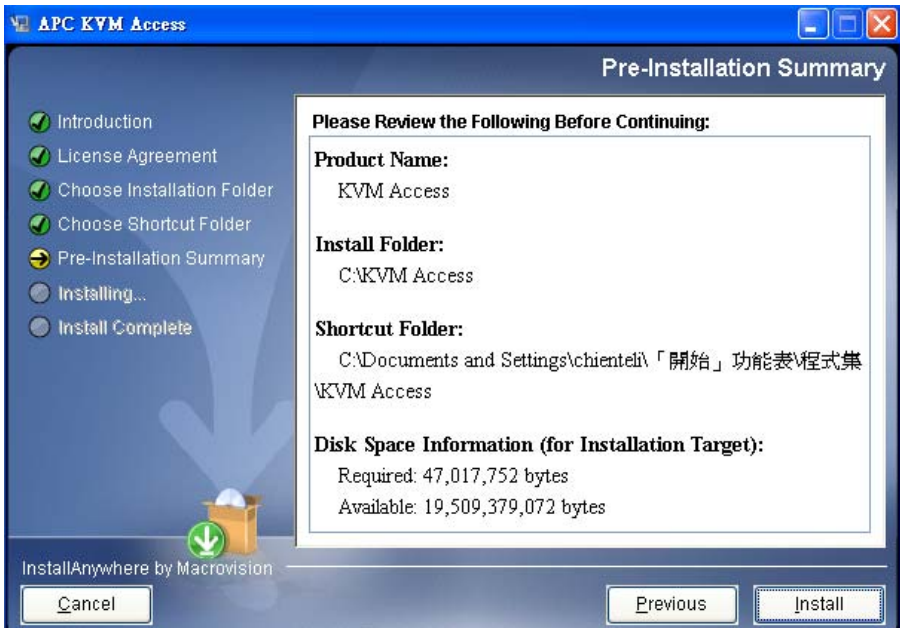
Heading	Description
Server name	The default name for the server - as defined in the Windows **Computer Name** setting. You can choose a different name to identify the server on the KVM ACCESS installation. The name can be from 2-32 bytes in any supported lantuage. **Note:** 1. The following characters may not be used: “ ‘ \ 2. The name is only for KVM ACCESS server purposes - it doesn’t change the actual computer name.
Viewer port	The port that the user uses to communicate with KVM ACCESS servers. The default is 8003. **Note:** 1. This is the **Viewer Port** referred to on the **This Server** web page. See .“Server Information” on page 74. 2. Each KVM ACCESS server on the system can use its own port setting, for ease of management it is recommended that all servers use the same port setting.
Device port	The port that the KVM ACCESS server uses to communicate with the devices on the installation. The default is 8000. Each KVM ACCESSKVM ACCESS server can have a separate device port number, but in order to communicate with the devices connected on its network segment, those devices must be configured to use the same port as the one set here.
HTTP port	The port that the KVM ACCESS server uses for web communication. The default is 80. If you use a different port, users must specify the port number in the URL of their browsers.
HTTPS port	The port that the KVM ACCESS server uses for secure web communication. The default is 443. If you use a different port, users must specify the port number in the URL of their browsers.

9. After the fields have been filled, click **Next** to continue.

Note: Any of these settings can be changed following the installation. See“Server Information” on page 74, for details.

10. The dialog box informs you that files are being copied to the installation folder. Once the files have been copied, click the **Continue** button.

11. The Pre-Installation Summary dialog box opens. Click **Previous** to go back and make changes. If the information is correct, click **Install**.



12. When the dialog box opens informing you that the installation has completed successfully, click **Done** to exit the installer.
13. At the completion of the installation, a KVM ACCESS entry is created in the Windows Start menu.

Post-installation check

After installation completes, the KVM ACCESS program starts automatically (and starts automatically with every bootup).

To check that KVM ACCESS has started, navigate through the following folders: **Control Panel > Administrative Tools > Services**. Look down the list to the KVM ACCESS entry. If KVM ACCESS is running, it will appear in the services list.

The entry in the Status field should say **Started**. If it does not, right click anywhere on the KVM ACCESS entry line and select **Start** from the pop up menu.

Linux Version Installation

Before you begin

The procedure for installing KVM ACCESS on a Linux system is similar to that for Windows, but there are Java considerations to note.

- If Java isn't already installed, download from the Java web site:

  `http://java.com`

  Installation instructions are provided on the Java download page.
- To determine the Java version on your system, open a terminal and enter the following:

  `java -version`

If the version is earlier than JRE 6, Update 11, install JRE Version 6, Update 11 or higher.

- Make sure PATH and JAVA_HOME environment variables point to the new version in your /root/.bash_profile file. For example:

  JAVA_HOME=/usr/java/jre1.6.0_0-b11

  PATH=$JAVA_HOME/bin:$PATH:./

  BASH_ENV= $HOME/.bashrc

  USERNAME= "root"

  export JAVA_HOME PATH BASH_ENV USERNAME
- If the original Java version is still used and the new version is not recognized, correct it.
  a. Copy the KVM ACCESS Setup_Linux.bin file from the distribution CD to your hard drive.
  b. Go to the directory where the KVM ACCESS Setup_Linux.bin file is located.
  c. Enter the following commands:
  export LAX_DEBUG=1
  sh KVM ACCESS_Setup_ForLinux.bin

  Note: If the installation program starts, cancel it.

  d. Look for the line that begins: **Using VM.....** to see to which Java version is defaulting.
  e. If the **Using VM** entry shows a file named java in the old Java version directory, go to that directory and delete the java file or rename it.
  f. Log out and log back in.

Installing

After making sure that the appropriate version of the JRE has been installed, do the following:

1. Put theKVM ACCESS software CD into the computer's CD or DVD drive.
2. Go to the folder where KVM ACCESS Setup_Linux.bin is located, and run it.

   Note: 1. You must run the installation program as the root user.

   2. Make sure that the installation file has executable permissions

   3. For some versions of Linux, the program must be run in a terminal.
3. When the **Introduction** window opens, click the Next button to continue.
4. The remainder of the installation procedure is the same as for Windows. Refer to the Windows installation procedure (page 6), for details.

Post-installation Check

After installation is finished, the KVM ACCESS program starts automatically (and starts automatically with every bootup).

To check that KVM ACCESS has started, issue the following commands (as root) to start, stop, and restart, the service from a terminal console:

/etc/init.d/KVM ACCESSservice start# to start the service

/etc/init.d/KVM ACCESSservice stop# to stop the service

/etc/init.d/KVM ACCESSservice restart# to restart the service

/etc/init.d/KVM ACCESSservice status# to check the service status

To check on the Java version your system is running, do the following:

1. Open the Start menu.
2. Navigate to the KVM ACCESS entry (Programs > KVM ACCESS), and select Java Version Checker.

Post Installation Setups

KVM ACCESS software comes with a default license that allows the server with 80 nodes. For anything beyond this minimum, you will need a license key that allows additional nodes.

- Insert the KVM ACCESS software's USB license key into a USB port, log into the server (see "Logging in" on page 13), go to the License page, and click Upgrade (see "Upgrading the License" on page 82). The number of nodes that are allowed depends on your license key purchase. Contact your dealer for details.

  Note: After upgrading the license, remove the key and place it somewhere safe. You will need it for future upgrades.

Uninstalling KVM ACCESS Software

Uninstalling from a Windows system

1. Open the Start menu.
2. Navigate to the KVM ACCESS entry (Programs > KVM ACCESS), and select **Uninstall KVM ACCESS**.

Note: Many KVM ACCESS files and folders that were created during installation must be removed manually for a complete removal (necessary if you plan on reinstalling). The default folder is C:\KVM ACCESS.

Uninstalling from a Linux system

As root, execute the following command:

```
/install-path/Uninstall_KVM ACCESS/Uninstall_KVM ACCESS
```

Where **/install-path/** represents the path and directory that you specified for the KVM ACCESS's location when you installed the program.

Note: Many KVM ACCESS files and folders that were created during installation must be removed manually for a complete removal (necessary if you plan on reinstalling). The default is /home/KVM ACCESS.

Upgrading KVM ACCESS

If the KVM ACCESS program has already been installed, it is not necessary to perform a full install. The latest KVM ACCESS version can be installed by running the KVM ACCESS-Upgrade program:

Preliminary steps

Taking the following backup steps before you begin is recommended. If a problem should occur after the upgrade, the backup created can be used to restore the database to its latest working level.

- You must have previously scheduled regular backups so you will have a backup file to restore. See “Backup the Server Database” on page 84 for details.
- You must have scheduled backup files from "Backup Device Configuration" (page 89).

Upgrade

Run the KVM ACCESS Upgrade procedure. Follow the installation Wizard to complete the procedure.

KVM ACCESS Upgrade_Win.exe (for Windows)
KVM ACCESS Upgrade_Linux.bin (for Linux)

Note: New versions of the Upgrade Program are posted on **www.apc.com** for download as they become available. Check the website to get the most up-to-date version.

After the Upgrade is completed, all settings/information are reset.

- Use the “KVM ACCESS Utility” on page 110 to restore database settings.
- Run Restore Device Configuration to restore Device Configurations and Account Information. See “Restoring Device Configurations” on page 62 for instructions on restoring device configurations and account information.

Browser Operation

To ensure multi-platform operability, access to the KVM ACCESS is available through most standard web browsers. Once users log in and are authenticated, the KVM ACCESS's browser GUI comes up. This chapter explains the login procedure, and describes the KVM ACCESS's browser GUI components.

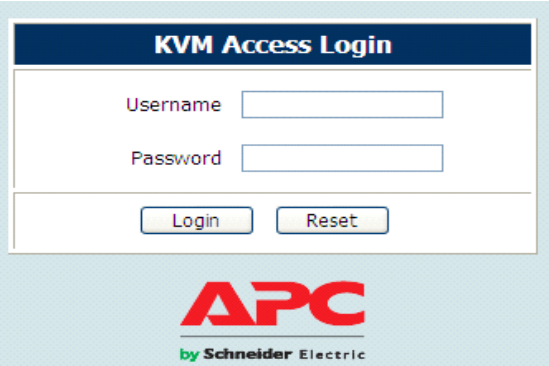
Logging in

To log in to KVM ACCESS:

1. Open the browser and specify the IP address of the KVM ACCESS in the browser's URL location bar.

   Note: If the system administrator has configured the HTTP or HTTPS port setting as something other than the KVM ACCESS defaults, you must include http:// or https:// before the IP address, and specify the port number along with the IP address. For example: **http://192.168.1.20:8082**
   Where 8082 is the http port number, and a colon is inserted between it and the IP address.

2. If any Security Alert dialog boxes appear, accept the certificate. It can be trusted. See “Trusted Certificates” on page 106 for details. The Login page will open.



3. Provide your KVM ACCESS Username and Password, then click the Login button.

   Note: There is a pre-installed system administrator account that can be used to log in for the first time. The Username for this account is **apc**; the password is **apc**. For security purposes, change this to something unique. See “Managing User Accounts” on page 33 for details.

KVM ACCESS Interface

After you have successfully logged in, the KVM ACCESS web page opens.

KVM ACCESS web page components:

Item Number	Item Name	Description
1	Tab bar	The tab bar contains the main operation categories. The items that appear in the tab bar are determined by the user's type, and the authorization options that were selected when the user's account was created.
2	Page menu bar	The page menu bar contains operational sub-categories that pertain to the item selected in the tab bar. The items that appear in the menu bar are determined by the user's type, and the authorization options that were selected when the user's account was created.
3	Sidebar	The Sidebar provides a tree view listing of items relating to the tab bar and menu bar selections. Click an item in the Sidebar to open its detail page.
4	About	About provides information regarding the current version of the KVM ACCESS.
5	Logout	Click this button to log out of your KVM ACCESS session.
6	Welcome message	If this function is enabled (see Preferences, page 29), a welcome message displays here.
7	Navigation buttons	These buttons move you through the Sidebar. Their use is discussed in the next section.
8	Interactive display panel	This is the main work area. The screens that appear reflect your menu choices and Sidebar item selection. The use of this panel is discussed on page 16.

The Navigation Buttons

The navigation buttons move you through the items in the Sidebar:

Button	Action
	Moves to the item in the tree that is one level out and one step up from the current selection (its parent item). In the diagram below: If the focus were on SLOT-01-TestA, it would move to CMC-599232S.
	Moves to the item in the tree that is on the same level of depth and one step up from the current selection (its sibling item). In the diagram below: 1. If the focus were on AP5615-4B-3B-7C, it would move to OutletA. 2. If the focus were on SLOT-01-TestA, it would move to AP5615-4B-3B-7C.
	Moves to the item in the tree that is on the same level of depth and one step down from the current selection (its sibling item). In the diagram below: 1. If the focus were on KN4132-23, it would move to PN0108RPSwitch. 2. If the focus were on OutletA, it would move to OutletB.
	Moves to the item in the tree that is one level in and one step down from the current selection (its child item). In the diagram below: If the focus were on PN0108RPSwitch, it would move to OutletA.

One of the advantages of using the navigation buttons instead of clicking on an item in the Sidebar is that you stay on the same Panel Menu page as you move from item to item.

Note: When you make a menu choice, a Panel Menu bar with further choices opens in the Interactive Display Panel. See “Interactive display panel” on page 16.

Example: If you made a change to SLOT-01-TestA that you also wanted to make to SLOT-01-TestB, by using the navigation buttons, you could move to the desired location in SLOT-01-TestB without clicking through all the Panel Menus to get there.

If you access an item by clicking on it in the Sidebar, the opening page for that item appears. To make the same change to SLOT-01-TestB that you made to SLOT-01-TestA, you have to start at the beginning and click through all the Panel Menus to get to the desired location.

Note: If an item's icon contains a question mark, it indicates there is a mismatch between the device's information and the information for it stored in the KVM ACCESS database. See “Update” on page 64, for information on resolving the problem.

Tree view considerations

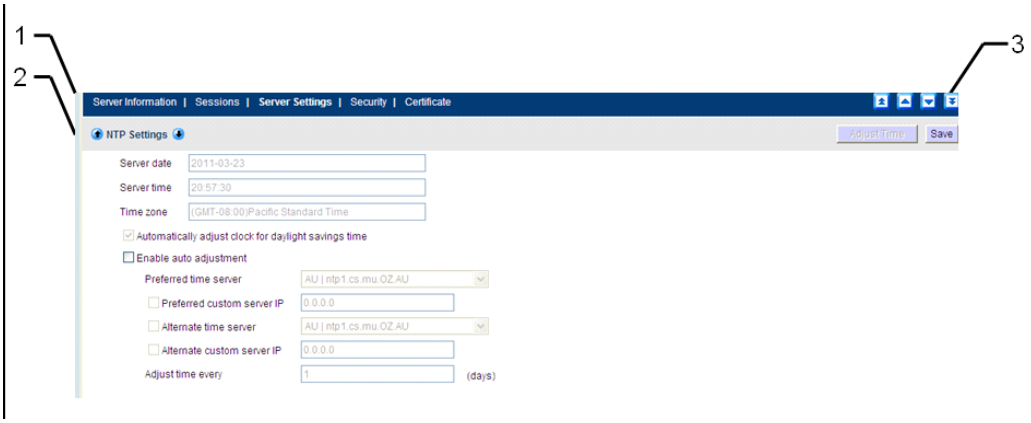
- Only items a user is authorized to access appear in the Sidebar tree view.
- A plus (+) sign in front of an item means that there are additional items nested inside. Click the plus sign to expand the view and show the nested items.
- The plus sign changes to a minus sign (-) when an item is expanded. Click the minus sign to collapse the view and hide the nested items.
- For devices, if the device is on line, its icon is in color; if it is off line, its icon is gray.

Note: Users can configure the way devices and ports display in the Sidebar tree view. See “User Preferences” on page 28, for details.

Interactive display panel

Overview

The Interactive Display Panel (also referred to as the main panel) is your main work area. The screens that appear reflect your menu choices and Sidebar item selection. The reason it is called an interactive display panel, is that in addition to displaying the contents of your menu choices, it is also a work area where you can make configuration settings and perform actions on selected devices.



Item	Description
Panel Menu Bar	• Refines the menu category into smaller related groupings. • If there are secondary Panel Menu pages, hovering over the Panel Menu title with the mouse opens a popup menu. Click on a menu item to go to the desired secondary page. • The items that appear in the Panel Menu bar are determined by the user's type and authorization permissions.
Panel Menu Title Bar	• Describes the Panel Menu category. • Additional Panel Menu pages are indicated by an arrow icon. • Click the Down arrow to go to the next page. • Click the Up arrow to go to the previous page.
Action Input Area	A button or input box displays directing you to take an action (Save, Delete, Next, etc.) with regard to the current page.

Selecting list items

Many of the pages displayed in the Interactive Display Panel contain a list of selection items (devices, users, groups, configuration files, etc.) on which to perform an operation.

- To select an item, click to put a check in the checkbox in front of the name.
- To select a group of items, put a check in the checkbox in front of each of their names.
- To select all of the items, put a check in the checkbox at the top of the column.

Preferences

Users can set individual preferences for their browser sessions by clicking the **Preferences** tab on the Tab Bar. The Interactive Display Panel opens to the default page - Web Options. The Panel Menu bar shows the available categories: Web Options, and Password.

Web options

Language.

- To set KVM ACCESS to display pages in the same language your browser uses, Click the **Use Browser Settings** radio button.

Note: If your browser is set to a non-supported language, KVM ACCESS looks at the the language of your server's operating system. If the operating system is set to a supported language it will use that language to display its pages. If the operating system is set to a non-supported language, KVM ACCESS defaults to English.

- Click the Use radio button to select from a list of supported languages.

Note: If the language selected is different from the browser's setting, there will be no change until after you log in.

- Login Page: You can choose to open to the default page when you log in (the first page of the first tab on the Tab Bar), or you can choose to open to the page you were on the last time you logged out.

Welcome Message.

- To have the Welcome Message appear, select Show. Select Hide if you don't want it to appear.
- To have a Screen Name appear with the Welcome Message, type the screen name into the Display screen name text box.

Note: 1. When you change your Screen Name here, the Screen Name entry in the User Accounts settings automatically changes to match what you entered here (see Adding User Accounts, page page 31).
2. The Screen Name will not display unless you choose to Show the Welcome Message.

When you have made your choices, click **Save**.

Password.

To change your password:

1. Check the **Change Password** box to enable the password input fields.
2. Enter your old password in the Old password field.
3. Enter your new password in the New password field.
4. Enter your new password again in the Confirm password field.
5. Click **Save**.

Port Access

Overview

Access and control the devices, ports and outlets that are managed over the KVM ACCESS network. The Menu Bar provides different organizational views. Click on a view in the Menu Bar to see the items organized according to the selected view's parameters.

Note: If no access rights have been assigned to a user, the Port Access tab and page do not display, even for System Administrators.

Table Headings

Headings vary depending on the view selected. Change the sort order of the items by clicking on the column headings.

Heading	Description
Name	The name given to the port when it was added to the KVM ACCESS installation.
Alias	The name given to the port when it was added to the KVM ACCESS installation.
Port	The port's port number on the device to which it belongs.
Port Type	Indicates the kind of device to which the port belongs.
Device Name	The name of the device to which the port belongs.
Device Type	The type of device that the port belongs to (KVMXXX, APXXX, Blade, etc).
Options	• For KVM ports, indicates the port's Access Mode. See Mode, page 68, for details.. • For PDU outlets, indicates the port's Power Management Configuration. See Port Settings, page 70, for details. • This item is blank for Target device ports.
Status	• For KVM ports, indicates whether the port is online or offline. • For PDU outlets, indicates whether the outlet port's power socket is On or Off. **Note:** This category does not apply to Blade Chassis or individual blades. **N/A** (not applicable) displays for Blade Chassis, and **Unknown** displays for individual blades.
IP Address	For physical devices - the device's IP Address displays here.
MAC Address	For physical devices - the device's MAC Address displays here.
Operation	The default action for accessing the device/port appears in this cell. • Click the arrow at the right of the table cell to see what other actions (if any), are available. • Click your choice to open a session for the device/port. The various device/port operation choices are described in the **Port Operation** section that follows.
Link	Click to go to the device's Device Management > Port page.

Action Buttons

There are two buttons at the top right of the main panel: **Filter**, and **Launch Multiviewer**:

Filter

Filter allows you to control which items appear in the main panel list.
Enter the information string and click the **Filter** button on the panel (or press the Enter key on your keyboard). Only items that have that particular information string in their names will display in the list.

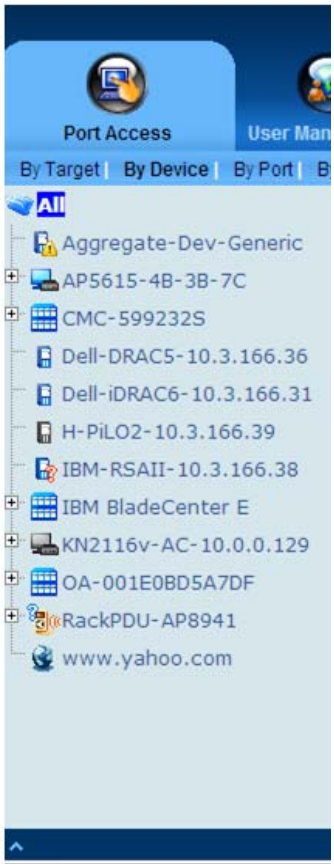
> For example, if TD is your information string, only items with names containing TD, such as TD-AGG-01, will display.

To clear the filter and bring back the complete list, erase the contents of the input box and click **Filter** again.

Launch Multiviewer

If you want to launch viewers for more than one port at the same time, click to put a check in the checkbox in front of the names of the ports you want to access, then click **Launch Multiviewer**.

The Sidebar



Devices, ports and outlets that have been configured on KVM ACCESS are listed in a tree structure in the Sidebar at the left of the screen:

Sidebar characteristics.

• Users see only the devices, ports and outlets for which they have access permission.

• Ports/outlets and child devices can be nested under their parent devices.

–Click the + in front of a device to expand the tree and see the ports/outlets nested underneath it.

–Click the - to collapse the tree and hide the nested ports/outlets.

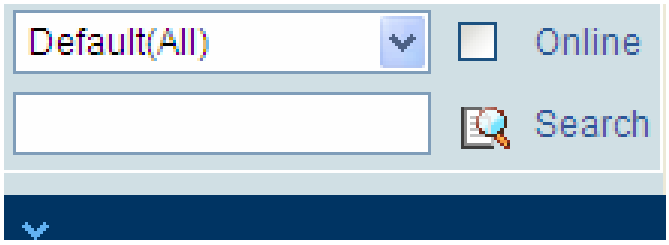
• Switches and ports that are online have Green monitor screen icons. The monitor screens are Gray for devices and ports that are offline.

• Clicking an item in the tree opens its Status and Operation page.

• Double clicking an active device or port opens the viewer for it.

• Right click an active device or port to open a pop-up menu. Select a viewer to access the device or port (see “Port Operation” on page 21).

Sidebar Filter. Control the number and type of devices, ports and outlets that display in the Sidebar. When you click the upward-pointing arrow at the bottom left of the Sidebar panel it brings up the Filter dialog box .



Choices	Description
All	This is the default view. With no other filter options selected, all of the devices, ports and outlets that are accessible to the user are listed in the Sidebar. Drop down the list box to see all of the available choices and select one of them instead of All. Only the items that match your selection display in the tree.
Online	If you enable Online (by putting a check in the checkbox) only items that are online display in the tree.
Search	If you enter a search string and click **Search**, only device, port, and outlet names that match the search string display in the tree. Wildcards (? and *) are acceptable, so that more than one item can display in the list. Example: if you enter Web*, both Web Server 1 and Web Server 2 show up in the list.

To close the Filter dialog, click the **Down** arrow at the bottom left of the Sidebar panel.

Port Operation

Depending on the item chosen, various port operation methods are available to access and control it. Click the arrow at the right of the Operation cell to select an operation method.

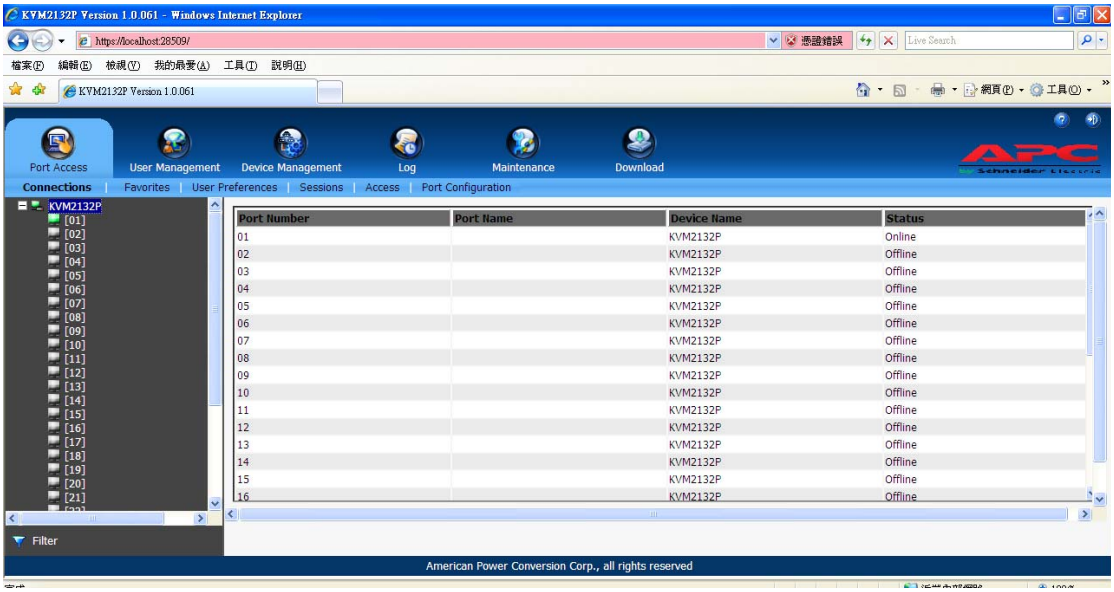
Clicking **KVM ACCESS Viewer** opens a KVM viewer directly to the device running on the selected port. It is just like what you would see if you logged into the device directly and then selected that port on the device's GUI. A window with that device's port session opens on your desktop.

To switch ports in the viewer, open the hidden Control Panel (by hovering the cursor over the top center of the viewer window), and select the Port List icon. The port list choices include all the ports belonging to the device.

- In the list, select the device to which the port belongs (KVM2132P in the screenshot), then click the port you want to access.
- The viewer window of each port has a hidden Control Panel. To switch to a different port on the device, bring up the port list and click the desired port.
- When you have finished with your session, open the Control Panel and select the **Exit** icon.

Web Access

Click **Web Access** to open a browser session for the device on your desktop (as if you had opened a browser and logged in from the URL bar).



Power ON / OFF

- For Aggregate and Power devices you can choose **All ON** or **All OFF** to turn all the outlets belonging to that device on or off.
- For Power outlets, you can choose **ON** or **OFF**. If the port's status is ON, the choice is OFF - click OFF to turn the power to the outlet off.

Note: The change doesn't appear in the table until you leave the page and come back to it.

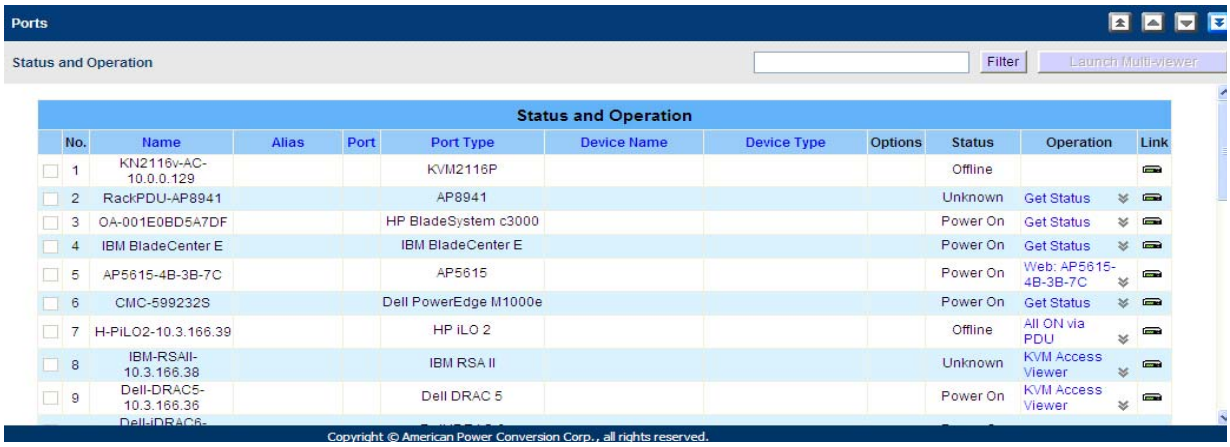
SSH / Telnet Session

Choose to open an SSH or Telnet session to the selected port. You get an SSH or Telnet viewer window just as if you had logged into the KVM device (KVM2116P, for example), with your browser and had chosen Telnet on the Main Web page.

Port Access Views

Port View

When Port Access is selected on the tab bar, the default page is Port View. This page lists all of the ports that have been deployed under the KVM ACCESS system, independently of their devices. To only see a particular port, click on it in the Sidebar.

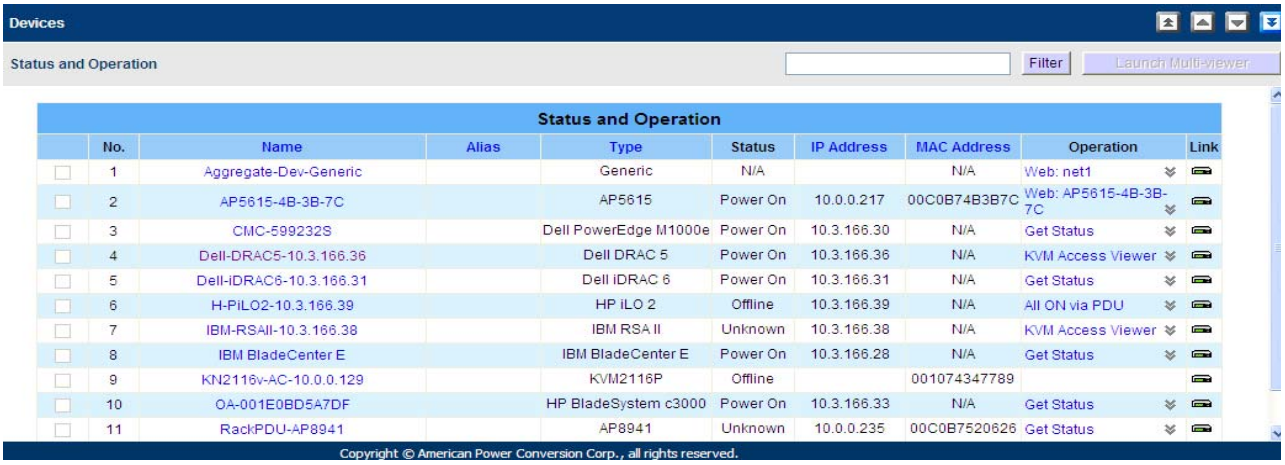


Target View

Target devices include Aggregate Devices, and Blade Chassis (and individual blades). The Target page default view has **All** selected at the top of the Sidebar, and the Status and Operation page displayed in the Interactive Display panel. To only see the ports for a particular device, click on the device in the Sidebar.

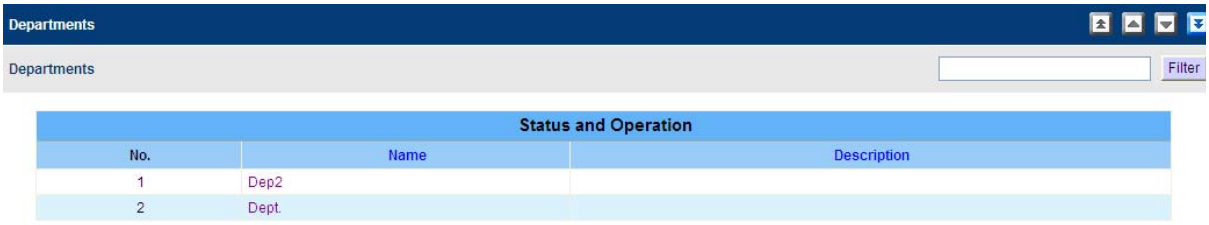
Device View

Device view displays all of the devices that have been deployed under the KVM ACCESS system. To only see the ports for a particular device, click on the device in the Sidebar.



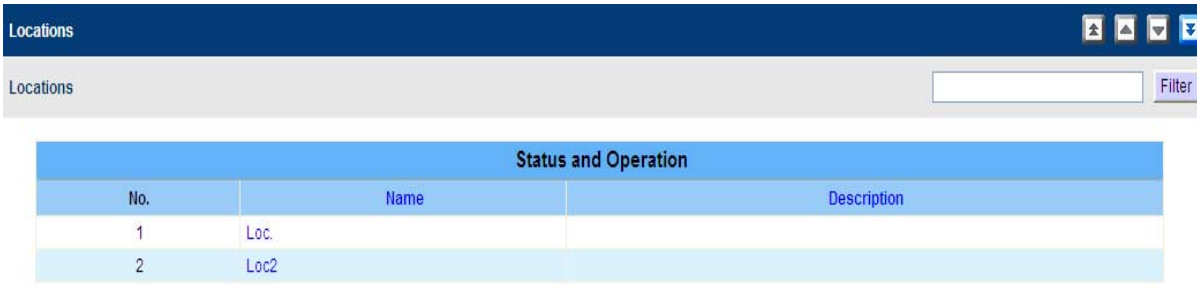
Department View

Department view displays all of the departments that have been created under the KVM ACCESS system, and the ports that have been assigned to each. To only see the ports belonging to a particular department, click on the department in the Sidebar.



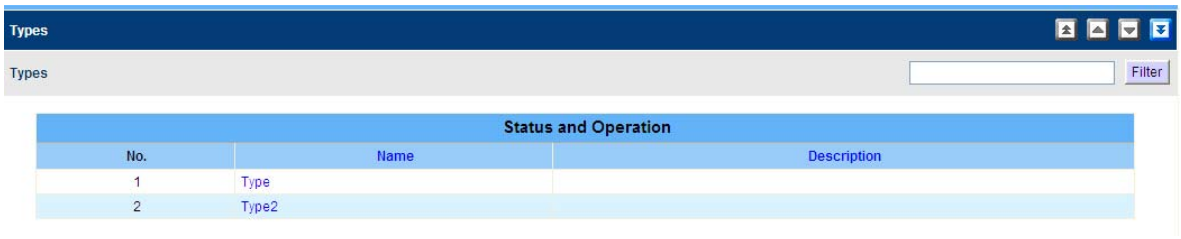
Location View

Location View displays all of the locations that have been created under the KVM ACCESS system, and the ports that have been assigned to each. To see only the ports belonging to a particular location, click on the location in the Sidebar.



Type View

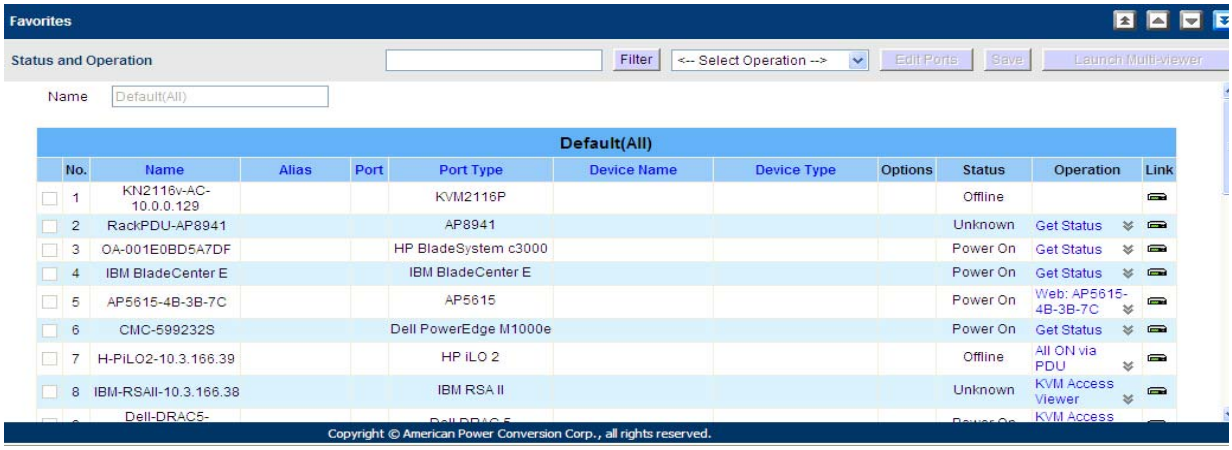
Type View displays all of the device types that have been created under the KVM ACCESS system, and the ports that have been assigned to each. To see only the ports belonging to a particular device type, click on the type in the Sidebar.



Favorites View

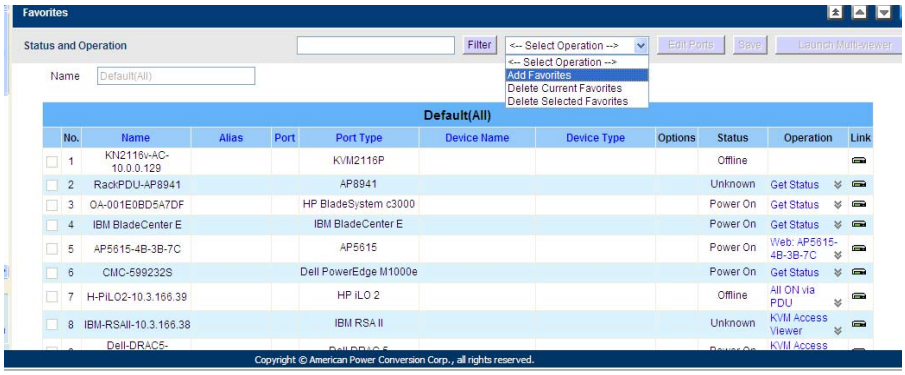
The Favorites page is similar to a bookmarks feature. Frequently accessed devices and ports can be saved under favorite names of your choosing here. Open this page and select the name, rather than hunting for devices and ports in the Sidebar. This feature is practical on large, crowded installations. When Favorites is selected on the menu bar, the default page comes up, listing all of the devices and ports that have been deployed under the KVM ACCESS system.

Note: Filter and Launch Multiviewer work the same as on the other View pages.



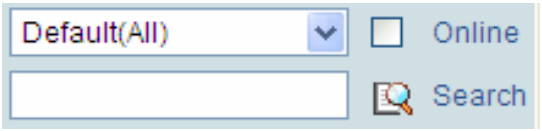
Adding a Favorite. To create a Favorite and populate it with ports.

1. Choose **Add Favorites** from the Select Operation list.



2. Give the Favorite a name in the page that opens. Click the checkboxes of the ports you want to include, then click **Save**. When the operation is finished your Favorite displays in the main panel and is also listed in the Sidebar.

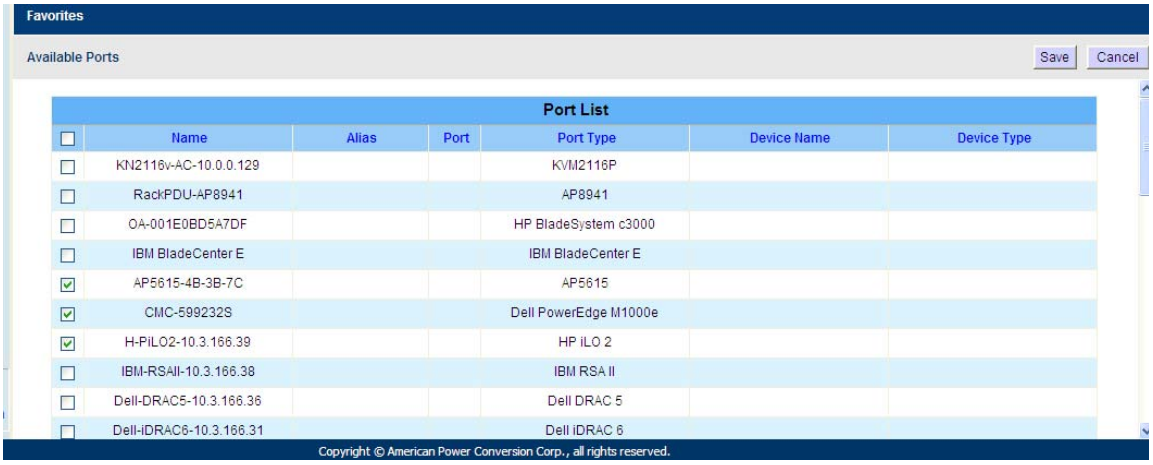
Viewing a Favorite. A filter panel at the bottom of the sidebar lets you control the items that display on this page.



Choices	Description
Default	This is the default view. With no other filter options selected, all of the ports that are accessible to the user are listed in the Sidebar and display in the main panel. Click the arrow to open the drop down menu and select a Favorite (if any Favorites have been created). When a Favorite is selected, only the items chosen for the Favorite list display in the Sidebar and main panel.
Online	If you enable **Online** (by clicking in the checkbox) only the ports whose attached devices are online appear in the Sidebar and the main panel.
Search	If you enter a search string and click **Search**, only port names that match the search string display in the Sidebar and main panel. Partial entries are acceptable. Enter “Web” and any ports that contain the string “Web” anywhere in the name, appear in the Sidebar and main panel.

Managing Favorites.

To add or remove ports from a Favorite:



1. Select the Favorite in the filter list.
2. Click **Edit Ports** (at the top-right of the panel) to open a page showing all of the ports available to the user. The ports that are currently included in the Favorites have a check in their checkboxes.
3. Check any ports you want to include in Favorites; uncheck any ports you want to remove from Favorites.
4. Click **Save**

User Preferences

User Preferences is different from the other Menu Bar items. It does not provide an organizational view of the devices and ports. It has two Panel Menu items: Port Display, and Alias. Port Display lets you configure how the device tree appears in the Sidebar; Alias lets you give nicknames to your devices and ports.

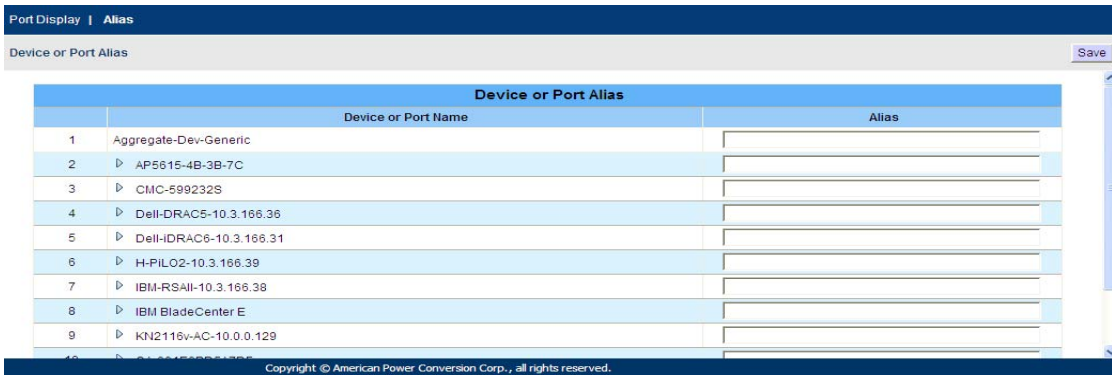
Port Display

The Port Display page is the default that opens when you select User Preferences.

Item	Description
Display Settings	• Select from the drop down list the view the page will open to when the Port Access tab is clicked. • Choose **Show complete tree** to see all the nested devices and ports when you click to expand the tree. • If you choose **Hide physical devices or ports that are included in group devices**, physical ports that are included in group devices will not display under their originating devices when you click to expand the tree.
Viewer Client Settings	• No matter which browser you logged in with, if you choose Java Client, KVM ACCESS will open the Java Client Viewer • If you choose **Auto detect**, KVM ACCESS will check to see if you logged in with IE or with another browser. If you logged in with IE, it will open the Windows Client Viewer when you access a device or port. If you logged in with a browser other than IE, it will open the Java Client Viewer.

Alias

Selecting **Alias** on the Panel Menu, opens a page that allows you to give your devices, ports, and outlets a nickname to make it more convenient to remember which items you are managing.



- The default view only shows devices. To give an alias to a port or outlet, click the arrowhead in front of the device's name to show them.
- Enter the alias into the **Alias** field of the device, port, or outlet. When you return to an organizational view page, the alias appears in the Sidebar instead of the device or port name.

Note: The alias is visible only for the user who created it. Other users see the original name (or an alias that they have created).

User Management

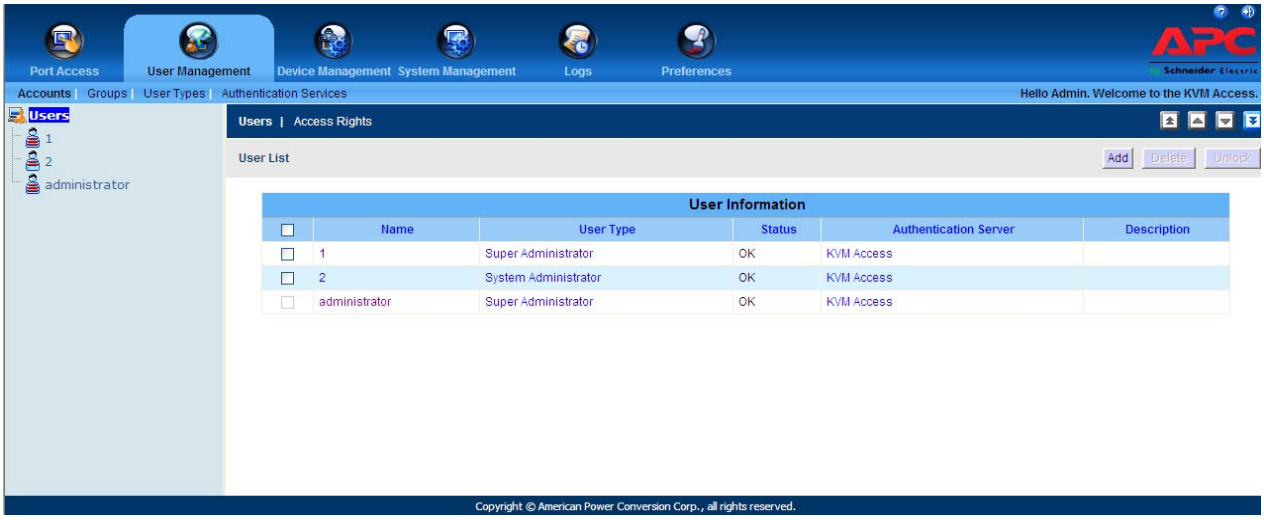
Overview

The User Management page is used to perform the following functions:

- Add, modify and delete user accounts.
- Create user groups and assign users to them.
- Specify device access rights for users and groups based on system default or custom defined user types.
- Specify whether the user's authentication will be performed via the KVM ACCESS (internal) or via an external authentication server.

Click the User Management tab to open the default Accounts page. All users and groups, are listed in the Sidebar and in a table in the Interactive Display Panel. To access any user or group, click on the name in either location.

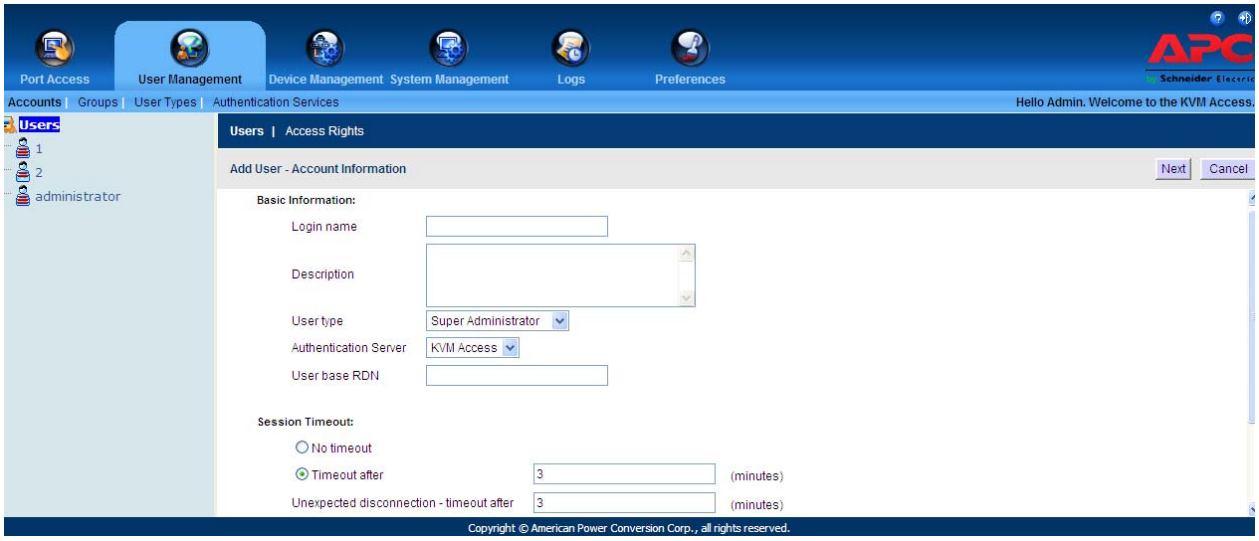
Note: The User Management page is for System Administrators and User Administrators.



Accounts

Add a user account

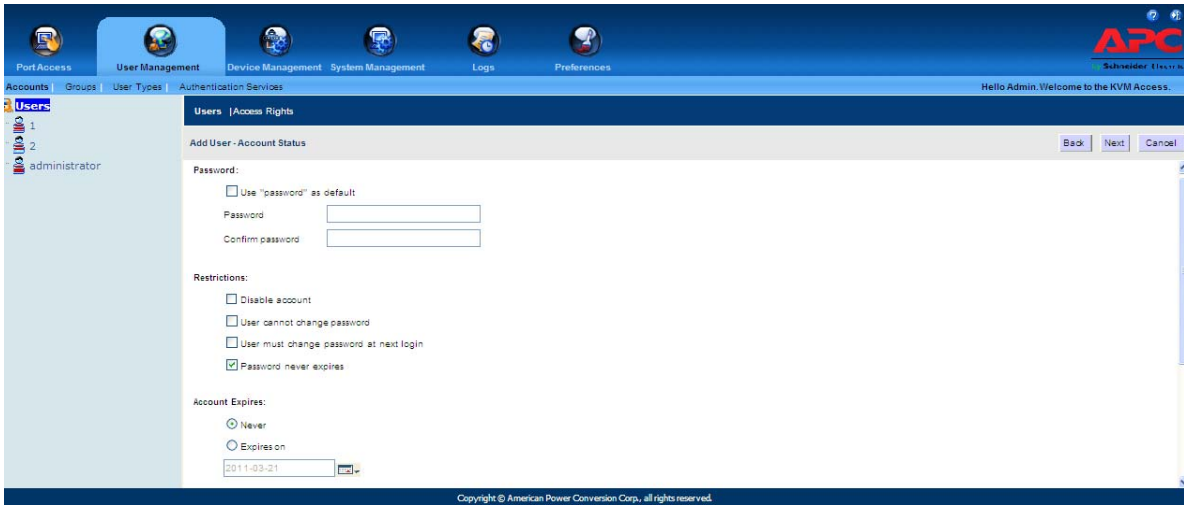
1. Select **Users** in the Sidebar.
2. Click **Add** at the top-right of the main panel to open the Add User-Account Information page.



3. Enter the information in the fields.

Field	Description
Login Name	• Internal (KVM ACCESS) Accounts: A maximum of the equivalent of 16 English alphanumeric characters is allowed. The minimum number of characters is based on the KVM ACCESS's account policy settings (see “KVM ACCESS Authentication” on page 44). • External Authentication: The Login name should be one that exists on the external authentication server. • **Note:** These external servers provide authentication services only. They do not provide authorization services. Authorization is provided through the KVM ACCESS system, therefore the access rights need to be set in KVM ACCESS.
Description	Optional additional user information is included here. A maximum of 256 Bytes is allowed.
User Type	Assign the new user a User Type from the drop down list. See p. 62 for details.
Authentication Server	• For authentication by KVM ACCESS, leave the selection as is. For authentication by an external authentication service, select one from the drop down list. • **Note:** Before making this selection, an external authentication server must first be added. See “External Authentication Servers” on page 45, for details.
User Base RDN	If the authentication server is an LDAP server, the user's base RDN (Relative Distinguished Name) setting must be in this field.
Session Timeout	• To have a session time out after the user has been idle for a specified amount of time, select the **Timeout after** radio button. Valid settings are from 1-99 minutes. The default is 3 minutes. • To have no session time out, select the **No timeout** radio button. • **Note:** This setting pertains to Web log in sessions.
Unexpected Disconection Timeout	If the user unexpectedly disconnects (closes the browser), KVM ACCESS ends the session after the time specified here. The setting is from 3-10 minutes. The default is 3 minutes.

4. Click **Next** at the top-right of the main panel. If KVM ACCESS was chosen for authentication, the Add User-Account Status page opens.



Field	Description
Password	• Click the checkbox to the left of **Use "password" as default** to set the user's password as the word **password**. • If you do not select **Use "password" as default**, enter the user's password in the Password field. A maximum of the equivalent of 16 English alphanumeric characters is allowed. The minimum number of characters is based on KVM ACCESS's account policy settings (see "KVM ACCESS Authentication" on page 44). • Entert the password again in the **Confirm Password** field. The entries must match.
Restrictions	• **Disable account** temporarily cancels a user's account without deleting it. The account can be reinstated. • If **User cannot change password** is enabled, the user can't change his own password. Otherwise, the user can use the **Preferences** tab to change his own password. See "Password" on page 18 for details. • If **User must change password at next login** is enabled, the user must change his password the next time he logs in. • Enabling **Password never expires**, prevents the user's password from expiring. This overrides the system configuration set on KVM ACCESS's account policy settings (see "KVM ACCESS Authentication" on page 44).
Account Expires	• Click the **Never** radio button so that the account never expires. • To have the account expire on a certain date, click the **Expires on** radio button, then click the calendar icon to select the expiration date.

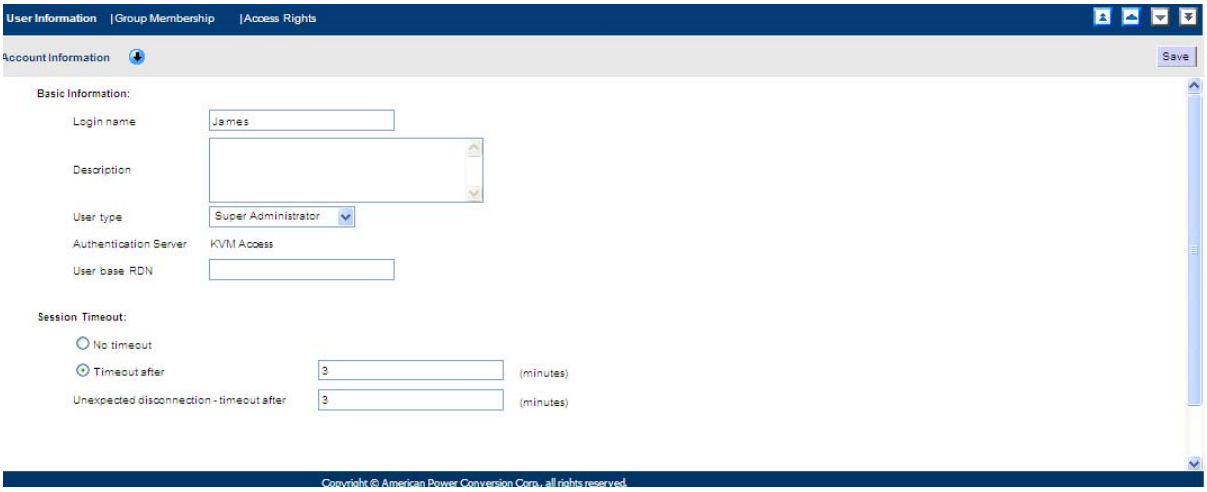
Note: If an external authentication server is used, the account status information is maintained on that server, so this page **does not** appear. Instead, the Add User-Personal Information page opens.

5. Click **Next** at the right of the panel to open the **Add User - Personal Information** page. The fields are optional and may be left blank or filled in.
6. When finished, click **Save** to open the **Add Access Rights** page and set the user's access rights to the devices and ports on the installation. See "Access Rights" on page 33 for details.
7. Click **Save** to add the user to the Users list, and open the Access Rights Summary page. See "Access Rights" on page 33, for details.

Note: To add additional users, click **Users** in the Sidebar to start.

Managing User Accounts

1. Select **Users** in the Sidebar.
2. Click the user's name in the Sidebar, or in the main panel to open the user's **Account Information** page. There are three Panel Menu items: User Information, Group Membership, and Access Rights.



User Information.

This item contains all three pages (Account Information, Account Status, and Personal Information) used in the Add a User task (see page 31). The pages are used to modify a user's account (such as changing the user's password). Click the arrow icons, or hover the cursor over the menu and select from the menu.

Group Membership.

Click to open a list of all the groups to which a user belongs. Click on a group name in the list to go to the group's Group Information page. See “Groups” on page 37 for details.

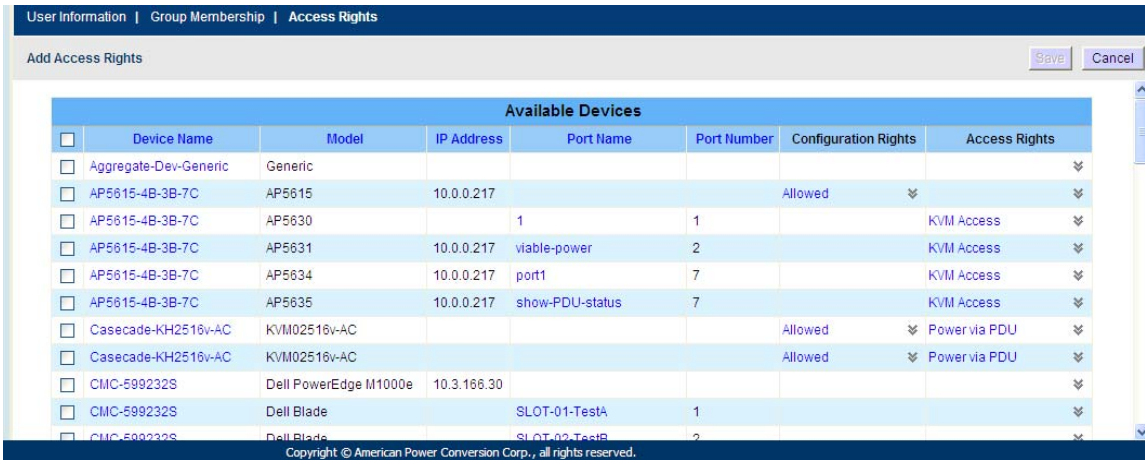
Access Rights.

To configure a user's access rights to devices, ports, and outlets:

1. Select Accounts on the Menu Bar.
2. Select the User in the Sidebar.
3. Select Access Rights in the Interactive Display Panel to open the user's Access Rights page. If no devices have been assigned to the user, the page will have no devices in the list.

Adding Device Access:

1. Click the **Add** button to open a list of all the devices on the installation.
2. Put a check in the boxes next to the devices, ports, and outlets that you want the user to access.
3. For each selection, click on the arrow in the **Configuration Rights** column.
   Allowed lets the user configure the device or port settings.
   Denied means that the user cannot configure the device or port settings.
4. For each selection, click on the arrow in the **Access Rights** column to set the user's access rights.



Rights	Port Type	Descriiption
Full Access and USB	KVM	The user can access the device (or specified ports on the device), view the screen and perform I/O operations with the keyboard and mouse. The user also has rights to use the virtual media function.
Full Access	KVM	The user can access the device (or specified ports on the device), view the screen and perform I/O operations on it with the keyboard and mouse.
View Only	KVM	The user can access the device (or specified ports on the device) and view the screen, but cannot perform operations.
No Access	KVM	The user has no access to the device (or specified ports on the device). The device (or the specified ports) will not appear in the Sidebar or List.
Allowed		The user is allowed to configure the power status of the device (or specified ports on the device).
Denied		The user is not allowed to configure the power status of the device (or specified ports on the device). The device (or specified ports) does not appear in the Sidebar or List.
Administrator	Generic Web SSO	The administrator can perform all configurations and operations.
User	Generic Web Access	The user can perform all operations.
View Only	Generic Web Access	The user can view the screen, but cannot perform any operations.
No Access	Generic Web Access	The user has no access. The Web Access option does not appear as an Operation choice on the Port Access page.

5. Click **Save** when finished.
6. To add access for additional devices, open the user's Access Rights page and repeat the steps.

Modifying Device Access. To change the access rights to a device, port, or outlet, open the user's Access Rights page; make the changes to the desired items; then click **Save**.

Removing Device Access. To remove access to a device, port, or outlet, open the user's Access Rights page; place a check in the box in front of the device you want to remove; then click **Delete**.

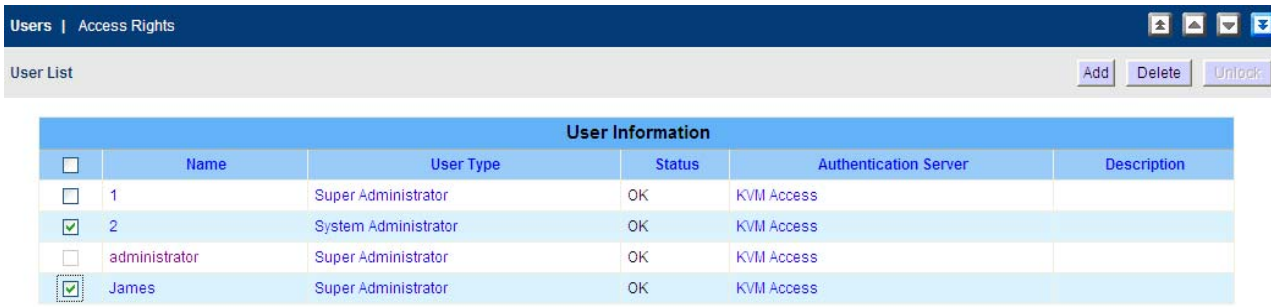
Managing Devices. Open the Management page of any device, port, or outlet, by clicking on it in the Device Name or Port Name list.

Deleting User Accounts

1. Select Users in the Sidebar.
2. From the Interactive Display panel, check the box of the user whose account will be deleted.

   Note: Delete more than one user by checking as many names as required. Delete all accounts by checking the box at the top of the column.

3. After making your selection, click **Delete**.
4. In the popup that opens, click **OK**.

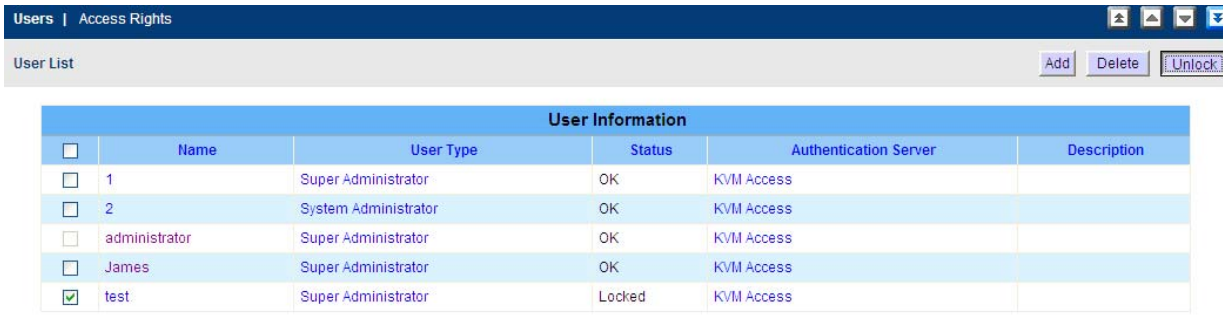


Unlocking User Accounts

If a user is locked out after exceeding the allowed login attempts, and the **Force Manual Unlock** option has been enabled (see “Lockout Policy” on page 94):

1. Select Users in the Sidebar. The locked user account will show **Locked** in the Status column.
2. In the Interactive Display panel, check the user whose account you wish to unlock.
3. Click **Unlock** at the right of the panel.
4. In the popup that opens, click **OK**.

Note: 1. Unlock more than one user by checking as many names as required. Unlock all locked accounts by checking the box at the top of the column.
2. If all users, including the System Administrator, get locked out, the System Administrator can use the KVM ACCESS Utility to restore his account and then unlock the users. See “Restore” on page 111.

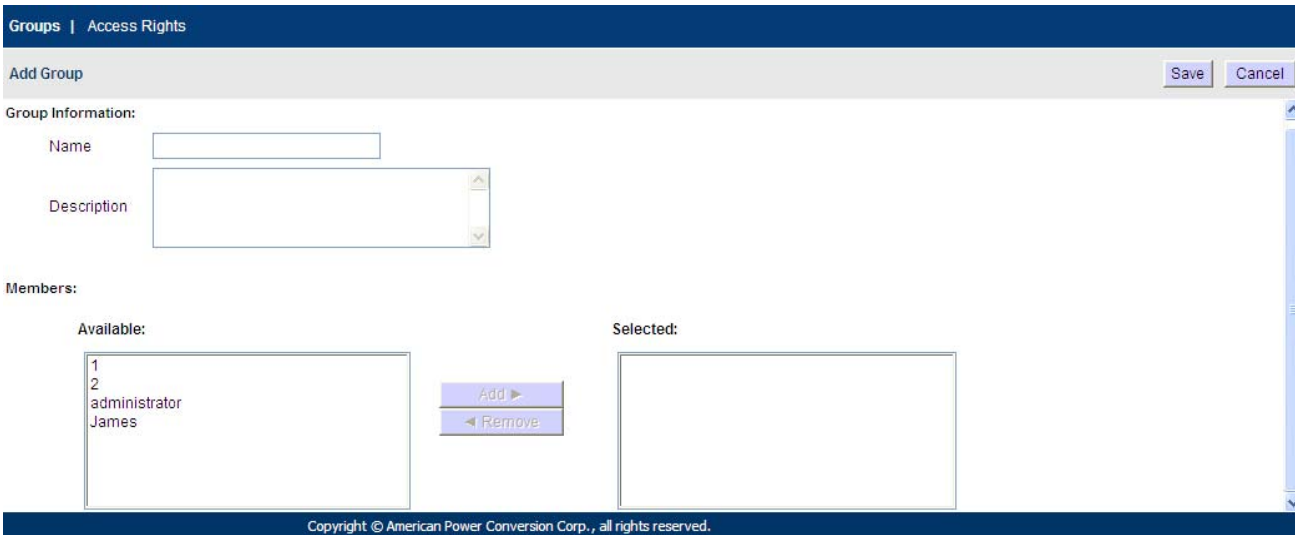


Groups

Groups allow administrators to manage users and devices. Since device access rights apply to anyone who is a member of the group, administrators set them once for the group, instead of for each user individually. Multiple groups can be defined to allow some users access to specific devices while restricting other users.

Creating Groups

1. Select **Groups** from the User Management menu bar to open the Group List page.
2. Click the **Add** button at the top-right of the main panel to open the Group Information page.



3. Enter a Name and Description (optional) for the group.

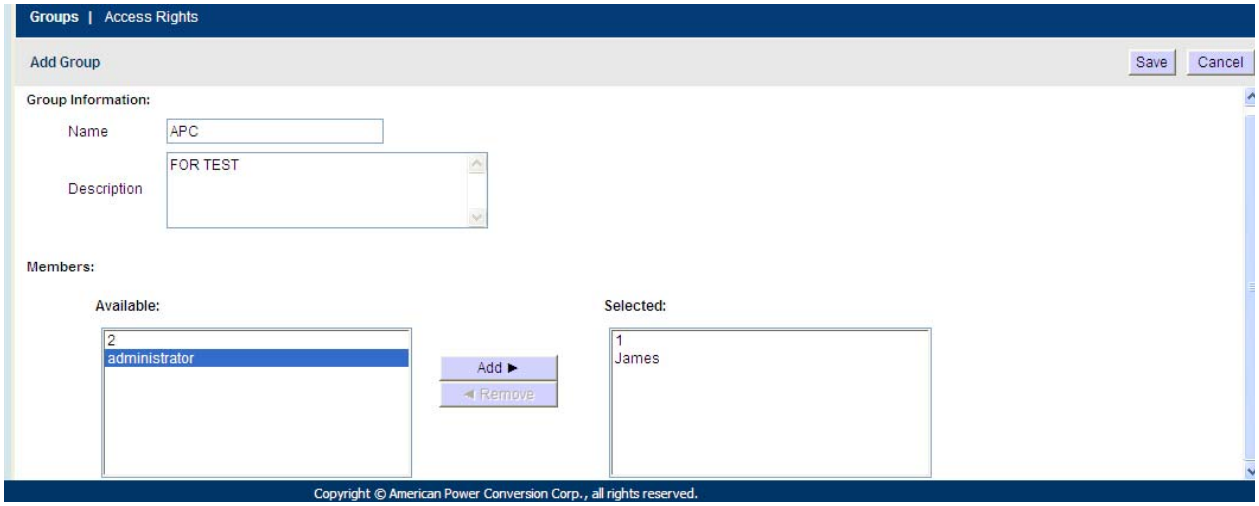
Note: 1. The Name can be the equivalent of from 2-32 English alphanumeric characters, but cannot contain the following: / \ [ ] :;|=,+*?<>@'"
2. The Description can be up to 256 Bytes.

4. Click **Save** to create the group. The group now appears in the Sidebar and the Group Information list in the Interactive Display Panel.

Note: You can add users to the group before performing this step. See the next section for details on adding users to groups.

Adding Users to Groups

1. Select **Groups** from the User Management menu bar.
2. In the Sidebar or the Interactive Display panel, click the group's name to open the Group Information page.
3. Select the user you wish to add to the group from the **Available** list, then click the **Add** button to move the user from the **Available** list to the **Selected** list.



4. Repeat step 3 for other users you wish to add to the group.

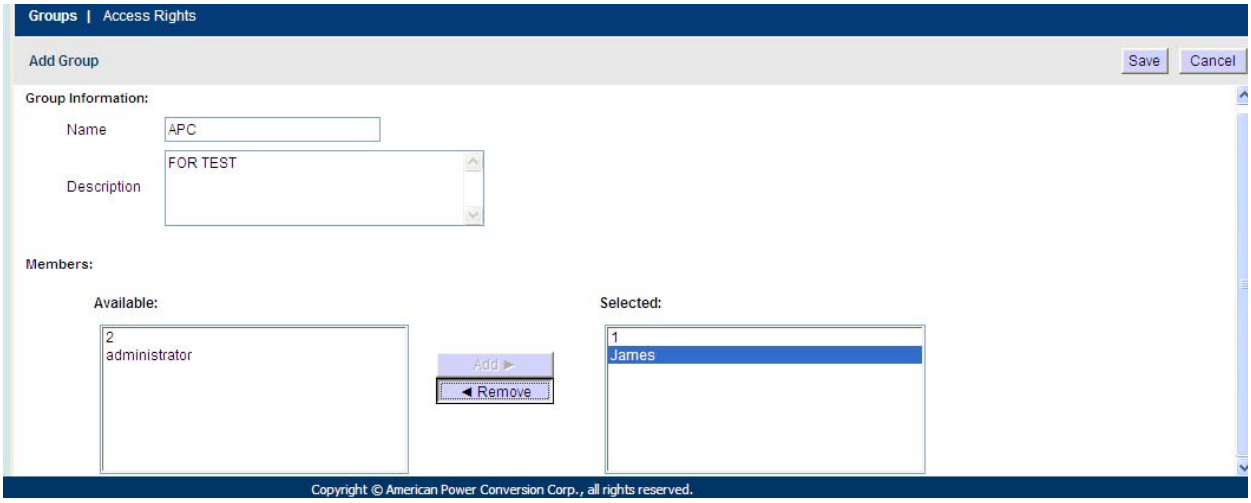
Note: A shortcut for adding multiple users is to select the ones you want in the Available column using **Ctrl+Click** or **Shift+Click** before clicking the **Add** button to move all the selected ones at once.

5. When you have finished adding users, click the **Save** button to complete the procedure.

Note: If a user has permissions in addition to the ones assigned to the group, the user keeps those permissions in addition to the group permissions.

Removing Users from Groups

1. Select Groups from the User Management menu bar.
2. In the Sidebar or the Interactive Display panel, click the group's name to open the Group Information page.



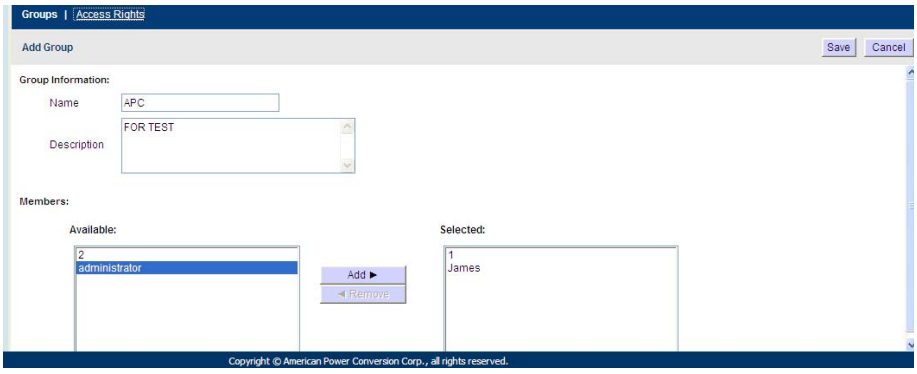
3. Select the user to be removed from the Selected list, then click the **Remove** button to move the user from the **Selected** list to the **Available** list.
4. Repeat step 3 for any other users you wish to remove from the group.

Note: Note: A shortcut for removing multiple users is to select the ones you want in the Selected column using **Ctrl+Click** or **Shift+Click** before clicking the **Remove** button to move all the selected users at once.

5. When you have finished removing users, click the **Save** button to complete the procedure.

Access Rights

1. Select Groups from the User Management menu bar to open the Group List page.
2. Select the group for which you want to configure the access rights.
3. In the Group Information page that opens, select Access Rights on the Panel Menu bar:



The procedures for configuring Group access rights are similar to those described for User Accounts. See “Access Rights” on page 33, for details.

Types

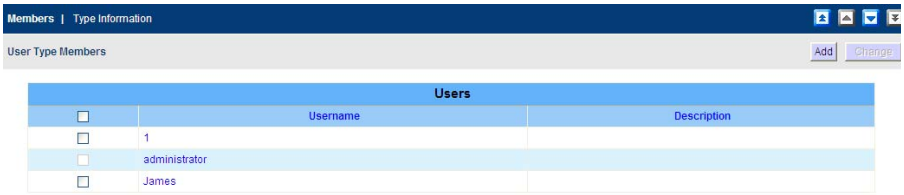
There are two user type categories: System and Custom. By default, KVM ACCESS supports six user types. These are referred to as System user types because they are built into the system. The roles assigned to members of these user types are fixed and cannot be changed.

The Custom category provides the flexibility of assigning various role combinations.

When you click Types on the menu bar, the User Type List opens in the Interactive Display panel, showing all the user types that have been configured:

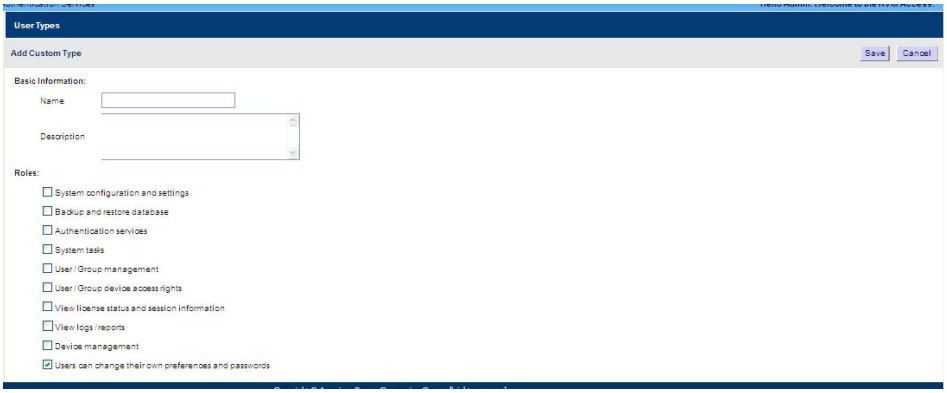
User Types

Members. Clicking a user type in the Sidebar or in the Interactive Display panel opens the Members Panel Menu page showing all the users that belong to that type.



- Click on a user's name to see that user's Account Information page.
- To add a user to the type, click the **Add** button at the top-right of the main panel. In the page that opens, select the user you would like to add, then click **OK**.
- To change the user's type, check the box in front of the user's name, then click the **Change** button at the top-right of the main panel. In the page that opens, select the new type for the user, then click **OK**.

Type Information. From the Members page, click on **Type Information** to see a description of that user type and the roles that are assigned to it.



Note: The only change you can make on this page is in the Description field where additional information can be added about the user type.

System Types

The roles performed by members of the System category are fixed.

Assigned Roles	Super Admin	System Admin	User Admin	Device Admin	User	Auditor
System configuration and settings	✔	✔				✔
Backup and restore database	✔	✔				✔
Set /Change relationship	✔	✔				✔
Authentication services	✔	✔				✔
System tasks	✔	✔				✔
User/Group management	✔	✔	✔			✔
User / Group device access rights	✔	✔	✔			✔
View license status and session information	✔	✔				✔
View logs / reports	✔	✔	✔	✔		✔
Device management	✔	✔		✔		✔
Users can change their own preferences and passwords	✔	✔	✔	✔	✔	✔

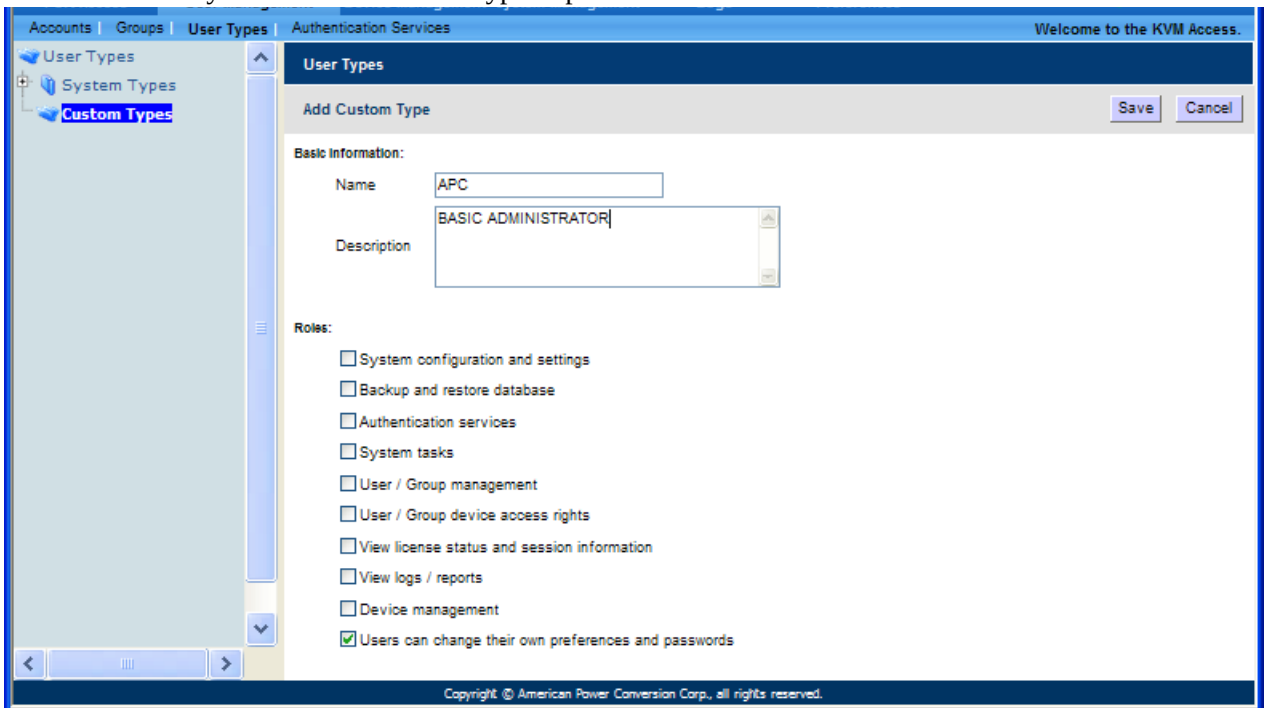
Super Administrator and System Administrator differences. The Super Administrator is authorized for all roles and access to all devices, ports, and outlets. The roles can't be changed. Each of the System Administrator's roles can be assigned manually, and access to devices, ports, and outlets must be assigned manually. The Super Administrator's user type cannot be changed while the System Administrator's type can be changed.

Auditor access. The Auditor type can access all tabs and pages, but has **View Only** rights. Under the Log tab, the Auditor type can export and print logs in addition to viewing them, but cannot change any settings. Under the Preferences tab, the Auditor type can change Web Options and Password settings.

Custom Types

Create custom user types, with any combination of roles assigned to them. Custom types may better suit your requirements than the pre-defined System types.

1. Select **Types** from the User Management menu bar.
2. In the Sidebar, click **Custom Types** to open the User Type List. All Custom user types that have been configured are displayed.
3. Click **Add**. In the page that opens, enter a name and description for the new type, then check the roles you want the new user type to perform.



Note: 1. The Name can be the equivalent of from 2-32 English alphanumeric characters, but cannot contain the following: " ' \
2. The Description can be up to 256 Bytes.

4. When your selections have been made click the **Save** button.

Authentication Services

KVM ACCESS provides an internal Username / Password authentication service. In addition, KVM ACCESS supports the following third party external authentication servers: LDAP, Active Directory, RADIUS, TACACS+, and Windows NT Domain.

Note: 1. Authentication refers to determining the authenticity of the person logging in; authorization refers to assigning permission to use the device's various functions.
2. These external servers provide authentication services only - they do not provide authorization services. Authorization is provided through the KVM ACCESS system.

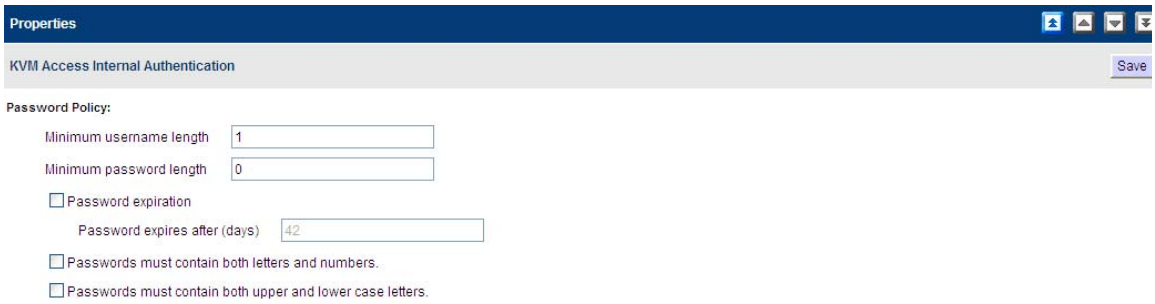
By adding an external authentication server to the KVM ACCESS system (see page 45 for details), when you add a user account, you can select the external authentication server from the list of authentication servers (see “Add a user account” on page 31).

Click Authentication Services on the menu bar to open the Authentication Server List in the Interactive Display panel and show all the authentication services that have been configured.

KVM ACCESS Authentication

There are some configuration settings you can make to the password policy function. All user accounts must follow the requirements you set here. To configure KVM ACCESS's password policy:

1. Select Authentication Services from the User Management menu bar.
2. In the Sidebar or the Interactive Display Panel, click **KVM ACCESS** to open the Properties page.



3. Configuration choices:

Item	Description
Minimum username length	1-16 English alphanumeric characters. The default is 6 characters.
Minimum password length	0-16 English alphanumeric characters. The default is 6 characters. 0 means that no password is required. A no password condition is not recommended.
Password expiration	For security purposes, users can be forced to renew their passwords at specific time intervals. Enable Password expiration and specify the number of days before the password will expire. Once a password expires, a new one must be set. Passwords start expiring from the time an account is created, or a new password is set.
Passwords must contain both letters and numbers	For security purposes, enabling this setting is recommended to force users to include both letters and numbers in the password.
Passwords must contain both upper and lower case letters	For security purposes, enabling this setting is recommended to force users to include both upper and lower case letters in the password.

4. When finished, click the **Save** button.

External Authentication Servers

In order to use a third party external authentication server, you must first add it to the Authentication Server list.

1. Select Authentication Services from the User Management menu bar to open the Authentication Server list.

2. Click the **Add** button at the top-right of the main panel to open the Add Authentication Service page. Click on the Server type to see the list. Select the service you want to add; give it a name and description, then click the **Next** button at the top-right of the panel.
3. The service you have chosen determines the page that opens. Follow the Wizard's pages, entering the information required for the external authentication server you selected. When you have finished, click the **Save** button.

Note: 1. The Server name can be the equivalent of from 2-32 English alphanumeric characters, but cannot contain the following: " '
2. The Description can be up to 256 bytes.

Service Information.

1. LDAP

Heading	Information
Connection Settings	Get the information for these fields from the LDAP administrator. The port default is 636. Check with the LDAP administrator to confirm. For example settings see “LDAP/LDAPS - OpenLDAP Setting Example” on page 118.
SSL Mode	• Click the **Do not use SSL** radio button to use LDAP.
LDAP User Schema	Get the information for these fields from the LDAP administrator. For example settings see “LDAP/LDAPS - OpenLDAP Setting Example” on page 118.
Browsing Method	When adding or modifying user accounts (see “Add a user account” on page 31), click the **Browse** button to see all users in User RDN to choose the Login name. • Select **Browse with user credentials** to allow the user to browse LDAP using credentials configured on the server. When selected, the user does not have to input his credentials each time he browses. • Select **User must input credentials** when browsing to have the user input his credentials each time he browses the LDAP.

2. Active Directory

Heading	Information
Connection Settings	Get the information for these fields from the Active Directory administrator. For example settings see Active Directory Settings Example, page 239.
SSL Mode	Click a radio button to choose whether or not to use SSL in Trust All mode.
Browsing Method	• Select **Browse with user credentials** to allow the user to browse the Active Directory using credentials configured on the server. When selected, the user does not have to input his credentials each time he browses. • Select **User must input credentials** when browsing to have the user input his credentials each time he browses the Active Directory.

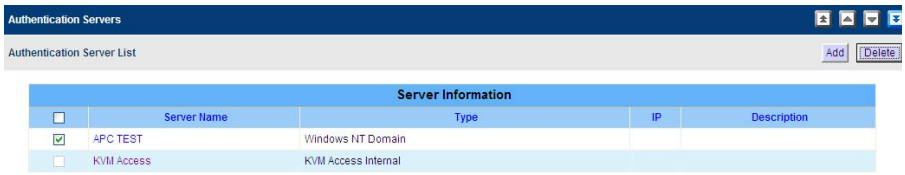
3. RADIUS and TACACS+

Heading	Information
Connection Settings	Get the information for these fields from the service administrator. The default for RADIUS is 1812; the default for TACACS+ is 49. Check with the service administrator to confirm. For example settings see “RADIUS Settings Example” on page 120 and “TACACS+ Settings Example” on page 121.
Authentication Settings	Get the information for these fields from the service administrator. For example settings see “RADIUS Settings Example” on page 120 and “TACACS+ Settings Example” on page 121. 1. Select the Authentication type your RADIUS server is configured for from the drop down list. 2. In the Shared Secret field, enter the character string that you use for authentication with the RADIUS server. 3. Enter the shared secret again in the Confirm Shared Secret field.

4. Windows NT Domain
   Get the Domain Name information from the service administrator. For example settings see “NT Domain Settings Example” on page 121.

Deleting an External Authentication Server.

1. Select Authentication Services from the User Management menu bar to bring up the Authentication Server list.
2. In the Interactive Display panel, click to put a check in front of the external authentication server you wish to delete.



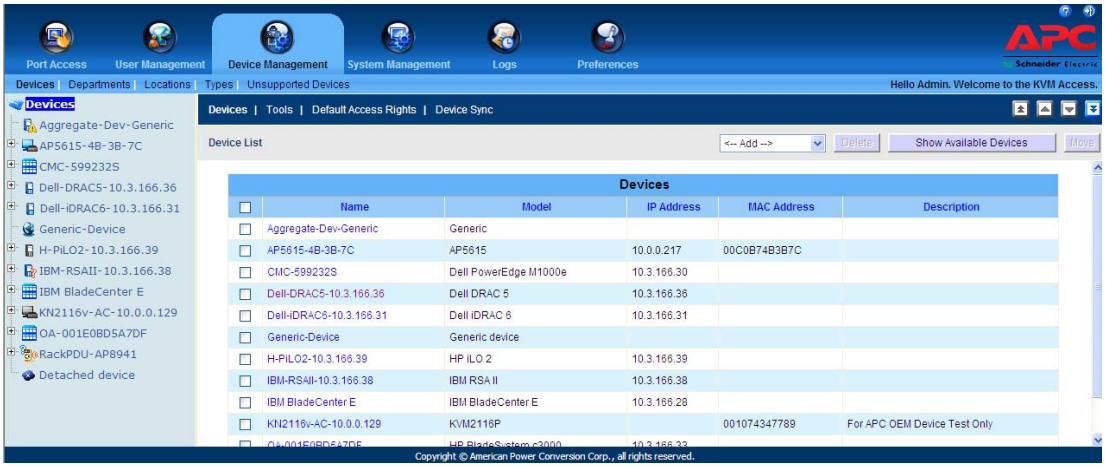
Note: 1. Delete more than one server by checking as many names as required.
2. Delete all eligible servers by checking the box at the top of the column.
3. If a user account has been created on KVM ACCESS that uses an external authentication server, the server cannot be deleted.

3. After you have made your selection, click **Delete** at the right of the panel.
4. In the confirmation popup that opens, click **OK**.

Device Management

Overview

Use the Device Management page to add, configure, and organize the devices that will be managed over the KVM ACCESS network. Click the Device Management tab to open KVM ACCESS to the default Devices page.



All devices and device folders in the KVM ACCESS database are listed in the Sidebar and in a table in the Interactive Display Panel. To access any device, click on it in either location.

Note: The Device Management page is for System Administrators and Device Administrators. Other user types do not have access.

Preliminary Procedures

Before devices can be managed, they must first be added into the system.

1. Connect the devices to the same network segment as the KVM ACCESS.
2. Once the devices have been connected to the same network segment as KVM ACCESS, KVM ACCESS must be made aware of them. This can be done by enabling the the Management function on the device's ANMS page (see page 104), or with the Initialize devices IP/Port function on the Tools menu (see page 61).

   Note: 1. The KVM ACCESS server can prove that the devices connected have been successfully recognized. Click the **Show Available Devices** button. If the devices have been successfully recognized, they will appear in the list that opens.
   2. Click the **Show Available Devices** button to list all the available devices. (This gives the same result as the **Add device** drop down list.)
   3. Devices that already have been added to the KVM ACCESS system do not appear in the list of available devices.
3. Next, the devices recognized in step 2 must be added to the management system (see “Adding a Folder or Device” on page 51 for details).
4. Finally, devices can be created either as actual physical port devices (by unlocking each port), or by combining various ports into logical device constructs (Aggregate Devices, Group Devices, etc.). See “Creating Devices” on page 53 for details.

Using VPN

In some installations you may prefer to use a VPN (virtual private network) environment for your KVM ACCESS functions. This is accomplished by enabling the Management function (on the device's ANMS page - see page 104) and entering the IP address of the KVM ACCESS. See “VPNs” on page 104, for more details.

Menu Structure

The Device Management menu structure:

Tab	Page Menu	Panel Menu	Page
Device Management	Devices	Devices	49
		Tools	61
		Device Sync	63
	Sidebar Device Tree	Properties (KVM)	63
		Access Rights (KVM)	65
		Device Configuration (KVM)	67
		Port Configuration (KVM)	68
		Properties (PDU)*	68
		Access Rights (PDU)*	69
		Device Configuration (PDU)*	70
		Outlet Configuration (PDU)*	70
	Departments, Locations, Types		71
	Unsupported Devices		72
* This item only appears when a PDU device is selected.			

Devices Menu

The Devices menu has three Panel Menu items: Devices, Tools, and Device Sync.The default page is the main page of the Devices Panel Menu.

Devices

The Devices Panel Menu is used to add, modify, delete, and organize devices and device folders. All device items that have been configured for use on the KVM ACCESS server and have been added into its database are listed in the Sidebar.

Device types that can be added and configured are found under the **Add** drop down list at the top of the main panel.

Type	Purpose
Device	Select to add devices into the KVM ACCESS system. **Note:** When devices are added all of their ports are locked by default and must be unlocked. See "Locking / Unlocking Ports" on page 60 for details. This allows addition of devices containing ports beyond the number allowed by the license. You can select specific ports to unlock to gain access to critical ports while remaining within the license restrictions.
Aggregate Device	Select to create a logical device consisting of ports selected from devices that have been added to the management system. This is used to manage a device with multiple connection methods (KVM, power, and serial ports, for example), without having to use a separate connection for each. Each Aggregate Device counts as one node regardless of the number of ports it contains, so that creating aggregate devices and adding ports to them allows you to manage a number of ports beyond the physical license restrictions. See Adding an Aggregate Device, page 85 for details. **Note:** 1. A port that has been made part of an aggregate device can only be used with that device. It cannot be assigned to any other device without being removed from the aggregate device. 2. Once a port has been made part of an aggregate device, it is no longer treated as an individual port, and cannot be locked or unlocked manually. If at some point you want to treat this port as a physical port, or add it to a group device you must first delete it from the aggregate device.
Blade Chassis	Select to add a blade chassis.
Generic Device	Third party generic devices (routers, switches, etc.) can consist of any device that contains an Ethernet interface and can be accessed by its URL or IP Address via HTTP/HTTPS, or Telnet/SSH. Since these devices have no provision for CC management, they cannot be authenticated through the KVM ACCESS, and are not part of the KVM ACCESS's single sign on configuration. Generic devices do not occupy device node licenses. There is no proxy support for these devices (see page 104). When you select this type of device the KVM ACCESS redirects to the device, itself. You must log in to the device using its own authentication procedure. **Note:** Generic Devices do not count against the number of license nodes.
Group Device	Group devices are also created as a composite of ports that exist on actual devices. The differences between Group and Aggregate Devices are: Once a physical port is added to an Aggregate device, it cannot be used with any other Aggregate Device - whereas a physical port can be added to any number of Group Devices **Note:** 1. Group Devices do not count against the number of licensed nodes. 2. A physical port that is added to more than one Group Device only counts as one license no matter the number of Group Devices to which it is added.
Folder	Device folders provide another method (in addition to Departments and Locations) of organizing related devices into useful categories to make it easy to configure and maintain similar types of objects. **Note:** 1. Folders are containers for devices and do not count against the number of licensed nodes. 2. Since Folders are organizational tools for device management, they do not show up in the Port Access Sidebar or main panel list.

Adding a Folder or Device

1. Click **Add** at the top right of the panel to open the list of items that can be added.

Note: Before dropping down the list, you can click **Show Available Devices** for a list of the physical devices that are available.

2. Click on the item in the list that you would like to add. Depending on your selection, a page appears to provide the interface to set it up.

Adding Folders. An organizational option that allows you to organize your enterprise-wide devices into useful categories. Select **Folder** to open the Add Folder page.

- Enter a name, and a description (optional) for the folder, then click **Save**. The new folder is added to the Sidebar and the Device List table.
- To place devices inside a folder, first select the folder in the Sidebar, then go through one of the Add procedures, described below.

Note: 1. Add devices after selecting the destination folder.
2. Folders can be nested. Complete the “Adding Folders” procedure after selecting the parent folder in the Sidebar.

Adding APC Devices. Add devices into the KVM ACCESS system.

Note: 1. Before attempting to add a device to the KVM ACCESS server, make sure it has been recognized. See “Preliminary Procedures” on page 48 for details.
2. To see a list of devices that are available to add, click **Show Available Devices** .

Select Device to open the Choose Device page listing all the online devices that can be added.

To add a device:

1. Click to put a check in the checkbox in front of the device you wish to add.
2. Click **Next** to open the Configure Device Properties page.

3. Fill in the fields according to the information in the following table.

Field	Information
Basic Information	Name: Provide a name to identify the device. The default is the name given to the device under its independent configuration. If you change the name here, the change only takes place in the KVM ACCESS database. The name on the original configuration remains the same. Model: KVM ACCESS recognizes the device model and fills in this field automatically. It cannot be edited. If the device is a Cat5e KVM switch, the KVM Adapter Cable model displays here. MAC Address: The KVM ACCESS fills in this field automatically. It cannot be edited. Department: For organizational purposes you can establish department categories (R&D, for example), and assign devices to them. If you wish to assign this device to a department, drop down the list of departments previously created and click the one you want. Location: For organizational purposes you can establish location categories (West Coast, for example), and assign devices to them. If you wish to assign this device to a location, drop down the list of locations previously created and click on the location category for the device. Type: For organizational purposes you can specify the type of device. You can drop down the list of types previously created and click the one you want. Description: Optional field. Enter extra information to describe the device here.
Contact Information	Optional fields. The name and telephone number of the device administrator.
Trap Destination	Optional field. The email address of the person who will receive trap notifications.
Restrictions	Hide IP Address: An added security measure, if enabled, keeps the device's IP address from appearing in the Port Access Status and Operation List when users log in via their browser. Hide MAC Address: An added security measure, if enabled, keeps the device's MAC address from appearing in the Port Access Status and Operation List when users log in via their browser.

KVM ACCESS Options	Disable other authentication: An added security measure, if enabled, the device will only accept logins through the KVM ACCESS. While the device is connected to the KVM ACCESS system, users cannot log in to the device using the device's own authentication system, and they can only manage the device through the KVM ACCESS's interface. **Note:** 1. If the device becomes disconnected from the KVM ACCESS system, users will be able to log into the device using the device's own authentication system. 2. If the checkbox is not checked it means that other authentication is enabled and users can log into the device using the device's own authentication system. Enable device log information to be sent to KVM ACCESS: If this feature is enabled, the KVM ACCESS acts as the device's log server - receiving and storing the device's tick event information, and having it available for retrieval. Enable Trap notification to be sent to KVM ACCESS: If this feature is enabled, KVM ACCESS receives notification of Trap events that take place on the device, and stores it for retrieval and auditing purposes. Enable monitor data to be sent to KVM ACCESS. If enabled, environment data that is being monitored is sent to KVM ACCESS to be recorded in its log files. After enabling this feature, drop down the list to set the Time interval between transmissions. Device session timeout: If enabled, when there is no input from the user for the amount of time set with this function, the session is terminated. The setting range is 2- 99 minutes. A setting of 0 (zero) disables this function. The default is 3 minutes.

4. When finished, click **Save** to complete the procedure and return to the main page. The device now appears in the Device List.

Note: 1. After adding a device, its ports are locked. See "Locking / Unlocking Ports" on page 60, for details.
2. For Cat5e KVM switches, only the ports that have a KVM adapter cable attached, and are online are recognized and are added to the Device List. This is because each adapter cable has its own independent identity and if it is not online there is no way for it to be recognized. Once a port has been added, it will appear in the list even if it is off line.

Creating Devices

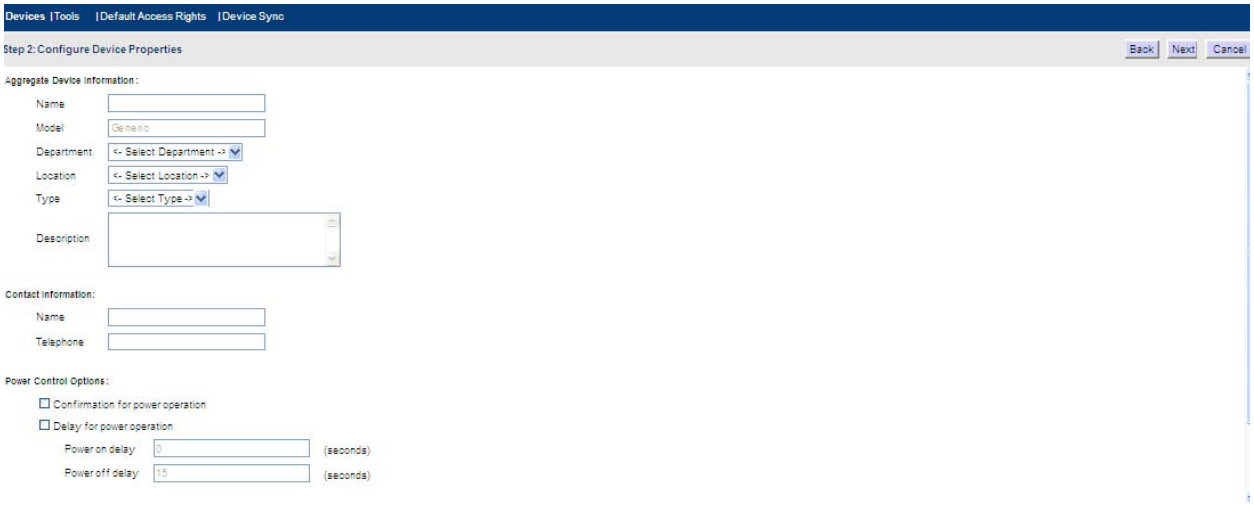
Once devices have been added, several types of logical device constructs can be created by combining various ports.

Adding an Aggregate Device. When you select Aggregate Device as an item to be added, the Add Aggregate Device page opens.

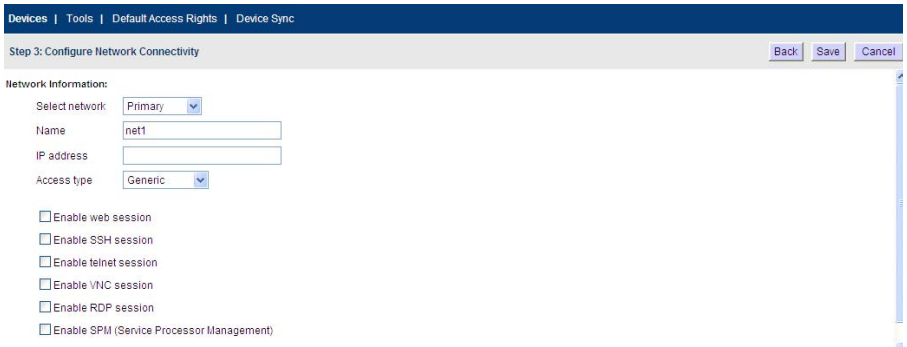
Note: See "Aggregate Device" on page 50, for more information.

To add an Aggregate Device:

1. Choose Aggregate Device Model from the drop down menu. Model options include Generic, IPMI, HP ILO2, IBM RSA II, Dell DRAC 5, and Dell DRAC 6.
2. Click **Next** to open the Configuration Properties page.



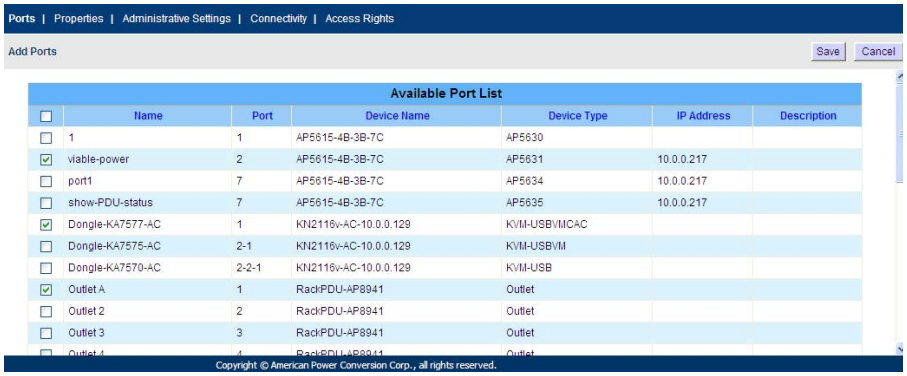
- To configure Aggregate Device properties:
  - Provide a name to identify the aggregate device in the Name field.
  - Provide a further description of the aggregate device in the Description field. (Optional)
  - Drop down the Department, Location, and/or Type list(s) and click on the one(s) to which you want the aggregate device to belong. (Optional)
  - Provide the name and telephone number of the device administrator in the Contact Information field. (Optional)
  - Choose Power Control Options. (Optional)
3. When finished, click **Next** to open the Configure Network Connectivity page.



4. Fill in the fields according to the information in the following table.

Field	Explanation
Network Information	Select the network: If the server for the aggregate device only has one network interface, select Primary, then configure the remaining fields. If it has more than one network interface, after you finish configuring the Primary network interface, come back to choose the additional network interfaces and configure each of them in turn. Name: For convenience, each of the network interfaces can be given a name. IP Address: Select the KVM ACCESS unit to which the Aggregate Device server is connected.
Web Session	IP address, Login name, Password, SSH port: To access the Aggregate Device server via an SSH session, enter the appropriate information into these fields according to the Aggregate Device server's authentication and authorization procedures.
Telnet Settings	To access the Aggregate Device server via a Telnet session, enter the information into the fields according to the Aggregate Device server's authentication and authorization procedures.

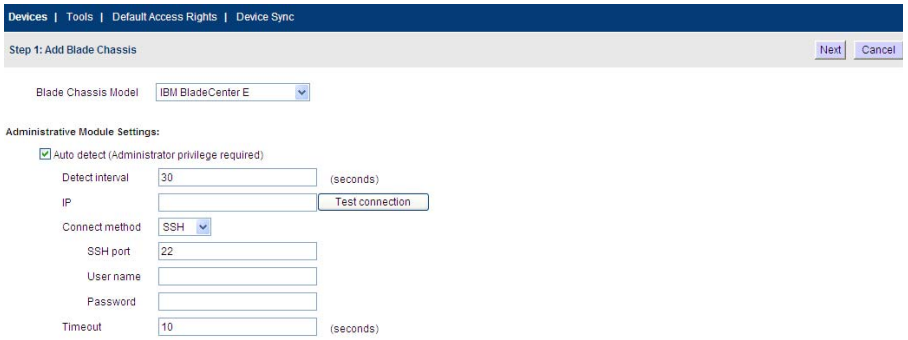
7. When finished, click **Save**. The Add Ports List page opens.



8. Click checkboxes to add ports into this Aggregate Device, click **Save** to open the Access Rights Summary page.
9. Select which user will use this aggregate device from the drop down list and click **Save**. The Ports List page opens showing which ports can be managed under this aggregate device:

Note: 1. Redundant Power settings are only enabled for Aggregate Devices if power outlets have been added to the device.
2. The Properties, Connectivity, and Access Rights Panel Menus bring up pages that offer the same fields as the ones encountered when the Aggregate Device was created. Use them to change any of the device's settings information.
3. Any ports listed on the page can be combined in the Aggregate Device. Put a check in the checkbox in front of the ports that you want, then click **Save**.
4. If a port is already part of another aggregate or group device, a dialog box appears to notify you that it will be removed from the original device when added to this aggregate device and asks you to confirm that this is what you want to do. Click **OK** to accept the change or **Cancel** to abort.

Adding a Blade Chassis. Select Blade Chassis as an item to be added and the Add Group Device page opens.



1. Fill in the fields according to the information provided in the table below.

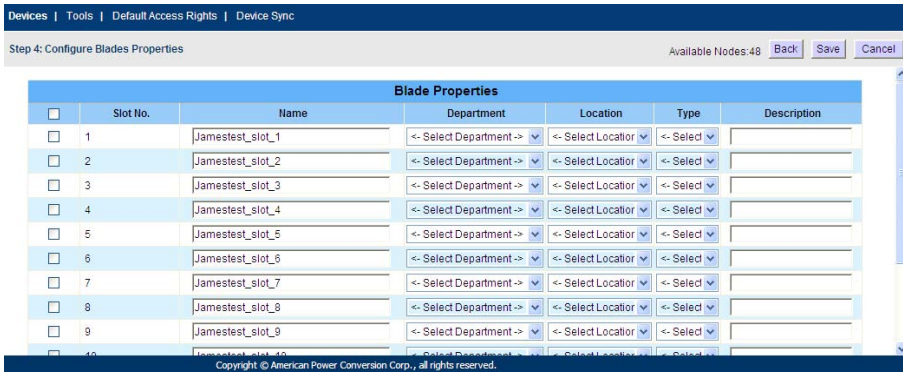
Field	Information
Model	Select the model type to add from the drop down list.
Auto detect	If you enable Auto detect, the Configure Blade Properties information (see page 57) will be filled in automatically.
IP / Port	If Auto detect is not being used, enter the blade server's IP address and the access port used to connect to it (via Telnet or SSH). The default port is 22 (SSH). Click **Test Connection** to confirm that the IP and port settings have been correctly detected.
Username / Password	Enter a username and password to access the blade server (via Telnet or SSH). **Note:** Use an account with administrator privileges to get needed information.
Timeout	Set the waiting time for a connection request to complete before the request is cancelled.
Server	Select the KVM ACCESS unit to which the Aggregate Device server will be connected.

2. When you have finished, click **Next** to open the Configure Device Properties page.
3. Fill in the fields according to the information provided in the table:

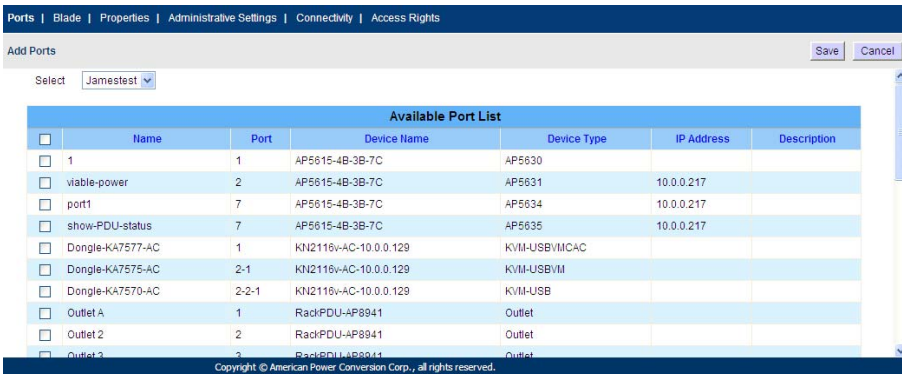
Field	Information
Device Information	Name: Provide a name to identify the device. Description: Optional field to provide extra information to describe the device. Department: For organizational purposes you can establish department categories (R&D, for example), and assign devices to them (see “Departments, Locations and Types” on page 71). To assign this device to a department, drop down the list of departments previously created, and click on the one to which you want the device to belong. Location: For organizational purposes you can establish location categories (West Coast, for example), and assign devices to them (see “Departments, Locations and Types” on page 71). If you wish to assign this device to a location, drop down the list of locations previously created, and click on the one to which you want the device to belong. Type: Drop down the list to select the type of device.
Contact Information	Optional Fields. The name and telephone number of the device administrator.

4. When you have finished, click **Next** to open the Configure Network Connectivity page.
    a. The **Maximum number of slots** field is for information purposes and can't be configured on supported chassis. It can only be set on generic chassis.
    b. Select your preference for the Blade switching hotkey from the drop down the list.
    c. The remainder of the fields are the same as for “Adding an Aggregate Device” on page 53.

5. When you have finished, click **Next** to open the Configure Blade Properties page.



6. For each blade, specify its Department, Location, and Type, and provide a brief Description.
7. When finished, click **Save** to open the Add Ports page.

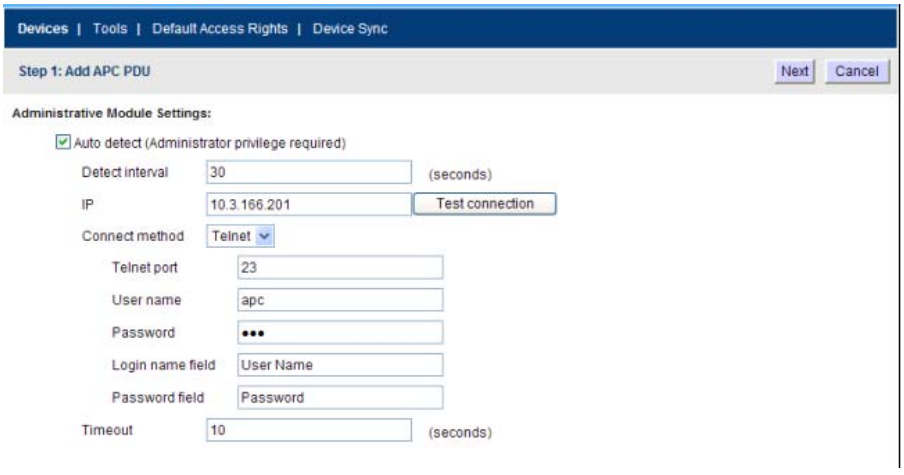


8. Check the boxes for any ports to which the blade chassis connects and click **Save**.

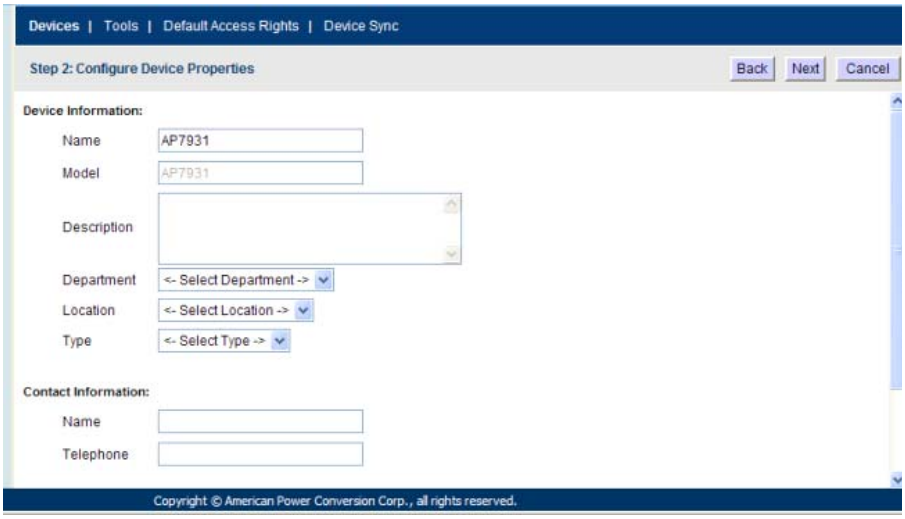
Adding a PDU:

1. Select **Add APC PDU** from the drop down menu.

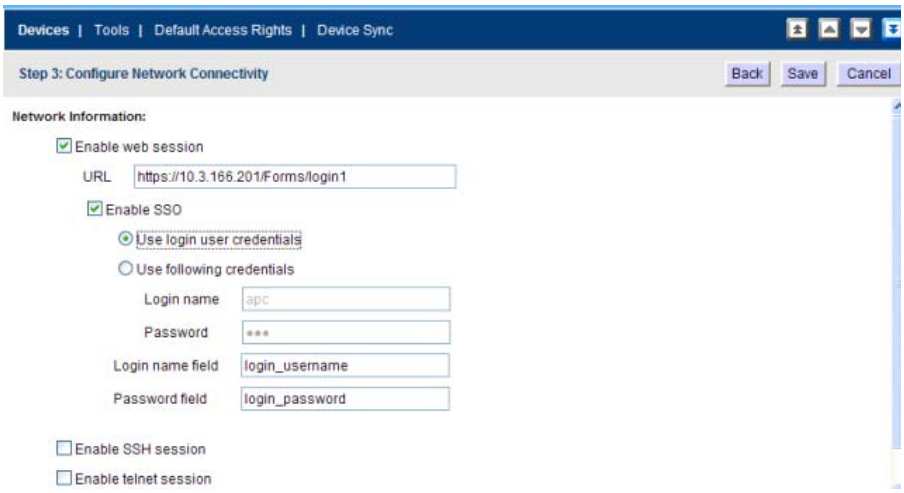
2. Configure the **Administrative Module Settings**. When finished, click the **Next** button.



3. Configure the **Device Properties**. When finished, click the **Next** button.



4. The **Configure Network Connectivity** page opens. Select Enable web session, Enable SSO session, or Enable telnet session. Click **Save** to finish.



Adding a Generic Device. Select Generic Device to open the Add Generic Device page.

Note: See “Generic Device” on page 50, for an explanation of generic devices.

1. Fill in the fields according to the information provided in the table below.

Field	Information
Device Information	Name: Provide a name to identify the device. Description: If you wish to provide extra information to describe the device, enter it here. This field is optional. Department: For organizational purposes you can establish department categories (R&D, for example), and assign devices to them (see "Departments, Locations and Types" on page 71). Open the drop down list of departments previously created, and click on the department to which you want the device to belong. Location: For organizational purposes you can establish location categories (West Coast, for example), and assign devices to them (see "Departments, Locations and Types" on page 71). Open the drop down list of locations previously created, and click on the one to which you want the device to belong. Type: Drop down the list to select the type of device it is.
Contact Information	Optional fields. The name and telephone number of the device administrator.
Network Information	Fill in the fields according to the following information: • If the Generic Device is to be accessed via a web browser, enter its web (or IP) address in the URL field. • If the Generic Device is to be accessed via Telnet or SSH, enter the IP Address in the IP Address field and the Telnet and/or SSH port numbers in their corresponding fields. • If the Generic Device has all three methods available, you can fill in all or any of them that you wish.
Restrictions	Optional setting. As an added security measure, if Hide IP Address is enabled, the device's IP address will not appear in the Port Access Status and Operation List.

2. Click **Save** when finished to return to the Device List page. The Generic Device now appears in the list and in the Sidebar.

To give users and groups access rights to the device:

1. Select the newly added Generic Device in the main panel or the Sidebar, then select Access Rights on the Panel Menu bar to open the User/Group List page.
2. Click **Add** (at the top-right of the panel). The Qualified User/Group List page appears, listing the users who can be given access rights to the device.

3. Put a check in the box if front of the user or group name, then click the arrow at the right of the Access column to open a drop down list of access rights choices.
4. Check the box in front of the rights you want the user or group to have, then click **Save** (at the top-right of the panel) to return to the Device List page. The Generic Device now appears in the list and in the Sidebar.

Note: The items that appear in the access rights panel depend on the settings choices that were made when the generic device was created (see "Network Information" on page 59).

Modifying Devices.

1. Select Devices either in the Sidebar, or on the main menu bar.
2. Select the device you want to modify either from the Sidebar list, or in the main panel list.
3. Make your changes using the links that become available on the Panel Menu bar. See “Sidebar Device Configuration” on page 63 for details concerning these Panel Menus.

Deleting Devices. To delete a device:

1. Select Devices either from the Sidebar list, or on the main menu bar.
2. Click to put a check in front of the device you wish to delete.

Note: You can delete more than one device by checking as many of them as you require. You can delete all of them at once by checking the box at the top of the column.

3. After you have made your selection, click **Delete** (at the top-right of the panel).
4. In the confirmation popup that appears, click **OK**.

Note: When you delete an Aggregate Device, all of its ports return to their original physical devices with their status changed to **locked**.

Detached Devices. Represents devices or ports that have been detected to have some sort of conflict with other valid devices or ports.
Examples:

1. On a KVM ACCESS managed Cat5e KVM switch, if there are Adapter Cables connected to ports 4 and 6, and you remove the adapter from port 4, the KVM ACCESS will assume that the device connected to port 4 is off line.
2. If on the KVM ACCESS managed Cat5e KVM switch you unplug the adapter cable from port 6 and plug it into port 4, the cable's Adapter ID will not match the device information for port 4 stored in the KVM ACCESS's database. The KVM ACCESS will recognize the new Adapter ID for port 4 and will treat the original port 4 Adapter ID as a detached device.
3. If you plug the Adapter Cable originally connected to port 4 in Example 2, into any other port on the KVM switch, KVM ACCESS will recognize the cable's Adapter ID and update its database accordingly, and the cable will not be treated as a detached device.

Detached devices can be found at the bottom of the tree. You can look at the device to try to resolve the conflict. Detached devices that haven't been resolved within 10 days are automatically removed.

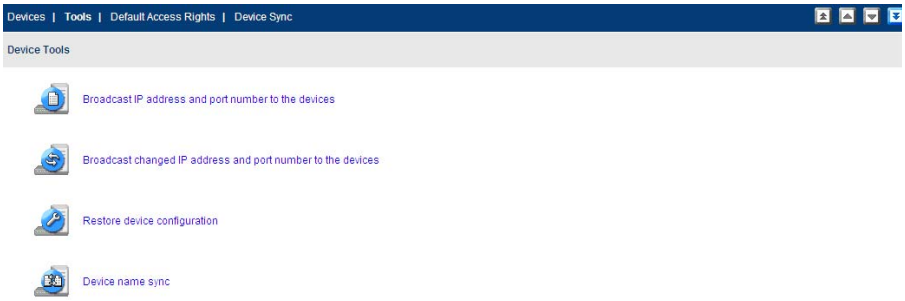
Locking / Unlocking Ports. When physical devices are added to the KVM ACCESS system, their ports are locked by default - to make a port available, it must be unlocked. When a port is selected, two buttons appear at the top-right of the Port Properties page: Lock and Unlock. To unlock a port, select it in the Sidebar or Interactive Display Panel, and click **Unlock**.

The ability to lock and unlock ports allows you to have pre-configured device nodes set up on your installation in excess of the amount licensed. If the total number of device nodes on the installation exceeds the number for which you have been licensed, choose which device nodes to exclude by selecting them and clicking **Lock**. Use them when necessary by locking different ports to create room.

Note: Ports are automatically unlocked when they are added to an Aggregate Device. If only one or two of the device's physical ports are used, it is not necessary to go through the procedure to create an Aggregate Device. Select the target port(s) and click **Unlock**.

Tools

Click **Tools** on the Panel Menu bar to open the page.



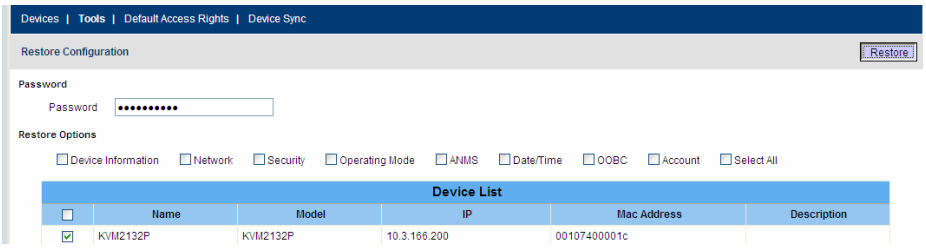
Click an icon to perform a specific task described in the table.

Icon	Icon Name	Task
	Broadcast IP address and port number to the devices	Before a device can communicate with KVM ACCESS, its ANMS settings have to specify KVM ACCESS' IP address and device management port number. Click this icon and KVM ACCESS will broadcast its IP address and device management port number to the devices connected to it on its network. This automatically sets them on the devices (instead of setting them manually on the device itself). This is done the first time a device is connected to the KVM ACCESS network, or if a device has been reset to its default settings. **Note:** 1. This function uses UDP to broadcast the information. Therefore the devices must be on the same network segment (VPN will not work). UDP uses port 18768. Make sure that the network settings for computers that KVM ACCESS is installed on have this port open. 2. For heightened security, once the broadcast is done and the information has been sent to the device, the device will not accept UDP broadcasts from any other KVM ACCESS . 3. If you change KVM ACCESS servers, you must use the ANMS settings page to specify the IP Address and port number (see Device Configuration (For KVM Devices), page 110).
	Broadcast changed IP address and port number to the devices	This feature is used when KVM ACCESS' IP address and/or device management port number changes. Click this icon to broadcast KVM ACCESS' new IP address and/or device management port number to the devices connected to it on its network, automatically updating their ANMS settings accordingly. **Note:** 1. This function uses UDP to broadcast the information. Therefore the devices must be on the same network segment (VPN will not work). 2. For heightened security, the receiving devices will only accept UDP broadcasts from the original KVM ACCESS that initialized them.
	Restore device configuration	This feature is used to restore a device's configuration and/or account information to one saved on a previously backed up configuration file (See "Backup Device Configuration/Account Information" on page 89). See page 62 for the restoration procedure.
	Device Name Sync	If device name changes have occurred, use this feature to manually sync the names between the devices and the KVM ACCESS. See "Device Sync" on page 63 for automatic syncing details.

Restoring Device Configurations. To restore a device's configuration and/or account information to one saved on a previously backed up configuration file:

1. In the **Device Management > Devices > Tools** Panel Menu, click Restore device configuration to open a list of saved configuration files.

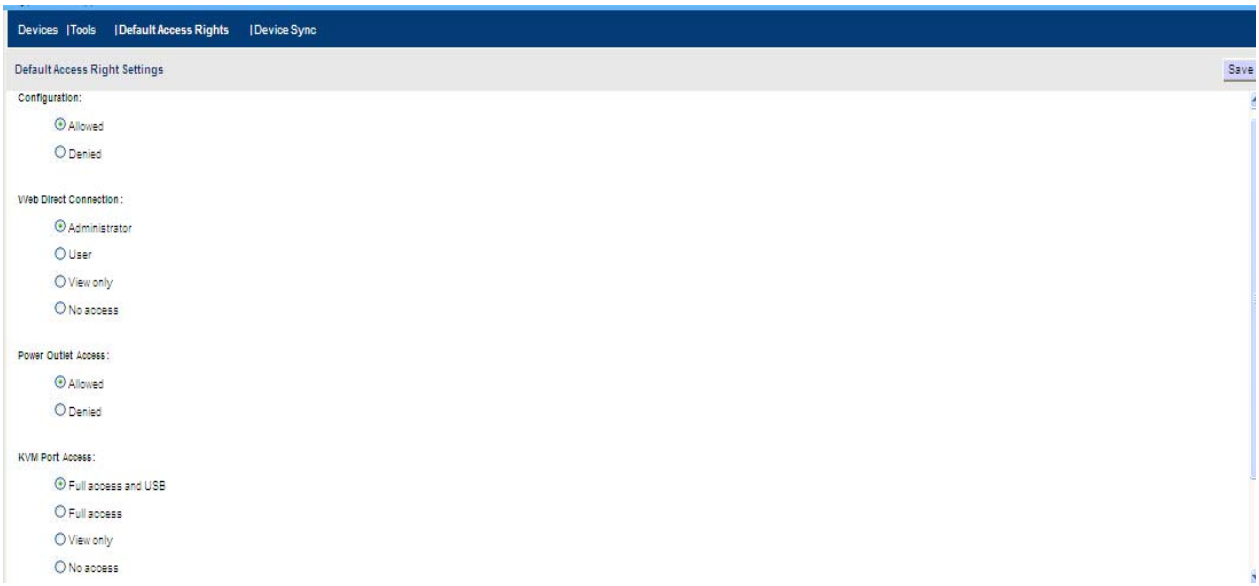
2. Select the file to be restored, then click **Next** to open the Restore Configuration page.



3. In the Password field, enter the password you used when the file was created.
4. Click to put a check in the checkbox to restore only the device account information, only the device configuration settings, or both.
5. Click the checkbox in front of the name of the device you want to restore, then click **Restore**. When the restoration is complete, a message appears informing you of the result.

Default Access Rights

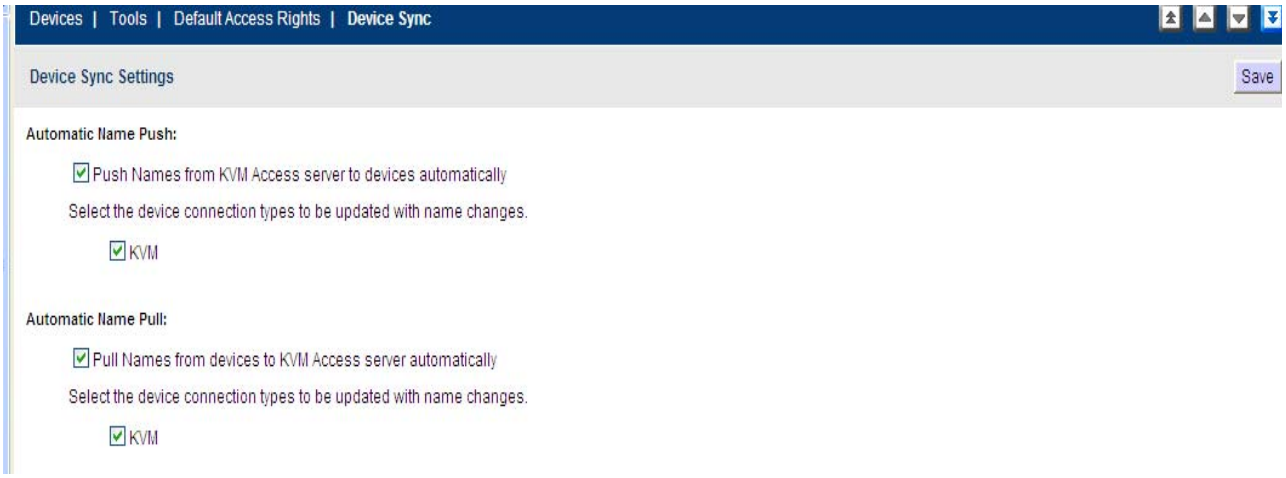
Click Default Access Rights on the Panel Menu bar to open the page.



Configure default access right settings from this page. Check the boxes for the features you want to enable, then click **Save**.

Device Sync

Click **Device Sync** on the Panel Menu bar to open the Device Sync Settings page. Configure automatic syncing of names between the KVM ACCESS and the installed devices. Check the boxes for the features you want to enable, then click **Save**.



Sidebar Device Configuration

Some device configuration aspects are established when devices are created. Manage additional device settings by selecting the device item in the Sidebar or from the Device List in the main panel.

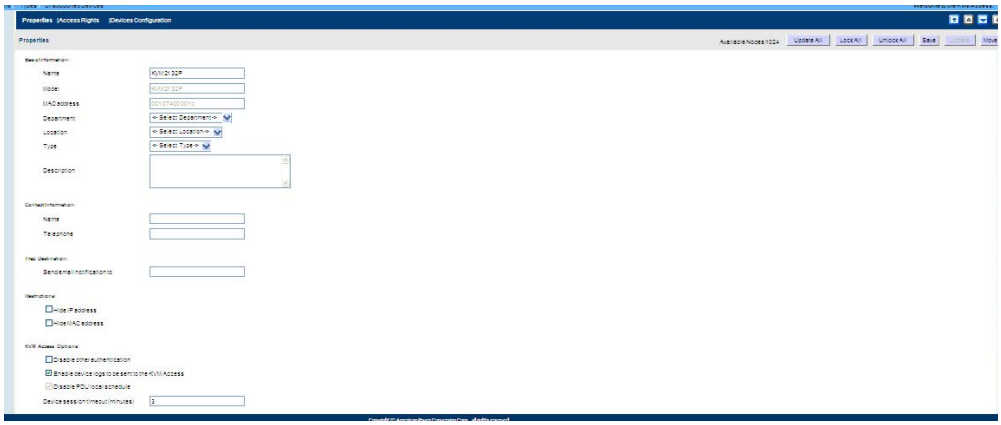
Click a device item to refine the device item's configuration settings. Settings vary depending on the device.

Note: Access rights can be configured on an individual port-by-port basis. Granting access and configuration rights to a device does not mean the user has rights to every port on the device.

KVM Devices and Ports

Selecting a KVM device or one of its ports opens a page with two entries: Properties and Access Rights.

Properties (KVM). The settings found on the Properties page for devices are similar to the ones in the Adding Devices section on page 52.



Properties page contents:

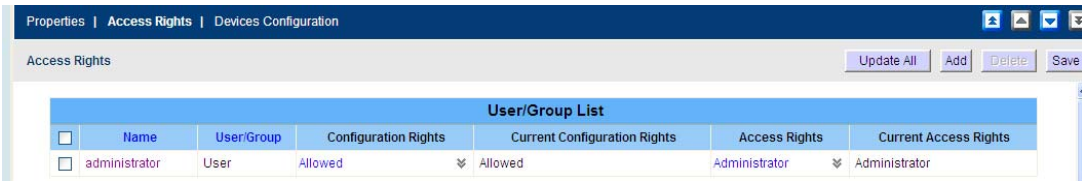
Item	Explanation
Basic Information	**Name:** Provide a name to identify the port. The default is the port name it was given under its original device configuration. If you change the name here, the change only takes place in the KVM ACCESS database. The name on the original configuration remains the same. **Model:** KVM ACCESS recognizes the device model and fills in this field automatically. It cannot be edited. If the device is a Cat5e KVM switch, the KVM Adapter Cable model displays here. **Port ID:** Port IDs are unique and permanent and cannot be edited. KVM ACCESS fills in the field automatically. The ID for Cat5e KVM switch ports is derived from the KVM Adapter Cable ID. **Port Number:** KVM ACCESS ascertains which port on the KVM switch is being configured and fills in this field automatically. It cannot be edited. **Department:** For organizational purposes, establish department categories (R&D, for example), and assign ports to them. Click to select a department (previously created, see page 71) from the list to which the port will belong. **Location:** For organizational purposes location categories (West Coast, for example) can be established, and ports assigned to them. Click to select the location choice from the list (previously created, see page 71). **Type:** For organizational purposes the device type can be specified. Click to select the type from the list (previously created, see page 71). **Description:** Optional field. Enter extra information to describe the port here.
Contact Information	Optional fields for the name and telephone number of the device administrator.
System Macro	If system macros have been made, select one from the drop down list. When you close the KVM viewer the macro will be sent to the server connected to this port and the server will run it. **Note:** This item only appears on ports that have servers connected to them.
Trap Destination	Optional field. The email address of the person who will receive trap notifications.
Restrictions	KVM ACCESS Options includr Disable other authentication, Enable device logs to be sent to the KVM ACCESS, and Device session timeout (minutes)

Properties Page Action Buttons. When a top-level (non-nested) APC device is selected in the Sidebar or the Interactive Display Panel, a series of action buttons appear at the top-right of the Interactive Display Panel.

Action	Purpose
Update All	Click to open a page listing all of the items nested under the top-level device. Configure (or reconfigure) the Department, Location, Type, Description, and Trap Destination of each nested (child) item.
Lock All	If the total number of device nodes on the installation exceeds the number designated by the license, exclude device nodes by locking them. Click the button to lock all of the device's ports. See “Locking / Unlocking Ports” on page 60 for more information.
Unlock All	Click to unlock all of the device's ports.
Save	Click to save any changes made on the Properties page.
Update	If the installation information for a device does not match the information stored in KVM ACCESS' database (if an adapter is moved to a different port, or a new adapter is connected to a port) a question mark is added to the icon in the Sidebar and the Update button is enabled. Select the device in the Sidebar and click **Update** to update the device's installation information in KVM ACCESS.
Move	Click to move the device to a different folder. Select the folder then click **OK** in the dialog box.

When a port is selected only the Lock, Unlock and Save buttons appear at the top-right of the page. These buttons allow you to lock and unlock the ports individually. See “Locking / Unlocking Ports” on page 60 for more information.

Access Rights - KVM Devices. When a KVM device is selected in the Sidebar or the Interactive Display Panel, you can set the configuration and access rights for it by clicking the Access Rights Panel Menu item. This opens a list of all users and groups given access to the device.



Add Users or Groups to the Device User/Group List:

1. Click **Add** to open a list of qualified users and groups.
2. Click to put a check in front of the names of users or groups allowed access to the device or port.
3. Set the configuration rights for the users or groups:
    a. **Allowed:** The user or group can configure the device's settings.
    b. **Denied:** The user or group cannot configure the device's settings.
4. Set the access rights for the users or groups:
    a. **Administrator:** When accessing the device, the user or group has administrator privileges (according to the device's authorization policy).
    b. **User:** When accessing the device, the user or group has user privileges (according to the device's authorization policy).
    c. **View Only:** When accessing the device, the user or group can only view its ports. No actions can be performed.
    d. **No Access:** The user or group cannot access any of the device's ports.
5. When configuration rights settings are complete, click **Save**. The new users and groups are added to the device's User/Group list.

Modifying a User's or Group's Rights.

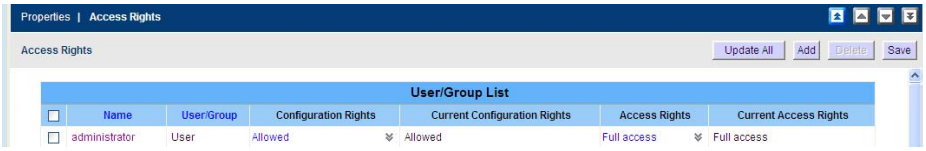
1. In the Configuration Rights column corresponding to the user or group to be modified, click on the arrow; make your new selection, then click **Close**.
2. In the Access Rights column corresponding to the user or group to be modified, click on the arrow; make your new selection, then click **Close**.
3. Click **Save** (at the top-right of the panel).

Deleting a User's or Group's Rights.

1. Click to put a check in front of the names of users or groups to be removed.
2. Click **Delete** (at the top-right of the panel).

Action Buttons. In addition to Add, Delete, and Save, an **Update All** button (at the top-right of the panel) opens a page where configuration and access rights can be set for all users and groups on the selected device or port.

Access Rights - KVM Ports. Select a port in the Sidebar or the Main panel list. Click the Access Rights Panel Menu item to open a page listing all users and groups with access. Set configuration and access rights here.



Adding Users or Groups to the Port User/Group List.

1. Click **Add** to open a list of qualified users and groups.
2. Click to put a check in front of the names of users or groups that will have access to the port.
3. Set the configuration rights for the users or groups:
   a. **Allowed:** The user or group can configure the port's settings.
   b. **Denied:** The user or group cannot configure the port's settings.

   Note: This setting is only available with ports on Cat5e KVM switches.
4. Set the access rights for the users or groups:
   a. **Full access:** The user can view the remote screen and perform operations on the remote system from his keyboard and monitor.
   b. **View only:** The user can view the remote screen but cannot perform any operations on it.
   c. **No access:** The port does not appear in the user's Port Access Sidebar or Status and Operation List (see “Port Access” on page 19).
5. Click **Save** when finished. New users and groups are added to the port's User/Group list.

Modifying a User's or Group's Rights.

1. In the Configuration Rights column of the user or group to be modified, click on the arrow; make your new selection, then click **Close**.
2. In the Access Rights column of the user or group to be modified, click on the arrow; make your new selection, then click **Close**.
3. Click **Save** (at the top-right of the panel).

Deleting a User's or Group's Access Rights.

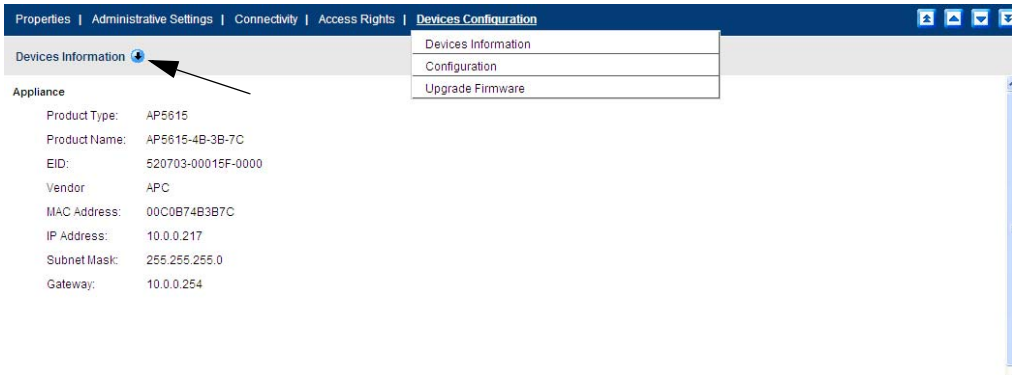
1. Click to put a check in front of the names of the users or groups to be removed.
2. Click **Delete** (at the top-right of the panel).

Action Buttons. In addition to Add, Delete, and Save, an **Update All** button (at the top-right of the panel) opens a page where configuration and access rights can be set for all users and groups on the port.

Device Configuration (For KVM Devices). Allows you to configure the device from within KVM ACCESS, without accessing the device directly.

Note: If the link between KVM ACCESS and the device should be broken, device configuration changes s will not be transmitted to the device. To make device configuration changes, log in to the device directly (see “KVM ACCESS Options” on page 53, for details).

This Panel Menu item contains several secondary pages. To modify the information on these pages, move through them sequentially clicking the arrow icons at the left of the main panel in the grey bar, or go directly to a page by moving the curser over the menu and selecting the page from the menu that opens.



Note: The Device Configuration Panel Menu does not appear if the device is offline.

The secondary Panel Menu pages correspond to the administration functions described in the device's User Manual. For configuring the settings, refer to the Device Management sections to obtain the necessary information. When you have finished making your configuration settings, click **Save**.

Note: 1. On KVM ACCESS's secondary Panel Menu ANMS settings page, in addition to the entry labeled Preferred Server Settings, there is an entry called Alternate Server Settings. The Preferred settings correspond to the ANMS settings on the device (see Device ANMS Settings, page 172) Changes to this setting take place on the device.
2. On KVM ACCESS' secondary Panel Menu Customization settings page, there is an entry called Port timeout. This field sets a time threshold for users on ports whose Access Mode has been set to Occupy (see “Mode” on page 68). This corresponds to the Access Mode setting on the original device. If there is no activity from the user occupying the port for the amount of time set here, the user is timed out and the port is released. The first user to send keyboard or mouse input after the port has been released gets to occupy the port. Input a value from 0 to 255 seconds. The default is 3 seconds. A setting of 0 causes the port to be released the instant there is no input.

Port Configuration (For Cat5e KVM Devices). Allows you to configure the port from within KVM ACCESS, without accessing the device directly.

Note: If the link between KVM ACCESS and the device is broken, device configuration changes will not be transmitted to the device. To make device configuration changes log in to the device directly (see “KVM ACCESS Options” on page 53, for details).

This Panel Menu page is used to set the I/O attributes of the selected port.

The attribute headings are described in the table:

Heading	Meaning
Port Name	This is the name given to the port.
Exit Macro	If system macros have been made, drop down the list to select the one you want. When you close the KVM viewer the macro will be sent to the server connected to this port and the server will run it.
Cable	Specifies the length of the Cat5e cable that is used to connect the computer to the port.
OS	Specifies the operating system that the computer on the connected port is using.
Language	Specifies the OS language being used by the computer on the connected port.
Mode	Corresponds to the Access Mode setting on the original device (Share, Occupy, Exclusive). It defines how the port is accessed when multiple users have logged on. **Exclusive:** The first user to switch to the port has exclusive control over the port. No other users can view the port. The Timeout function does not apply to ports which have this setting. **Occupy:** The first user to switch to the port has control over the port. However, additional users may view the port's video display. If the user who controls the port is inactive for longer than the time set in the Timeout box, port control is transferred to the next user to move the mouse or strike the keyboard. **Share:** Users simultaneously share control over the port. Input from the users is placed in a queue and executed chronologically.

To configure the settings, refer to the device's User Manual to obtain the necessary information. When you have finished making your configuration settings, click **Save**.

PDU Devices and Outlets

Selecting a Power device or one of its outlets opens a page with two entries on the Panel Menu bar: Properties, and Access Rights. Each of these items is discussed in the sections that follow.

Note:: 1. When you select a Power Device in the Sidebar, and expand the entries below it, the first station shown below the entry is the entry itself.

Properties (PDU). The settings found on the Properties page for the device, station, or outlet are similar to the ones described in the KVM Devices and Ports section. See page 63 for details.

Properties Page Action Buttons. The action buttons on the devices and outlets pages are the same, and perform the same functions as those found on the KVM properties pages. See “Properties Page Action Buttons” on page 64 for details.

Access Rights (PDU), Stations, and Outlets. Access rights can be configured for the entire device (nested stations and outlets), station-by-station, or outlet-by-outlet. After selecting the device, station, or outlet, clicking this Panel Menu item brings up a page that shows a list of all the users and groups that have been given access to it.

Adding Users or Groups to the Device, Station, or Outlet Access List. Configuration and access rights for devices, stations and outlets, can be set for users and groups. To set the rights for users or groups:

1. Click **Add** to open a list of qualified users and groups.
2. Click to put a check in the box in front of the names of the users or groups that you want to have access to the device, station, or outlet.
3. Set the configuration rights for the users or groups. (See page 66 for details.)
4. Set the access rights for the users or groups. (See page 66 for details.)
5. Click **Save** when you have finished to add the new users and group to the device, station, or outlet User/ Group list.

Modifying a User's or Group's Rights.

1. In the Configuration Rights column for the user or group to be modified, click on the arrow, select the new value, then click **Close**.
2. In the Access Rights column for the user or group to be modified, click on the arrow, select the new value, then click **Close**.
3. Click **Save** (at the top-right of the panel).

Deleting a User's or Group's Rights.

1. Click to put a check in front of the names of users or groups to be removed.
2. Click **Delete** (at the top-right of the panel).

Device Configuration (PDU). This Panel Menu item is similar to the one for KVM device configuration on page 67 except it has different secondary pages. The purpose of the secondary pages is to allow configuration of the device from within KVM ACCESS, without having to access the device directly.

Note: 1. If the link between KVM ACCESS and the device is broken, device configuration changes made on these pages will not be transmitted to the device. You can log in to the device directly to make the changes. See“KVM ACCESS Options” on page 53 for details.
2. Device Configuration does not appear if the device is offline, or if the device is on a port nested under another device.

The secondary pages correspond to the administration functions described in the device's User Manual. For configuring the settings, refer to the manual's Administration chapter to obtain the necessary information. Click **Save** when finished.

Port (Outlet) Configuration (PDU). Power outlets are nested under each of their stations. Each outlet's settings can be configured independently on an outlet-by-outlet basis. The Port Configuration Panel Menu has two secondary items: Port Settings and Schedule Settings.

Note: 1. The Port Configuration Panel Menu does not appear if the device is offline, or if the device is on a port nested under another device.
2. If the link between KVM ACCESS and the device should be broken for some reason, port configuration changes made on these pages will not be transmitted to the device. When this happens, you can log in to the device directly to make the changes. See“KVM ACCESS Options” on page 53 for details.

Port Settings. To bring up the port settings page for a particular outlet, select it in the sidebar, then click Port Configuration on the Panel Menu bar.

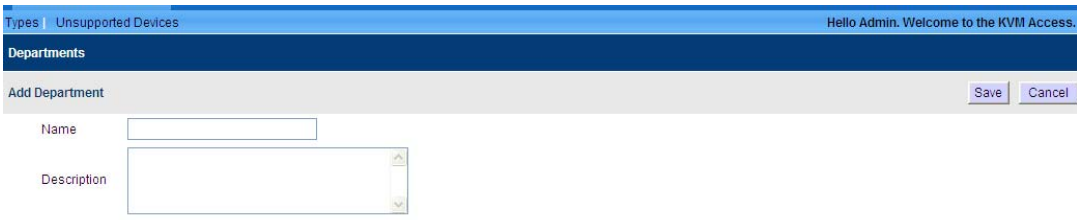
Departments, Locations and Types

For convenience and ease of management the Departments, Locations, and Types pages provide three more ways of organizing your devices. To use this organizational scheme, first create appropriate categories (such as R&D and Manufacturing under Departments; East Coast Operations under Locations; and Power under Types) and then assign devices to them (from the device's Properties page), as described in the sections that follow.

Adding a Department Location or Type

1. Select Department, Location, or Type on the Menu Bar to open the page.

2. Click **Add** (at the top-right of the panel) to open the page.



3. Fill in the Name and Description fields, then click **Save**

Assigning Devices and Ports

To assign a device or port to a Department, Location, or Type:

1. Select Devices on the Menu Bar.
2. In the Sidebar, select the device or port to assign to a Department, Location, or Type to open its Properties page (see page 71).
3. Select from the list the Department, Location, or Type to which the device or port will belong.

Modifying a Department, Location, or Type

To change the name or description of a Department, Location, or Type:

1. Select Department, Location, or Type on the Menu Bar.
2. In the Sidebar or Main Panel, select the Department, Location, or Type to modify.
3. On the Panel Menu bar, select Properties.
4. Make your changes, then click **Save**.

Deleting a Department, Location, or Type

To delete a Department, Location, or Type:

1. Select Department, Location, or Type on the Menu Bar to open the page.
2. Click to put a check in front of the name of the Department, Location, or Type to be removed, then click **Delete** (at the top-right of the panel).

Unsupported Devices

Devices whose firmware level is not compatible with the KVM ACCESS' current firmware level are unsupported. Click **Unsupported Devices** on the Menu Bar to open a page that lists all such devices deployed on the KVM ACCESS installation:

To make these devices available for management under KVM ACCESS, upgrade their firmware to the latest version.

1. Add the device's firmware upgrade file to KVM ACCESS. See “Appliance Files” on page 92 for details.
2. Once the device's firmware upgrade file is stored on KVM ACCESS, its checkbox on this page becomes active. Click to put a check mark in the checkbox.
3. The Firmware Upgrade button (at the top-right of the panel), becomes active.
4. Click **Firmware Upgrade** to upgrade the device's firmware.

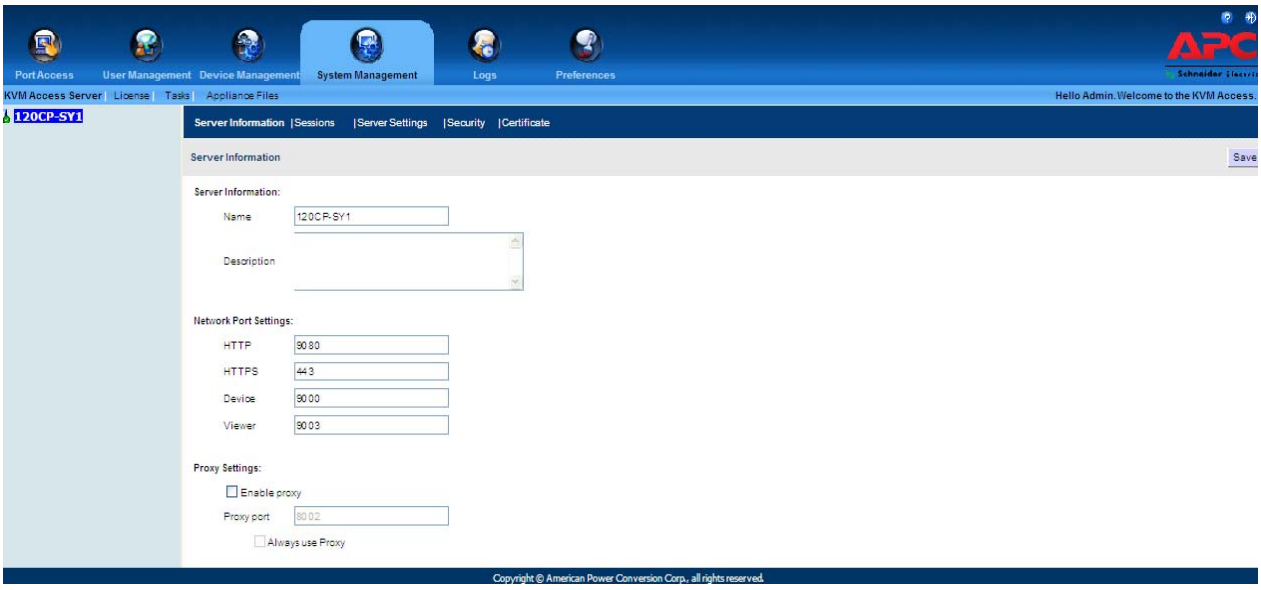
Once the firmware upgrade completes, the device is removed from the **Unsupported Devices** list, and now appears in the **Available Devices** list (see “Adding a Folder or Device” on page 51).

System Management

Overview

By connecting individual KVM ACCESS server segments through their IP addresses into an integrated worldwide network, KVM ACCESS provides secure, centralized, single IP address login access, to all your data center equipment from anywhere there is an internet connection.
When you click the System Management tab, KVM ACCESS opens to the default page.

Note: The System Management page is only available to System Administrators.



Menu Structure

The System Management menu structure is described in the table below:

Tab	Page Menu	Panel Menu	Panel Menu Submenus	Page
System Management	This Server	Server Information		74
		Server Settings	SMTP	75
			NTP	76
			Syslog	77
		Sessions		94
		Security		78
		Certificate		79
	License			81
	Tasks			83
	Appliance Files			92

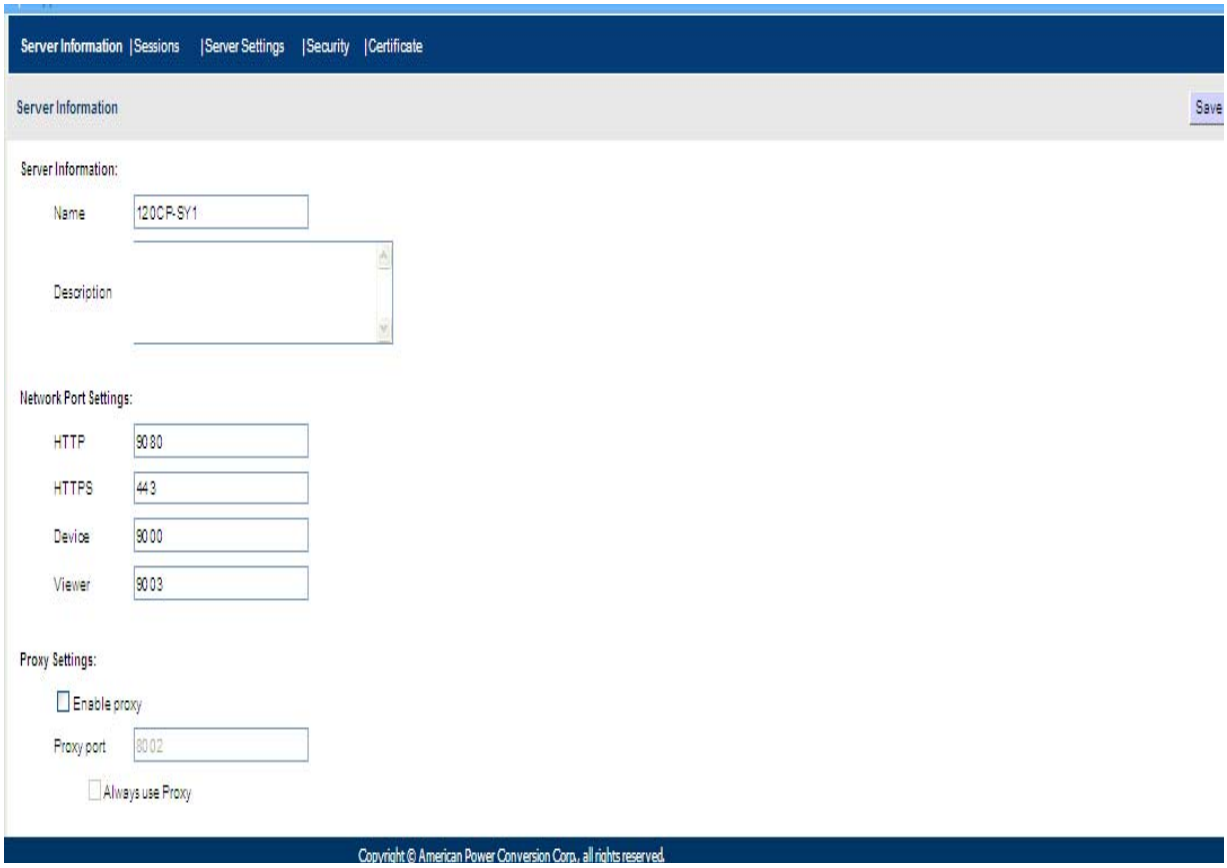
The KVM ACCESS Server

This page refers to the KVM ACCESS server you are currently logged into. Other KVM ACCESS servers on the installation are ignored. The menu offers five Panel Menu choices: Server Information, Server Settings, Session, Security, and Certificate.

Note: Changes to other servers on the installation can only be made by logging into them directly.

Server Information

The default page is Server Information:



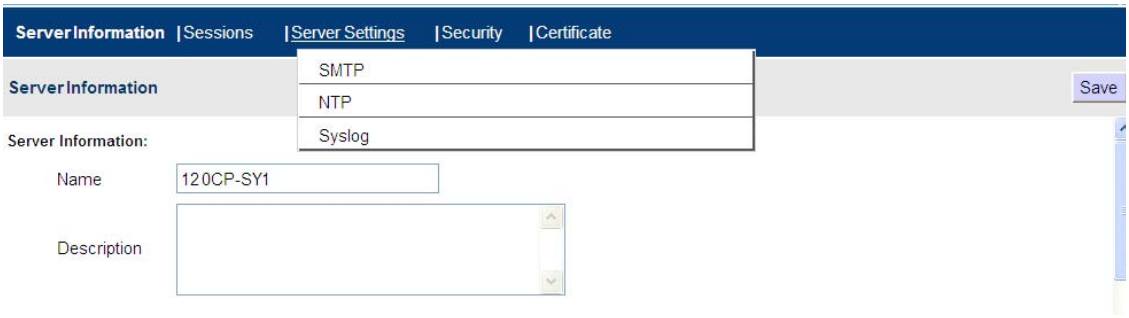
This page allows you to configure the KVM ACCESS server's settings.

Field	Description
Name*	Change the KVM ACCESS server's name by editing this field.
Description	Change the KVM ACCESS server's description by editing this field. The description can be from 2-32 Bytes in any supported language.
HTTP*	The port that KVM ACCESS uses to communicate with internet browsers.
HTTPS*	The secure port that KVM ACCESS uses to communicate with a browser over the internet.
Device Port*	The port that KVM ACCESS uses to communicate with devices on the installation.
Viewer Port	The port that KVM ACCESS uses for viewers to communicate with when Multiviewer is in effect. See “Launch Multiviewer” on page 20.
Enable Proxy	If you need to use the proxy function, check this box, then specify the proxy port in the indicated field. See “KVM ACCESS Proxy Function” on page 104.
* See page 8 for details.	

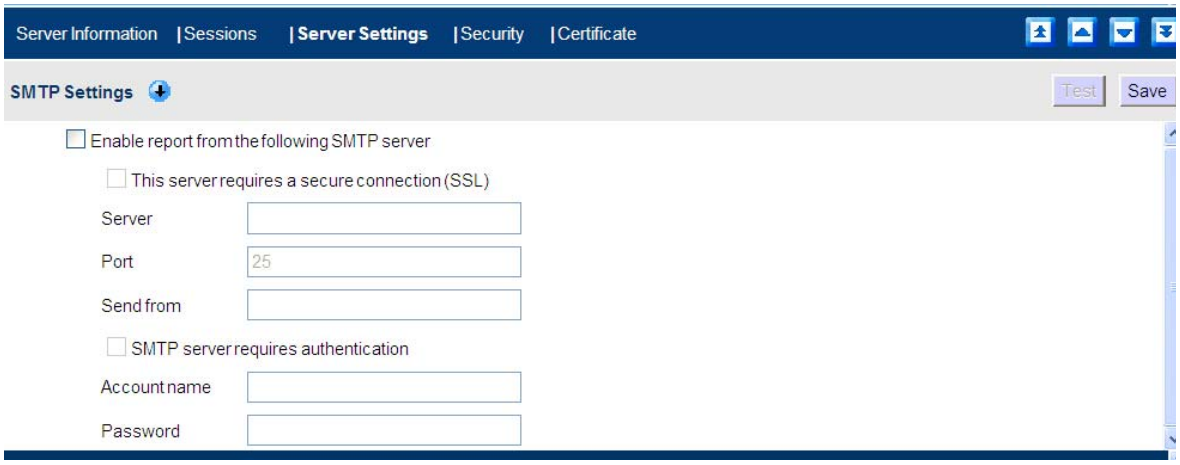
When all your configuration settings have been made, click **Save**.

Server Settings

To modify the information, move through them sequentially by clicking the arrow icons at the left of the main panel in the grey bar, or go directly to a page by hovering over the menu and selecting the page from the popup menu that opens.



SMTP. KVM ACCESS can send email notification of event traps on the installation to specified users.



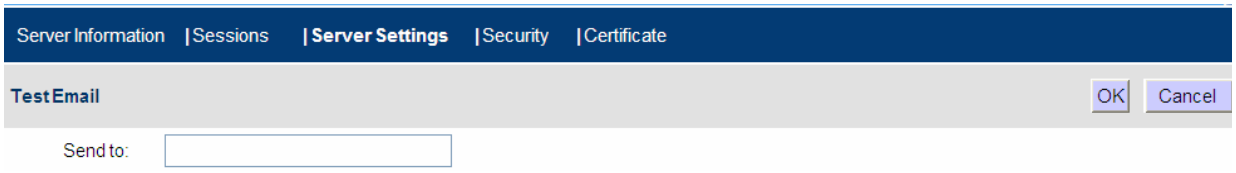
Note: Event notification recipients are designated on the The Notification Settings page. See page 97 for details.

To enable SMTP server setting:

1. Check **Enable report** from the SMTP server checkbox.
2. Specify the IP address or domain name of the computer running your SMTP server in the Server field.
3. Specify the port number that the SMTP server monitors.
4. Specify the KVM ACCESS administrator's email address in the **Send from** field.

Note: This field cannot be blank.

5. If the SMTP server requires authentication, check the SMTP server requires authentication checkbox, then specify the authentication account name and password in the appropriate fields.
6. Click **Test** to check that the SMTP server setting is configured properly and the page opens.

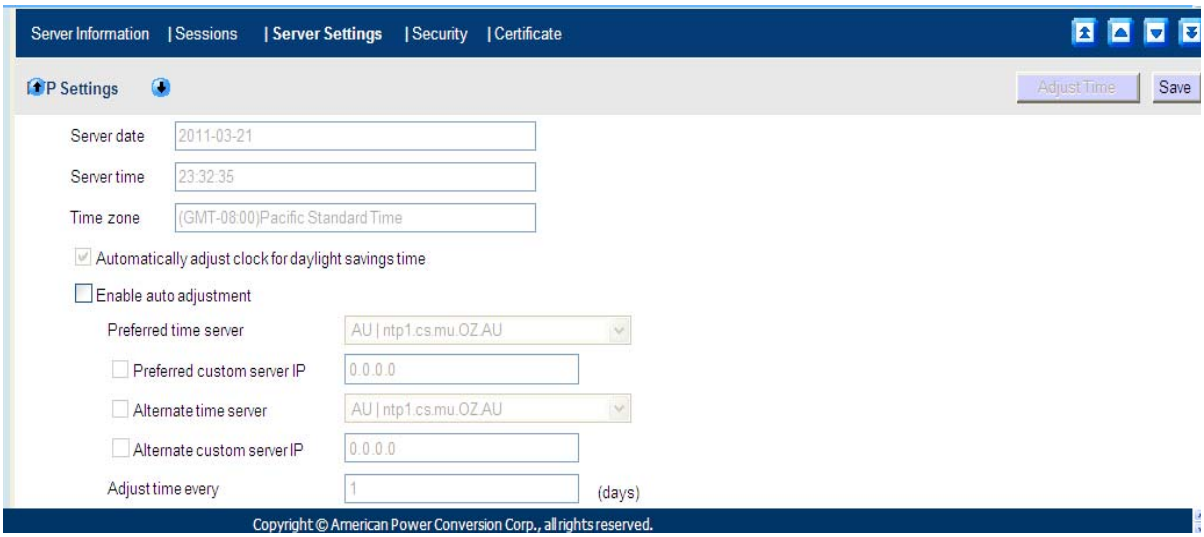


7. Enter an email address for the recipient of the test email then click **OK**. If the settings have been configured correctly, the recipient will receive the test email.

Note: The email address of the recipient cannot exceed the equivalent of 128 English alphanumeric characters.

8. Click **Save** to complete the procedure.

NTP. The NTP page lets you automatically synchronize to a network time server:



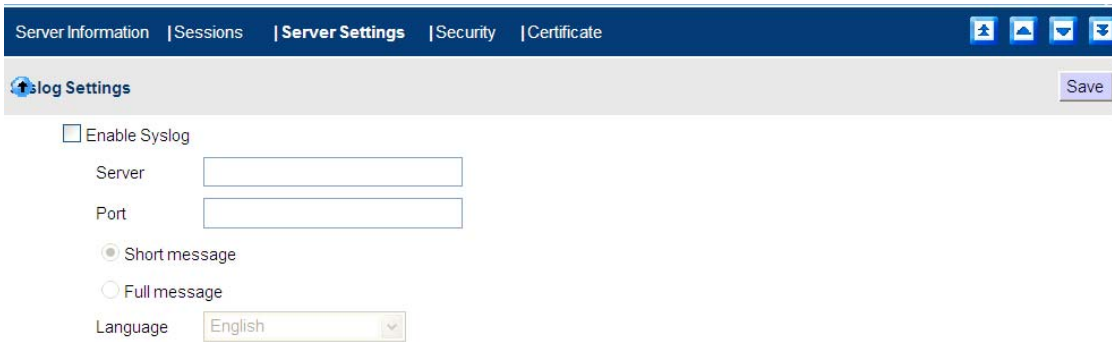
Note: 1. The top three fields are filled automatically by KVM ACCESS, and can't be edited. 2. If you are in a timezone that doesn't have daylight savings time, the **Automatically adjust clock for daylight savings time** checkbox is disabled.

To have KVM ACCESS' time automatically synchronized to a network timeserver:

1. Check the **Enable auto adjustment** checkbox.
2. Select your preferred time server from the drop down list or check the Preferred custom server IP checkbox and enter the IP address of the time server of your choice.
3. To configure an alternate time server, check the **Alternate time server** checkbox, and repeat step 2 for the alternate time server entries.
4. Enter the number of days between synchronization procedures.
5. If you want to synchronize immediately, click **Adjust Time Now**.

When all your settings have been made, click **Save**.

Syslog. To record all the events that take place on KVM ACCESS and write them to a Syslog server:



1. Check **Enable**.
2. Enter the IP address and port number of the Syslog server. The valid port range is 1-65535.
3. Select whether to log a short message or a full message.
4. Select the message's language from the drop down list.

When all your settings have been made, click **Save**.

Dial In. In addition to Internet connections, KVM ACCESS can also be accessed from PPP (modem). The Dial In settings page is used to specify which users can access this feature and the connection methods.
To allow PPP dial in connections:

1. Put a check in the **Enable Dial In** checkbox.
2. Supply a Username and Password that users dialing in must use in order to be authenticated over the dial in connection.

If **Enable Dial Back** is enabled, the switch disconnects the connections that dial in to it and dials back to either to a fixed number or a flexible number.

Item	Action
Enable Fixed Number DialBack	If this radio button is selected, the switch will dial back to the modem whose phone number is specified in the Dial back number field. Enter the number that you want KVM ACCESS to dial back in this field. **Note:** Specify a number here even if you intend to use flexible dial back
Enable Flexible Dial Back (Use dial back phone number as the username)	If this radio button is selected, the modem that KVM ACCESS dials back doesn't have to be fixed. It can dial back to any modem that is convenient for the user. To do so, when you dial in to KVM ACCESS: • When logging in, use the phone number of the modem that you want the switch to dial back for your Username. • Use the phone number specified in the Dial back number field (see above) for your Password.

When all the settings have been made, click **Save**.

Sessions

Clicking the Sessions Panel Menu item that appears when KVM ACCESS Network is selected on the Page Menu, or in the Sidebar, lists all the sessions currently taking place on all the KVM ACCESS on the installation, and provides information concerning the "who, where and when" of each.

Note: 1. To only see the sessions for a particular KVM ACCESS server, use the navigation buttons at the top-right of the main panel to select it.
2. To end a session, you must do it from the KVM ACCESS Servers Sessions Panel Menu.

Security

This page provides a level of security by controlling access to KVM ACCESS.

IP Filtering. IP filtering controls access to KVM ACCESS based on the IP addresses of the computers attempting to connect to it.

- To enable IP filtering, check the **Enable IP Filter** checkbox.
  - If the **Include** button is selected, all the addresses specified in the Address List are allowed access; all other addresses are denied access.
  - If the **Exclude** button is selected, all the addresses specified in the Address List are denied access; all other addresses are allowed access.
- IP filters can consist of a single address, or a range of addresses. You can add as many IP addresses as you require. Enter the addresses directly into the IP address text input box.
  - For multiple single address entries, use a comma between the IP addresses. There is no space before or after the commas.
  - For a range of filters, enter the starting IP address, followed by a dash, then the ending IP address.
- To modify or delete a filter, make your changes directly in the IP address text input box.

MAC Filtering. MAC filtering controls access to KVM ACCESS based on the MAC addresses of the computers attempting to connect to it.

- To enable IP filtering, check the Enable IP Filter checkbox.
  - If **Validate MAC at KVM ACCESS login** is enabled, KVM ACCESS will verify the client PC's MAC address when the user attempts to log in. Otherwise, the MAC address will only be verified when attempting to open a viewer.
  - If the **Include** button is selected, all the addresses specified in the address list are allowed access. All other addresses are denied access.
  - If the Exclude button is selected, all the addresses specified in the address list are denied access; all other addresses are allowed access.
- MAC filters can consist of a single address, or a range of addresses. You can add as many MAC addresses as you require. Enter the addresses directly into the IP address text input box, using a comma between the addresses. There is no space before or after the commas.

Single Sign On. If enabled, users that are authenticated through KVM ACCESS are automatically authenticated on all the devices deployed on the system. They don't have to be authenticated on each device individually.

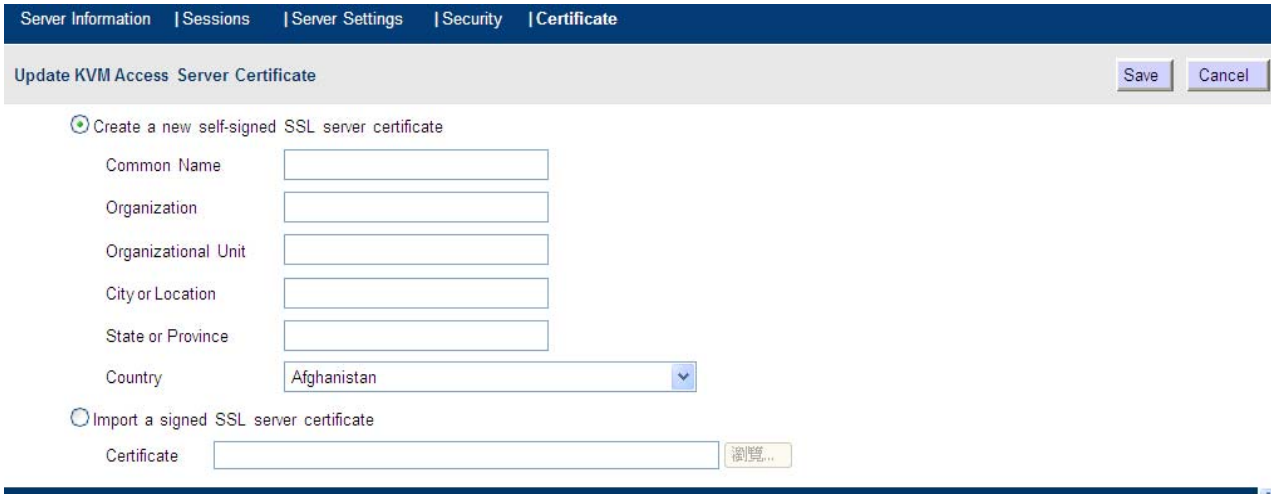
Certificate

When logging in over a secure (SSL) connection, a signed certificate is used to verify that the user is logging in to the site he intended. The Certificate page is used to create, modify, or obtain a certificate for this purpose.

During installation, each KVM ACCESS creates its own independent, self-signed certificate based on the installation information, similar to the one below:

Changing a Self-Signed Certificate. Changing a self-signed certificate allows you to provide additional information in the certificate that wasn't generated in the installation certificate. The way to change a self-signed SSL certificate is to create a new one. To create a new self-signed certificate:

1. At the top-right of the Certificate panel, click **Update** to open the page:



2. Select the **Create a new self signed SSL server certificate** radio button, then fill in the fields according to the information in the table below:

Field	Description
Common Name	The Fully Qualified Domain Name (FQDN) for which you requested the SSL certificate. For example: www.yourdomainname.com
Organization	Your Full Legal Company or Personal Name as legally registered in your locality.
Organizational Unit	The branch of your company that is ordering the certificate (accounting, marketing, etc.).
City or Location	The full name of the city or location.
State or Province	The full name of the state or province.
Country	The two letter country code where the organization is located. **Note:** If you are not sure of the code, do an online search for ssl+country codes.

3. When you have finished filling in the fields, click **Save**.
   A message opens asking you to wait while the database updates with the new information. The web page closes and the login sequence opens. Accept the security certificate and log in.

Importing a Signed SSL Server Certificate. In order to avoid making users go through the certificate acceptance prompt each time they log in, administrators may choose to use a third party certificate authority (CA) signed certificate.

To use a third party signed certificate:

1. After generating the self-signed certificate, click Get CSR (Certificate Signing Request) at the top-right of the panel. (See the screenshot on page 153.)
2. Go to the CA website of your choice and apply for an SSL certificate using the information generated in step 1.
3. After the CA sends you the certificate, open the Server Certificate page, click Update at the top-right of the panel.
4. Select **Import a signed SSL server certificate**, browse to the certificate file location, and select it.
5. Click **Save** at the top-right of the panel.

Note: Each of the certificate types mentioned in this section provides an equal level of security. The advantage of the changed self-signed certificate is that it allows you to provide more information than the installation certificate. The advantage of a CA third party certificate is that users do not have to go through the certificate acceptance prompt each time they log in, and it provides the additional assurance that a recognized authority has certified that the certificate is valid.

License

The KVM ACCESS license controls the number of nodes permitted on the KVM ACCESS server installation. The default license that comes with your purchase is a demo license for one server that allows 16 nodes. To add more, you must upgrade the license.

Select License from the System Management menu to open the page.

Page items are described in the table below:

Item	Description
Key serial number	The serial number of the license key. **Note:** This is different from the software serial number that you used when installing the KVM ACCESS server. The license serial number is on the key.
Nodes	The total number of nodes permitted on the installation according to the license purchase. **Note**: The number of nodes that can be increased to 1024.
Available Nodes	The number of unused nodes permitted by your license that are still available for deployment.

Upgrading the License

1. Contact apc to obtain a license key for the number of nodes you want to access.
2. Insert the license key into a USB port on your master server.
3. Click Upgrade at the top right of the main panel.

Note: 1. Once the upgrade has completed, it is not necessary to keep the key plugged into the USB port. Store the key in a secure location. It will be needed for future upgrades.
2. If you lose the USB license key, contact APC to obtain another one. If you supply the key's serial number, the new key will contain all of the information that was stored on the lost key.

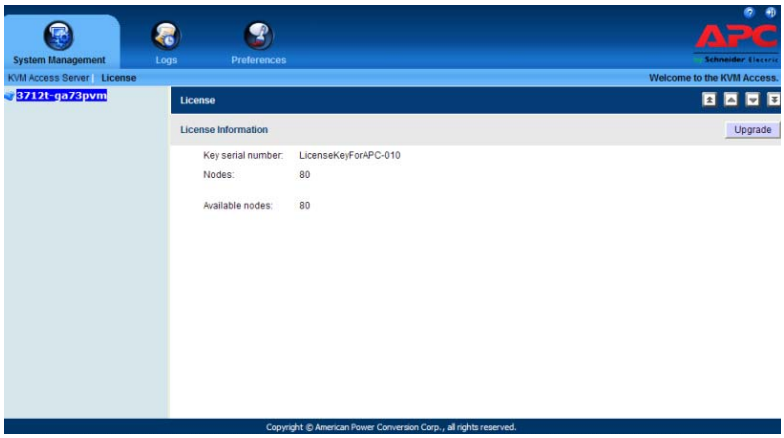
License Sharing. Only as many nodes as there are licenses can be created for management (see “Preliminary Procedures” on page 48).

When devices are added to the KVM ACCESS system, the default configuration is for them to be locked. Although their configuration information is stored by the KVM ACCESS, they cannot be managed.

Locked ports can be unlocked either by selecting a physical port and unlocking it by clicking the Unlock button (see “Locking / Unlocking Ports” on page 60), or by making the port part of an aggregate device (see “Adding an Aggregate Device” on page 53).

If all the licenses are in use, only if a currently unlocked port is locked, or if an aggregate device is deleted, freeing up the license it was using, can a locked port (or new aggregate device) use that license.

License Conflict. If two servers on the same network segment have been upgraded with the same license key, a license conflict will occur. The second server installed will cause a page to open similar to the one below:



To confirm that a conflict has occurred, click the **Logs** tab. A message will open in the log file: **A license violation has been detected at KVM ACCESS server (IP: [the conflicting servers' IP]).**

To resolve the conflict:

1. Shut down, disconnect from the network, or uninstall KVM ACCESS from one of the servers.
2. If you want to have two independent KVM ACCESS installations, purchase a separate key for the second KVM ACCESS server.

Tasks

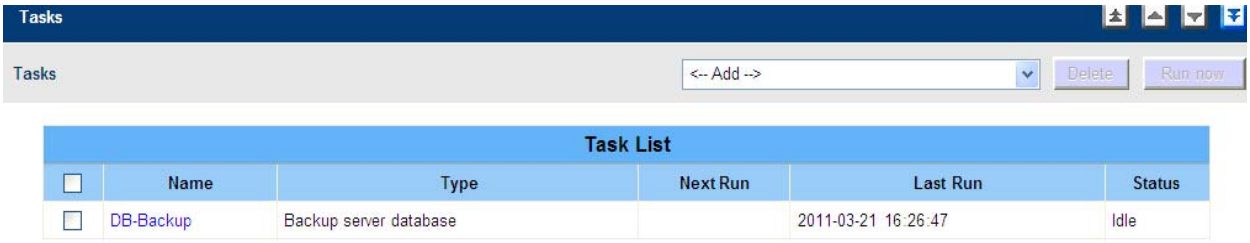
The Tasks menu allows authorized administrators to perform a number of system maintenance tasks. The tasks that can be performed are determined by the user's type, and the authorization options that were selected when the user's account was created. These include:

- Backing up the server database

  Note: Restoring the database requires a separate utility and procedure. See “Restore” on page 111, for details.

- Exporting event logs
- Controlling PDU devices
- Upgrading the firmware of selected appliances
- Backing up device configuration and account information
- Exporting the device log
- Exporting the session history

Open the Tasks page on the master KVM ACCESS to see the screen below:

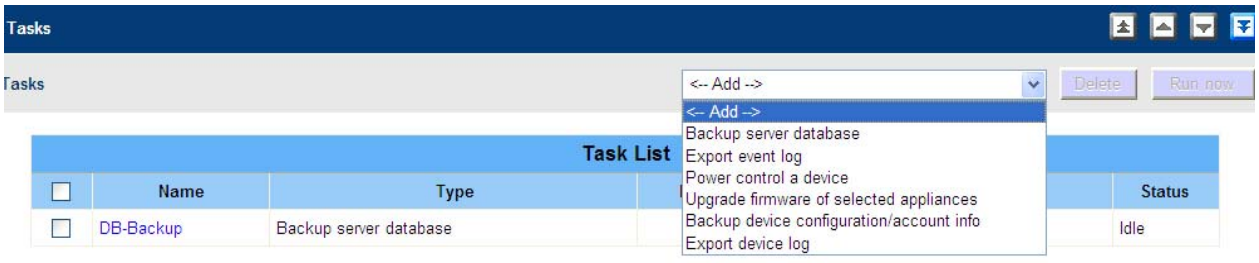


The Task List table lists all the tasks that have been configured.

Heading	Explanation
Name	The name you gave to the task when you configured it.
Type	The type of task that it is.
Next Run	If the task is scheduled to be run at a certain time, the time that it will run appears here.
Last Run	Indicates the last time that the task ran.
Status	Indicates whether the task is running or is idle.

Adding a Task

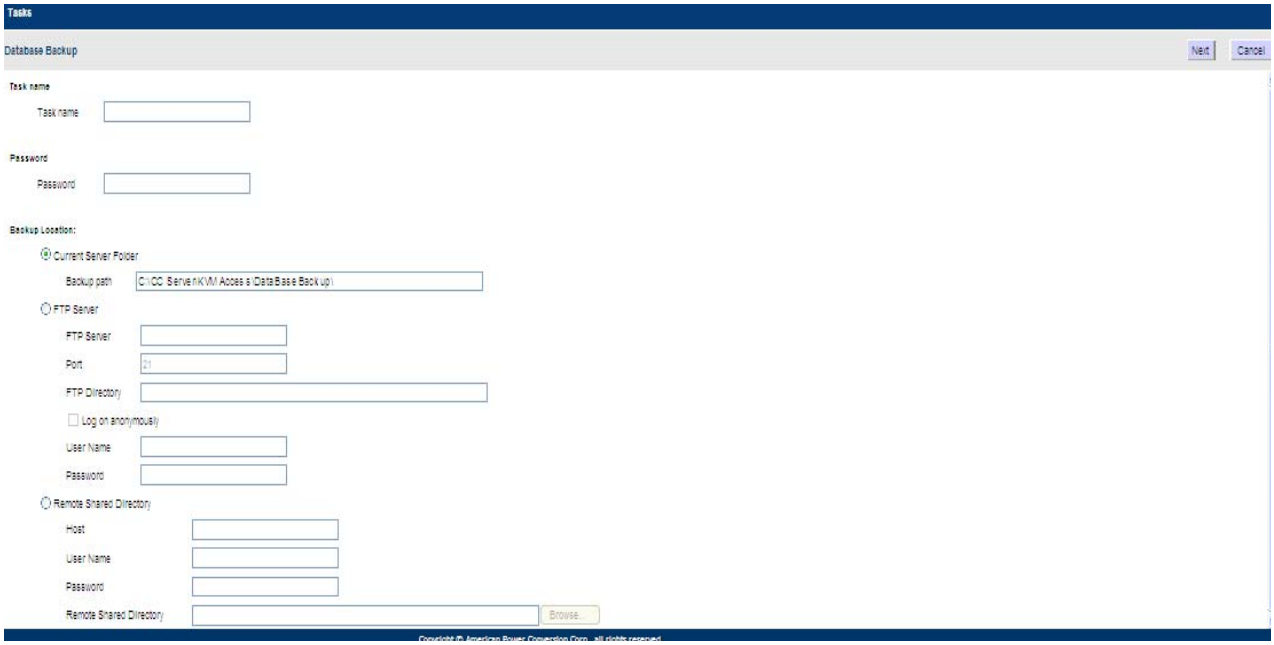
1. Click the arrow at the right of the Add field to view the task choices in the list:



2. Click on the task you want to add.
   Depending on the task you choose, a page comes up with choices. While each of the tasks is different, the procedures involved in setting them up are similar.

Backup the Server Database

When you choose the Backup the server database task, the following page appears:



1. Enter a name for the task, and a password.

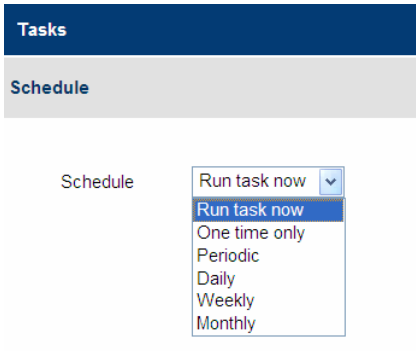
   Note: The password is **optional**. If you set one, store it in a safe place. You will need it when restoring the database. (You can restore the database without a passord. See “Restore” on page 111, for information.)

   3. The password cannot exceed the equivalent of 8 English alphanumeric characters.
   4. The extension of the backup file is cbk (*.cbk).

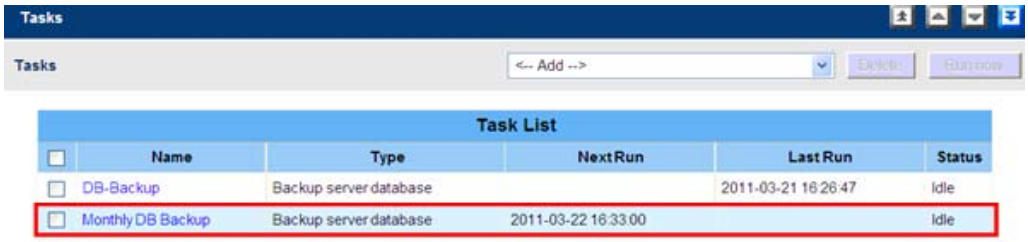
2. Select the location to store the backup file, and fill in the fields. The default setting is the local directory where KVM ACCESS was installed. Example: C:\KVM ACCESS\DataBaseBackup.

3. When you have filled in the information, click **Next** to open the Schedule page:

4. Use the drop down list to see the available choices. Depending on the selection, further scheduling choices may appear. For example, if you choose Monthly, a page that allows you to set the monthly schedule appears:

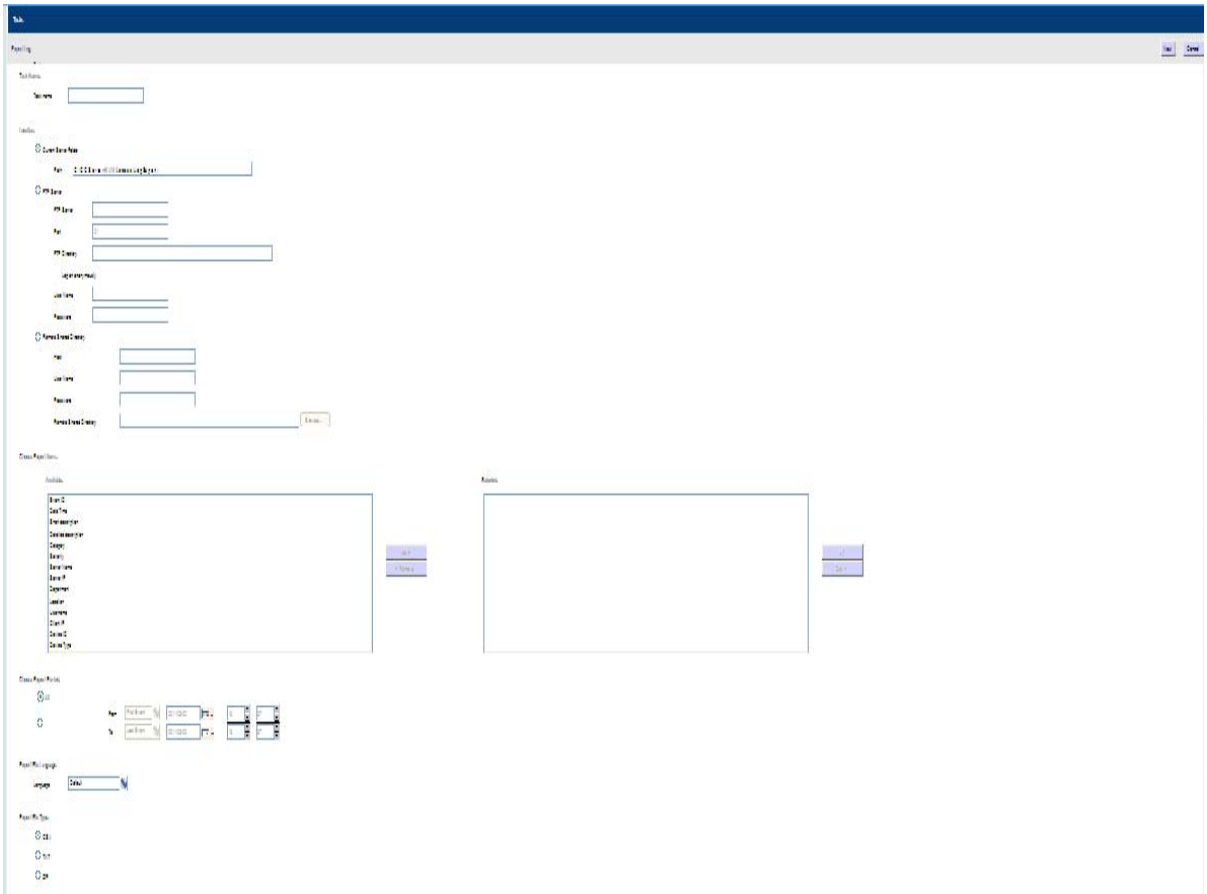


5. Complete the schedule choices and click **Next**.
   The task is now added to the Task List on the main page.



Note: Run a task (or tasks) at any time by putting a check in the box in front of its name and clicking **Run Now** at the top-right of the panel.

Export Event Log



1. Enter a name for the task in the Task name field.

   Note: The Export Event Log operation is performed on each server independently. To search a server's records you must look at its file. You can identify the file by the Task name you gave it.

2. Select the location to store the exported file, and fill in the fields. The default setting is to a directory at the same location as the KVM ACCESS server: C:\KVM ACCESS\KVM ACCESSLogExport.

3. Select an item to include in the exported file in the Available column. Click **Add** to move it into the Selected column. Repeat for any other log file items to be included.

   Note: To select multiple items, use Shift+Click or Ctrl+Click.

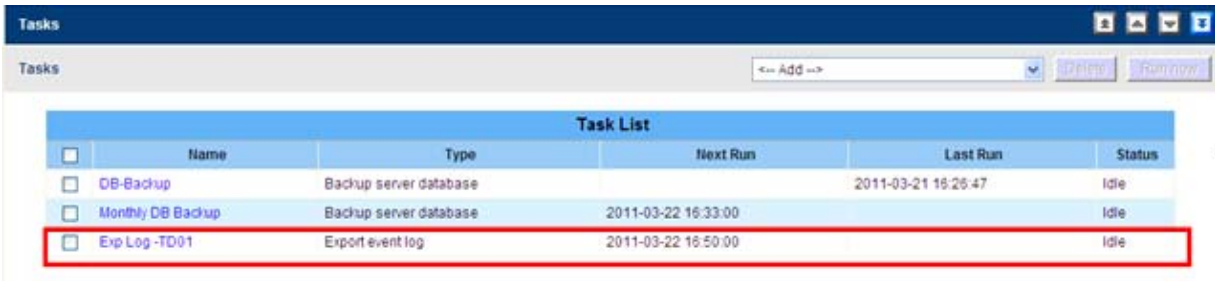
4. To change the order of the Selected items, click on the item you want to move, then click **Up** or **Down** to change the position.
5. For Choose Export Period, selecting **All** exports all the records in the database. To export records for a particular time period, select the radio button below it and set the time parameters with the **From** and **To** settings.
6. For Export File Language, choose **Default** to have the file exported in the language that your browser is set to. A different language can be selected from the drop down the list.
7. For Export File Type, click the radio button in front of your choice. If you choose one of the encryption options (AES or DES), enter a password into the Password field that opens.

   Note: Make a note of the password. You will need it to import the file (see “Import Logs” on page 100 for details).

8. When finished, click **Next**.
9. Make schedule choices in the pages that open.

   Note: The schedule choices are similar to those for the Backup server database task. Refer to page 84 for details.

10. Comlete the schedule choices and click **Next**.
    When the procedure finishes, the Tasks main page opens and the Export Event Log task is now added to the Sidebar and the Task List.



Power Control a PDU

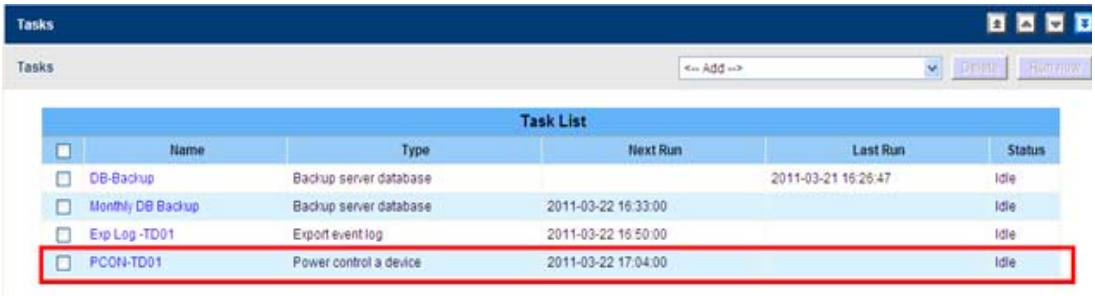
Set a schedule to automate turning power ports on and off for the selected device as a whole, or on a port-by-port basis. Choosing this task opens the Power Control page with the Target Device category selected:

To perform the task on a port-by-port basis, select the Outlets category.

1. Provide a name for the task.
2. Put a check in front of the target devices or ports you want to control or put a check at the top of the column to select all of them.
3. Select whether to turn the ports On or Off in the Operation column.
4. When finished, click **Next** (at the top-right of the panel).
5. Make schedule choices in the Schedule page that opens.

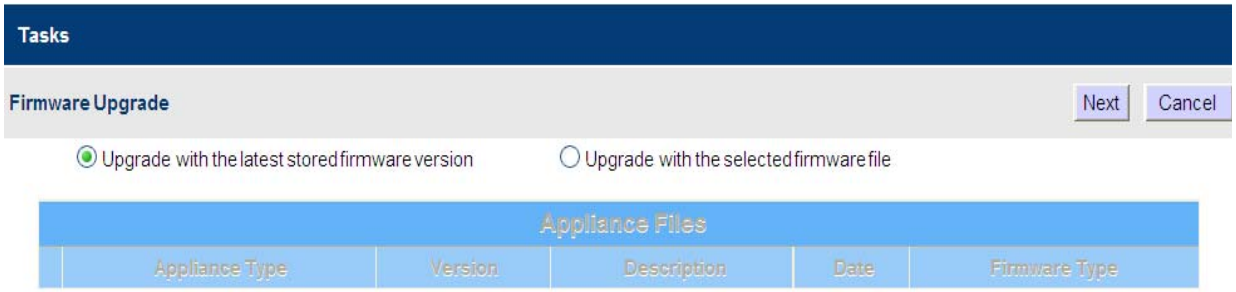
   Note: The schedule choices are similar to the ones described for “Backup the Server Database” on page 84.

6. Comlete the schedule choices and click **Next**.
   When the procedure completes, the Tasks main page opens and the Power Control a Device task is now added to the Sidebar and the Task List.



Upgrade Selected Appliance Firmware

This task allows you to schedule firmware upgrades of devices on your installation to take place at the most convenient time. Choose Upgrade Selected Appliance Firmware to open the Firmware Upgrade page.

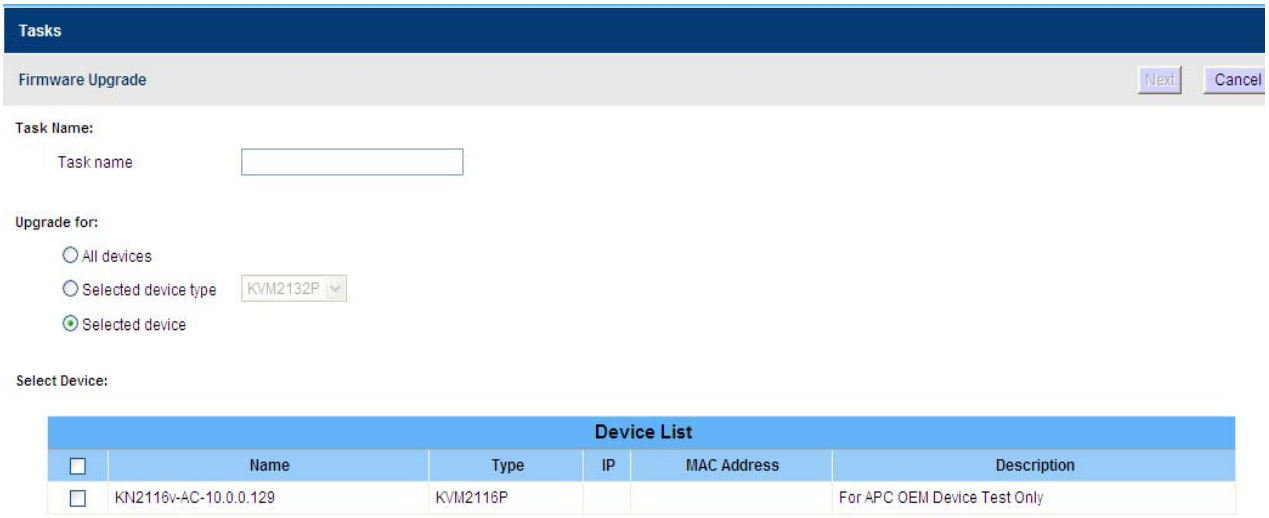


To schedule firmware upgrade of selected appliances:

1. Click a radio button to choose the latest upgrade file stored with the KVM ACCESS server or a file that you have uploaded.

   Note: 1. The files stored with the KVM ACCESS server came as part of its firmware. These are usually the latest versions that are compatible with the KVM ACCESS. We recommend using them unless you have a particular reason for choosing another one. 2. If you choose Upgrade with a selected firmware file, before upgrading, you must first upload the upgrade file. See “Firmware Files” on page 92, for details

2. If you choose Upgrade with the latest stored version (recommended), all the devices are automatically selected for the upgrade. If you choose Upgrade with a selected firmware file, click the button in front of the device type you want to upgrade.
3. Click **Next** to open the Firmware Upgrade page.



4. Enter an appropriate name to describe the task in the Task name field.
5. Click a radio button to select which appliances will receive the upgrade.
6. Choose **Selected device type**. From the drop down list select the device type. Only the devices that are the selected device type receive an upgrade.

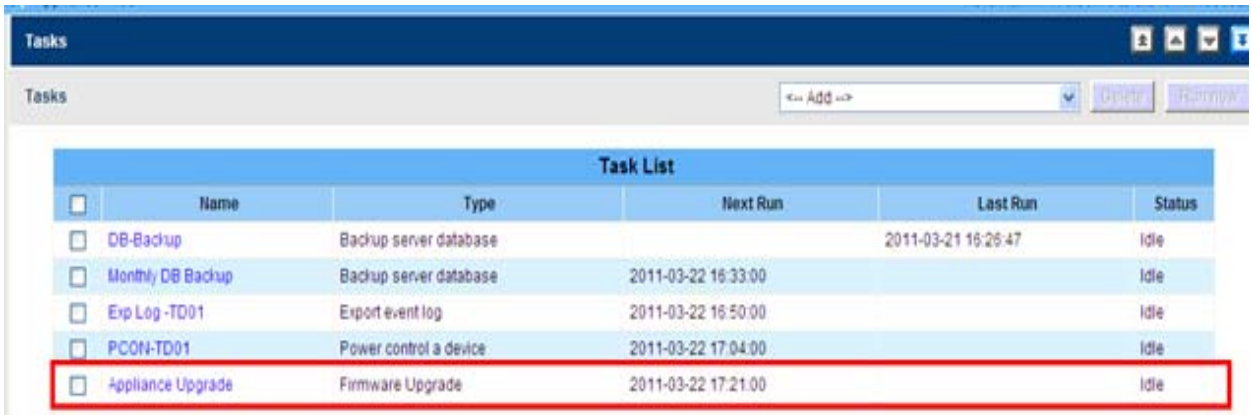
7. Choose **Selected device** and check the box in front of the devices to upgrade (or check the box at the top of the column to select them all).

Note: For KVM switches with Adapter Cables, click the arrowhead in front of the switch's name to select the Adapter Cable firmware to upgrade.

8. Click **Next**.
9. Make schedule choices in the Schedule page that opens.

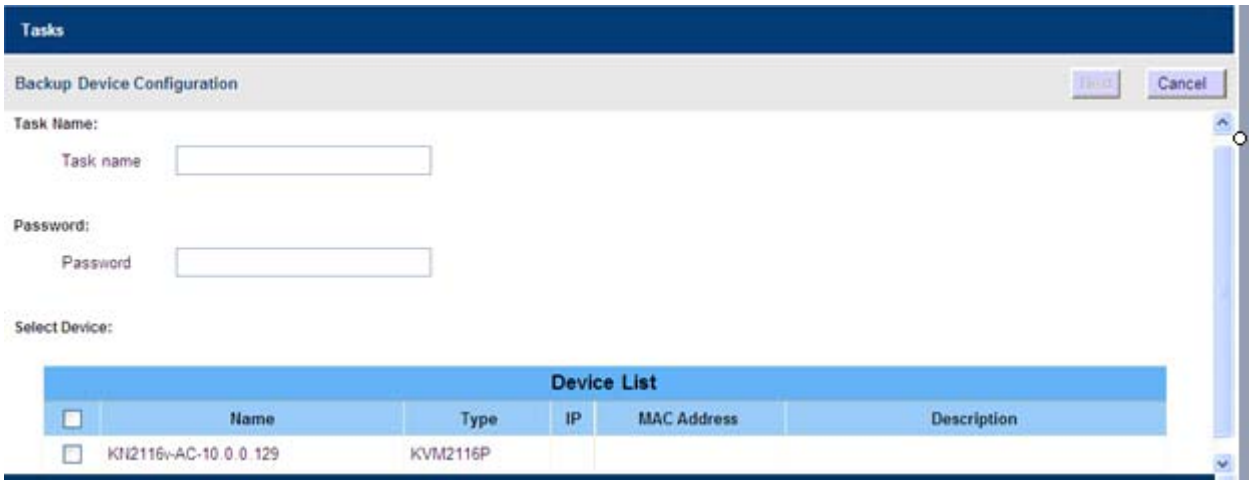
Note: The schedule choices are similar to the ones described for “Backup the Server Database” on page 84.

10. Comlete the schedule choices and click **Next**. When the procedure finishes, the Tasks main page opens and the task is now added to the Sidebar and the Task List.



Backup Device Configuration/Account Information

Select the Backup device configuration/account information task to open the page.



1. Provide a name for the task and a password.

Note: Store the password in a safe place. It will be needed when restoring the configuration/account information. See “Restoring Device Configurations” on page 62 for details.

2. In the Device List, check the box in front of the device you want to back up, then click **Next**.

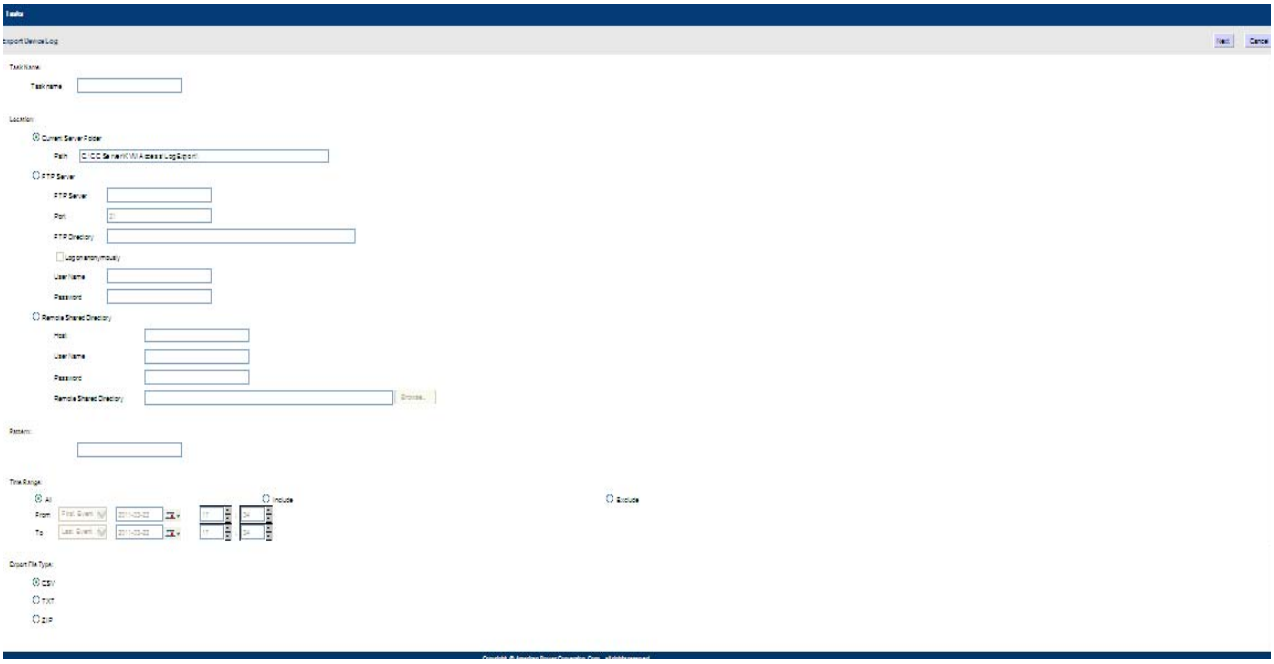
3. Make schedule choices in the Schedule page.

Note: The schedule choices are similar to those described for the Backup server database task. Refer back to page 84 for details.

4. Complete the schedule choices and click **Next**.
   When the procedure finishes, the Tasks main page opens, and the Backup device configuration/ account information task is now added to the Sidebar and the Task List.

Export Device Log

KVM ACCESS acts as a log server for all APC devices, recording the system events that take place on the devices in the database. This task writes the contents of the device database to a file. Choose the Export device log task to open the Export Device Log page.



1. Provide an appropriate name for the task. For example, if you want to export the device log for all devices you might name the task **All-device-log**, if you want to export the device log for PDU devices on a weekly basis, you might name the task **PDU-weekly-device-log**.

Note: The Export Device Log operation is performed on each server independently and stored on each server independently. To search the records, go to each server to look at its particular file.

2. Select the location in which to store the exported file, and fill in the fields. The default setting is for the file to be exported to a directory on the current KVM ACCESS server.

Note: The path to the directory on your server that will hold the backup file is pre-configured based on the directory in which the KVM ACCESS was installed. Example: C:\KVM ACCESS\KVM ACCESSLogBackup

3. The Pattern field can be used as a filter to limit the scope of the log file.

4. For the Time Range:
    a. Selecting **All** exports all the records in the database.
    b. To export records for a particular time period, select the Include radio button and set the time parameters with the **From** and **To** settings. To export all records that do not include a particular time period, select the Exclude radio button and set the time parameters that you do not want to include with the **From** and **To** settings.
5. For Export File Type, click the radio button in front of your choice. If you choose one of the encryption options (AES or DES), enter the password in the Password field.
6. When finished, click **Next**.
7. Make schedule choices in the pages that open.

    Note: The schedule choices are similar to those described for “Backup the Server Database” on page 84.

8. Complete the schedule choices and click **Next**.
    When the procedure completes, the Tasks main page opens and the Export Event Log task is now added to the Sidebar and the Task List.

Export Session History

KVM ACCESS keeps a record of all user sessions that take place (see Session History, page 193). This function lets you save the session history of each device and port to file. When you choose the Export session history task, the following page appears:

1. Except for the device list, this page is the same as the Export Device Log. Fill in the rest of the page according to the information given under Export Device Log, starting on page 170.
2. For the device list, put a check in the checkbox in front of the desired devices (or check the box at the top of the column to select them all). If you prefer to only export the session history for selected ports, instead of clicking the device's checkbox, click the arrowhead in front of the device's name to expand the port list and click to select the ports.
3. When you have finished with this page, click Next (at the top-right of the panel), to move on.
4. Make your schedule choices in the pages that come up.

    Note: The schedule choices are similar to the ones described for the Backup master server database task. Refer back to page 162 for details, if necessary.

5. When schedule choices are completed, click **Next**. The procedure finishes and returns to the Tasks main page. The Export Event Log task is now added to the Sidebar and the Task List.

Editing a Task

There are two editing tasks that you can perform: changing a task's schedule, and changing the parameters of what you want the task to perform.

To change a task's schedule:

1. Click on the task name on the Sidebar or in the Task List.
2. When the Schedule page opens, make the schedule changes, then click **Save**.

To change the parameters of the task:

1. Click on the task name on the Sidebar or in the Task List.
2. When the Schedule page opens, click **Task Properties** on the Panel Menu.
3. When the Task Properties page opens, make the changes and click **Save**.

Deleting a Task

If a task is no longer needed, put a check in the box in front of its name and click **Delete** at the top-right of the panel.

Replicate Database

Select Replicate Database, to open the Schedule page. The schedule choices are similar to those for the Backup server database task. Refer to page 84 for details.

Note: The default is for the database to automatically replicate once a day at 00:00. Use this page to change the replication schedule. Setting the replication schedule to a too small time interval can adversely influence system performance. If the schedule is set to a too large interval, there can be a long time period when the databases don't match.

When the schedule choices are made, click **Save.**

Appliance Files

The Appliance Files menu is used to centralize firmware management and restore previously backed up configuration files.

Firmware Files

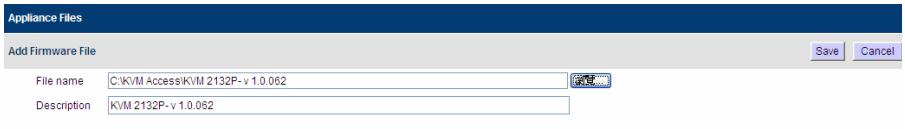
The Appliance Files menu opens to the Firmware Files page. This page lists all the firmware upgrade files stored on KVM ACCESS - showing the specific information about each file.

By making the latest firmware upgrade files available for distribution from this single location, upgrades can be performed from within KVM ACCESS ensuring that all devices on your installation are operating at the same firmware level.

Note: 1. Firmware upgrades are performed under the Tasks submenu.
2. New firmware upgrade packages are posted on the apc website (**www.apc.com**) as they become available. Check the website regularly to find the latest packages and information relating to them.

Adding Firmware Files.

1. Click **Add** to open the Add Firmware File page.



2. Browse to the location where the downloaded files are stored and select the file.
3. Provide a description for the file.
4. Click **Save** to complete the procedure and add the firmware file to the list.

Note: If the firmware file isn't KVM ACCESS compliant (even though it is compliant for the device in a stand-alone configuration), KVM ACCESS will not let you load it.

Deleting Firmware Files.

1. Select Firmware in the Sidebar.
2. In the Interactive Display panel, put a check in front of the file to be removed from the list.

Note: Remove more than one file by checking as many items as required. Remove all the files by checking the box at the top of the column.

3. After selection are complete, click **Delete** at the top-right of the panel.
4. Click **OK** in the confirmation popup.

Configuration Files

Deleting Configuration Files.

Click **Configuration** in the Sidebar to open the Configuration Files page. This page lists the backup configurations for the server made with the Backup device configuration/account information task (and allows you to delete the files you no longer wish to keep.

1. Put a check in front of the configuration to be deleted.
2. Click **Delete** (at the top-right of the panel).

Sidebar Server Tree

When KVM ACCESS Network is selected on the menu bar, clicking on a server name, either in the Sidebar or in the Interactive Display Panel, opens a page with two Panel Menu entries: Properties, and Sessions.

Properties

The Properties page opens as the default. This page displays information reflecting the server's configuration settings. It is view only. Any changes to these settings must be made through the Server Information Panel Menu of the This Server menu (see page 74).

Sessions

Click the Sessions Panel Menu item that appears when KVM ACCESS Network is selected on the Page Menu or in the Sidebar to list all the sessions currently taking place on all KVM ACCESS on the installation and provide the “who, where and when” information for each.

Note: 1. To only see the sessions for a particular KVM ACCESS server, use the navigation buttons at the top-right of the main panel to select it.
2. To end a session, you must do it from the KVM ACCESS Server Sessions Panel Menu.

Login Policy. Select **Allow single login** if you do not want users to be able to log in more than once at the same time.
Select **Allow duplicate logins** if you want users to be able to log in with the same account more than once at the same time. This is the default.

Lockout Policy. To lock users out after a specified number of failed login attempts, click to put a check in the **Lockout users after invalid login attempts** checkbox. The default is enabled.

Note: If you don't check this box, users can attempt to log in an unlimited number of times with no restrictions. For security purposes, enabling the lockout policy is recommended.

- Enter the number of login failures you wish to allow before the user gets locked out in the **Maximum Login Failures** field. The value specified here must be at least 1. The default is 5.
- Enter the amount of time (in minutes) a locked out user must wait before being allowed to log in again in the Timeout field. The value specified here must be at least 1. The default is 30.
- Enabling **Require manual unlock**, means that users will not be able to log in after their account has been locked until they contact an administrator to have the administrator manually unlock the account. See Unlocking User Accounts, page 58, for details. The default is disabled (no check in the checkbox).

Logs

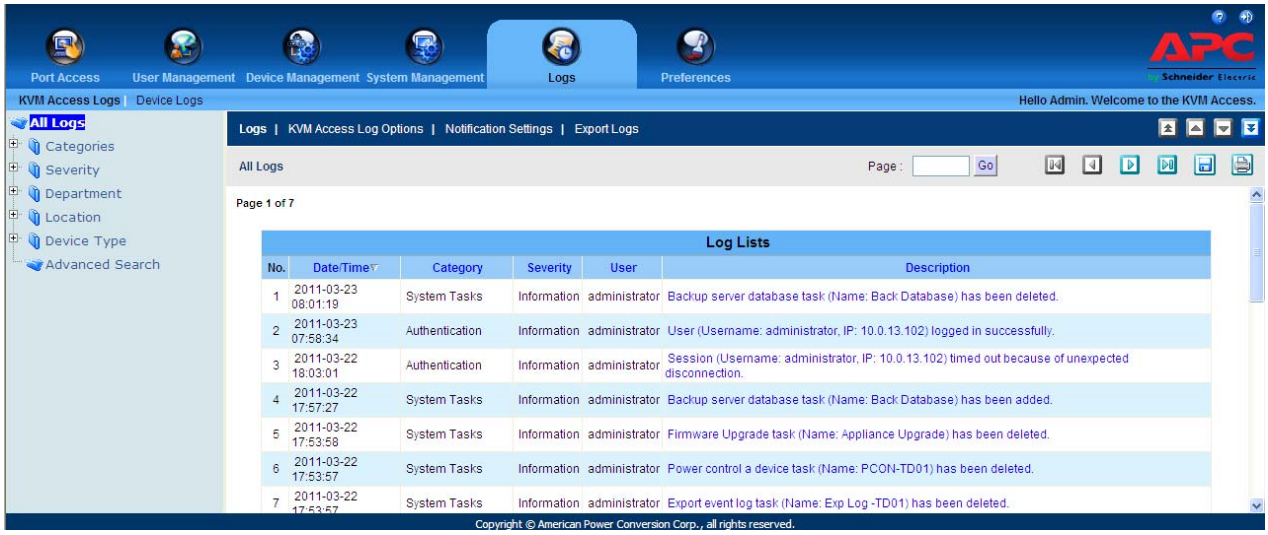
Overview

KVM ACCESS keeps a record of all transactions that take place on its installation. The Logs page provides filters and functions to view and export the log file data, as well as email alerts of specified events as they occur.

KVM ACCESS Logs

Logs

Click the Logs tab to open the default KVM ACCESS Logs page.



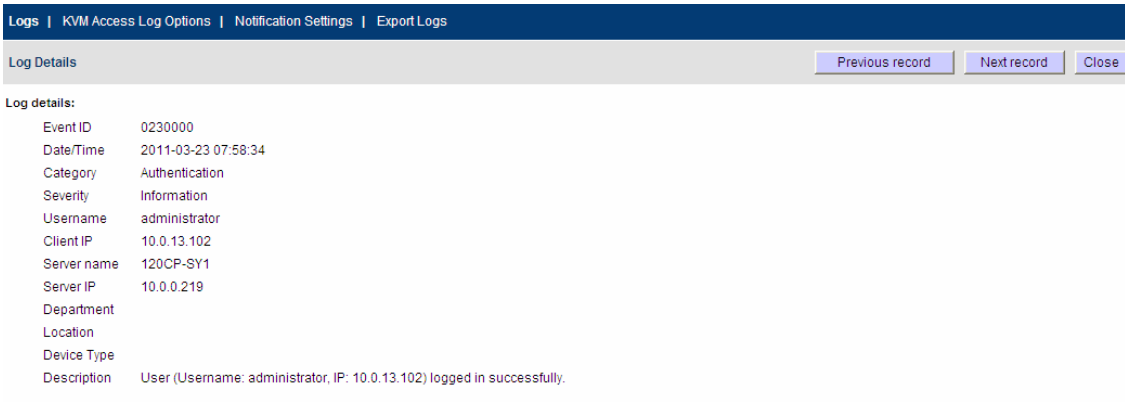
- The default layout shows information concerning all of the events on all the logs on the entire KVM ACCESS installation, displayed in reverse chronological order.
- Change the sorting order of the display by clicking the column headings.
- Reverse the order of a selected heading by clicking the column heading a second time.
- The Sidebar provides a filtering function. Click an item to display only the events that pertain to it. Advanced Search is described in detail on page 100.

Note: 1. A blank page indicates that no log events were recorded for that category. 2. If the Device Traps page (Categories > Device Traps) is blank, it may indicate that Event Trap Notification has not been enabled.

- The top row of buttons at the upper-right of the main panel navigate through the Sidebar (see The Navigation Buttons, page 15).
- The first four buttons on the lower row navigate through the pages of the listed events. To move to the first page, click the leftmost arrow. Click the rightmost arrow to go to the last page. The middle arrow buttons move one page forward or back.

Note: These buttons are only active when there is a relevant action they can perform. Example: From the first page of several, the **move forward one page** and **move to the last page** buttons are active, but the **move backward one page** and **move to the first page** buttons are not.

- Click on an item's Description to open a page with detailed information about the item.

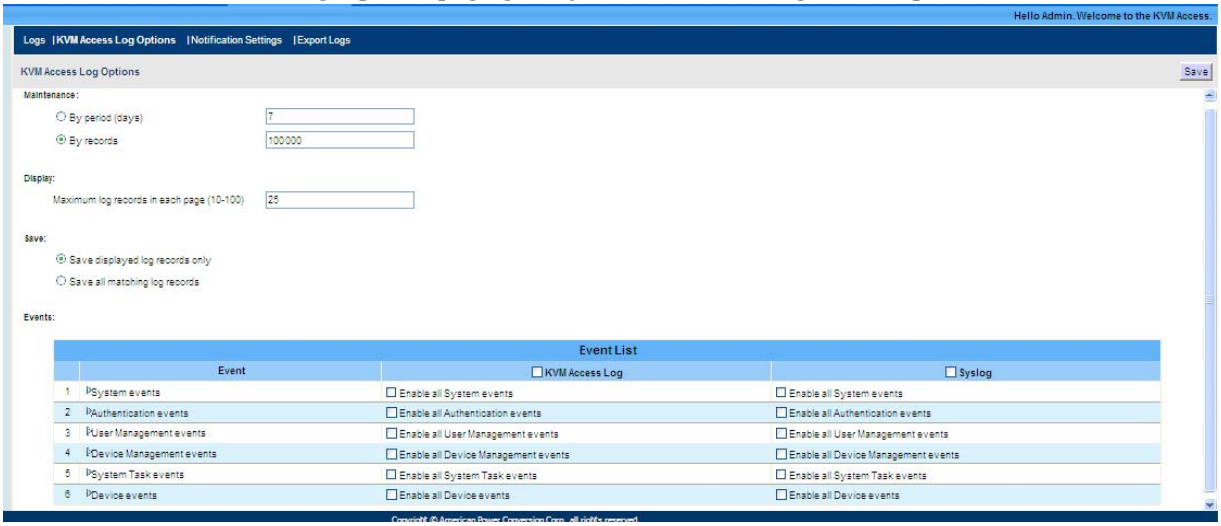


Use the buttons at the top-right of the panel to move to the previous or next item in the details view, or close the page and return to the Log page.

- To save the log list to a file, click the **Diskette** icon button. Only the displayed list (All, or a filtered choice) is saved.
- To print out the log list, click the **Printer** icon button. Only the displayed list (All, or a filtered choice) is printed.

KVM ACCESS Log Options

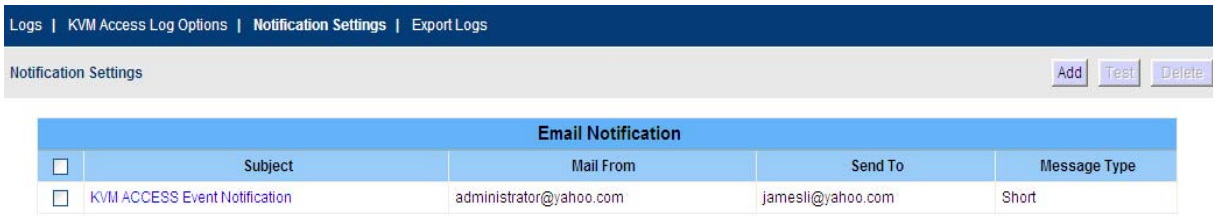
The KVM ACCESS Log Options page gives you control over log file composition and maintenance.



Item	Description
Maintenance	Click a radio button to select to maintain the log database on a **Days** or **Records** basis. Select the number of days or records. When the number is reached, events are discarded on a "first in, first out" basis. The range is from 7-90 days, and 1000-100,000 records.
Display	Set the maximum number of events to display on the web page. The range is from 10-100.
Save	Click a radio button to save only the events that are displayed or all the events that correspond to the selections made in the Events List when the log file is saved.
Events	• Select which events to track and record in the KVN Access Log, the Syslog, or both. • There are 7 event categories. Each contains a list of separate events. To record all events for a category, put a checkmark in front of the **Enable all ...** events entry. • To only record selected events for a category (rather than all of them), click the arrowhead in front of the category name to open the list of events, then check or uncheck each event. 

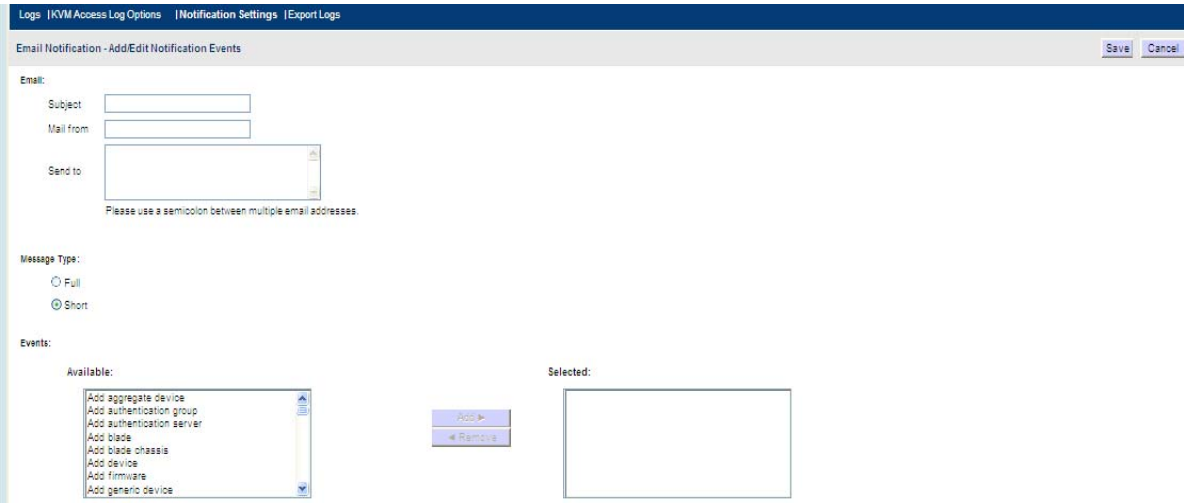
Notification Settings

This page informs a selected user of specific events that occur on the KVM ACCESS installation.



Adding and Configuring Notification Users.

1. Click **Add** at the top-right of the panel to open the Email Notification - Add/Edit Notification Events page.



2. Enter an appropriate title for the notification message in the **Subject** field
3. Enter the email address of one of the administrators in the **Mail from** field.
4. Enter the email address of the person who will receive the email notification in the **Send to** field. If the notification will go to more than one person, use a semicolon to separate the email addresses. Do not leave a space before or after the semicolon.
5. Select the message type: **Full** or **Short**.
6. Select the event in the **Available** column, then click **Add** to move it into the **Selected** column. To receive email notification of other events, repeat the steps.
7. Click **Save** when finished to save the configuration and return to the Notification Settings page.

Note: In order for users to receive email notification of events, SMTP settings information must be configured on the KVM ACCESS' SMTP Settings page. See page 75 for details.

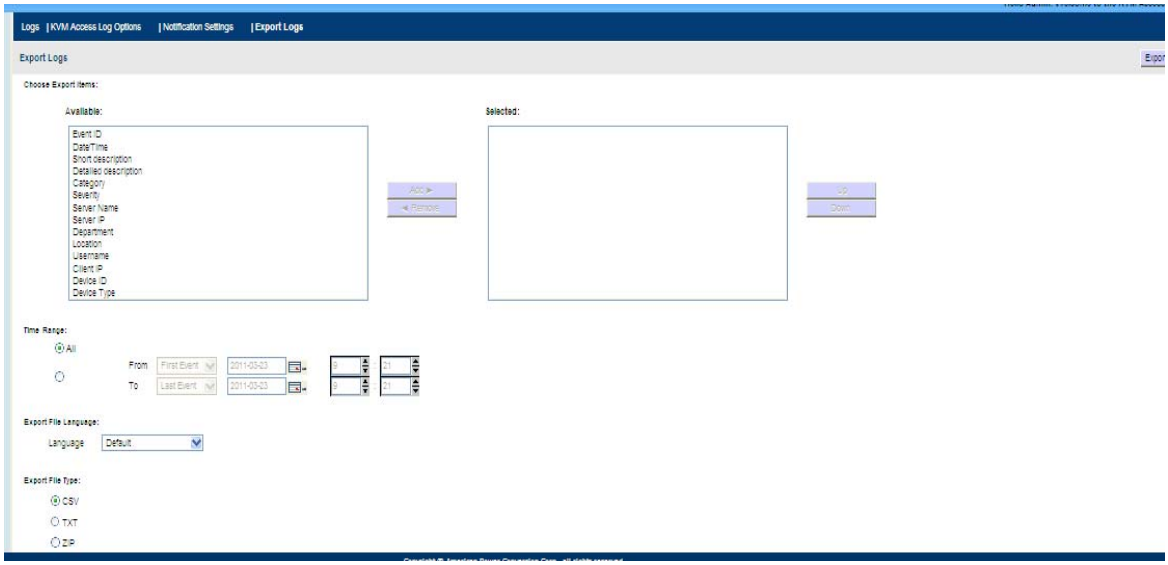
Modifying Notification Configurations. To modify a notification configuration, click its Subject name in the Email Notification table, make changes on the Email Notification - Add/ Edit Notification Events page, and click **Save** at the top-right of the panel.

Deleting Notification Configurations. To delete a notification configuration, click to put a check in the checkbox in front of its Subject name in the Email Notification table, then click **Delete** at the top-right of the panel.

Testing Event Notifications. To check that an event notification is working properly, click to put a check in the checkbox in front of the notification's Subject name in the Email Notification table, then click **Test**. If the system is working properly, the event notification recipient will receive an email with the event notification.

Export Logs

The Export Logs page is used to save selected logged events to a file.



To save selected logged events to a file:

1. Select a log file item to include in the exported file in the **Available** column, then click **Add** to move it into the **Selected** column. Repeat for any other log file items to be included.
2. To change the order of the Selected items, click on the item to be moved, then click **Up** or **Down** to change the position.
3. Time Range: Select **All** to export all the selected items' records in the database. To export records for a particular time period, select the radio button below it and set the time parameters with the **From** and **To** settings.
4. Export File Language: Choose **Default** to have the file exported in the same language as the browser uses. To use a different language, select one from the drop down list.
5. Export File Type: Click the radio button in front of your choice. If one of the encryption options is chosen, enter a password into the Password field that opens.

   Note: Make a note of the password. It will be needed to import the file.
6. When finished, click **Export** (at the top right of the panel) to open a dialog box.
7. Select the **Save File** option to save the log file to the location you specify.

   Note: The files can be renamed, as long as the extension is not changed.

Import Logs

The Import Logs page is used to open previously saved log files for viewing.

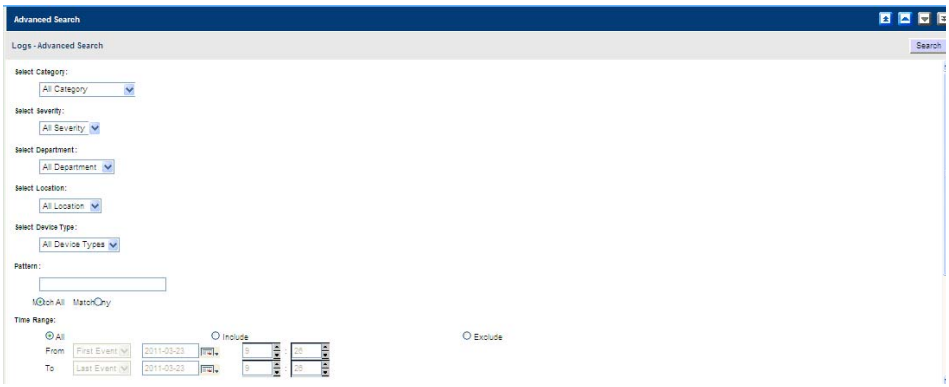
To import a previously saved log file, do the following:

1. Enter the full path to the file in the Log file field or click Browse to navigate to it.
2. If the file has been encrypted, enter the password that was used when it was created into the Password field.
3. Click **Import** (at the top-right of the panel). When the file is imported, its contents appear in the KVM ACCESS Log List panel.

Advanced Search

Fine tune your search by narrowing down the parameters for each of the search choices. To perform an advanced search:

1. In the Sidebar, click Advanced Search. The Logs - Advanced Search screen opens:



2. Select specific search parameters from the drop down lists.
3. To search for a particular word or string, enter it in the Pattern field, then select the terms required for a match.
4. Time Range: Select **All** to search all the records in the database. To search for a particular time period, click **Include** or **Exclude**, and set the parameters with the **From** and **To** settings.

Note: 1. If **Include** is selected, all events in the specified time range are searched.
2. If **Exclude** is selected, only events that fall outside of the time range are searched.

5. When finished, click **Search** (at the top- right of the panel).

The search results are displayed in the Log List in the main panel.

- To save the search results to a file, click the **Diskette** icon button.
- To print out the search results, click the **Printer** icon button.
- Change the sort order of the list by clicking the column headings.

Device Logs

KVM ACCESS acts as a log server for all APC devices, recording the system events that take place on those devices in a database. Click **Device Logs** on the Submenu bar to open the Device Logs Search page to search for events containing specific words or strings.

- The default layout shows log information for all devices on the KVM ACCESS installation displayed in reverse chronological order.
  - Click the Date/Time column heading to change the sort order between standard and reverse chronological order.
  - Click the Description column heading to change the sort order between standard and reverse alphabetical order.
- To use the Sidebar filtering function, click on a device to display only the events that pertain to it.
- Use the navigation buttons (arrowheads) at the top-right of the main panel to move through the pages of the log list. To move to the first page, click the leftmost arrow. Click the rightmost arrow to go to the last page. The middle arrow buttons move one page forward or back.

Note: These buttons are only active when there is a relevant action they can perform. Example: From the first page of several, the **move forward one page** and **move to the last page** buttons are active, but the **move backward one page** and **move to the first page** buttons are not.

To save the log list to a file, click the **Diskette** icon button . Only the displayed list (All, or a filtered choice) is saved.

To print the log list, click the **Printer** icon button. Only the displayed list (All, or a filtered choice) is printed.

Device Log Search

To search the logs:

1. To search for a particular word or string, enter it in the Pattern field.
2. Time Range: Select **All** to search all the records in the database for the selected pattern. To search records for a particular time period, select the **Include** or **Exclude** radio button, and set the time parameters with the **From** and **To** settings.

   Note: 1. If **Include** is selected, all events in the specified time range are searched.
   2. If **Exclude** is selected, only events that fall outside of the time range are searched.

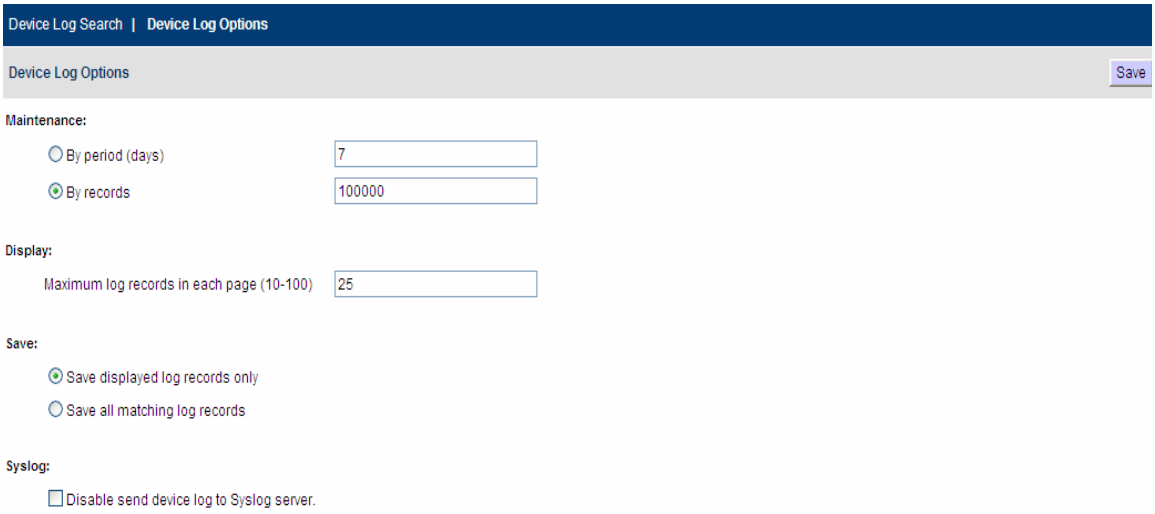
3. When finished, click **Search** (at the top- right of the panel).

The search results are displayed in the Log List in the main panel.

- To save the search results to a file, click the **Diskette** icon button.
- To print out the search results, click the **Printer** icon button.
- Click the column headings to change the sort order.

Device Log Options

The Device Log Options page provides management options regarding the KVM ACCESS's device log database. Select Device Log Options, to open the page.



- Maintenance: Click a radio button to maintain the device log database by **Days** or **Records**, then enter the number of days or records. When the number is reached, events are discarded on a “first in, first out” basis.
- Display: Set the maximum number of record events to display on the web page.
- Save: Save the device logs to a file:
  - Click a radio button to choose to save only the currently selected device log records, or all of the device log records, then click **Save** (at the top-right of the panel).
  - In the dialog box that opens, select **Save File**. The log file is saved in CSV format, which can be read by a spreadsheet program.

Specifications

Technical Support

For online technical support, go to **www.apc.com/support**.
Product information to have available:

- Product model number, serial number, and date of purchase.
- Your computer configuration, including operating system, revision level, expansion cards, and software.
- Any error messages displayed at the time the error occurred.
- The sequence of operations that led up to the error.

USB Authentication Key Specifications

Function		Key
Environment	Operating Temp	0 - 40 C
	Storage Temp	-20 - 60 C
	Humidity	0 - 80 % RH
Physical Properties	Composition	Metal and Plastic
	Weight	14 g
	Dimensions	8.36 x 2.77 x 1.37 cm

Compatible Products

KVM Switches that are capable of being managed in a KVM ACCESS installation:

- KVM2132P
- KVM2116P
- KVM1116P

Note: 1. These are the currently supported devices. Visit the web site to see if any additional devices are supported.
2. The switches can be used as parents to cascade the switches mentioned in the next section.

Supported KVM Switches

Fully supported KVM switches that can be used in a cascaded installation:

- KVM2132P
- KVM2116P
- KVM1116P
- KVM0216A
- KVM0116A
- KVM0108A

Note: The installation cannot be cascaded beyond the second level.

Device ANMS Settings

To enable KVM ACCESS Management of a device from the device's ANMS settings page:

1. Log into the device.
2. Refer to the device's User Manual to locate its ANMS settings page.
3. In the ANMS page, click the checkbox to enable KVM ACCESS Management, then enter the IP address and device port number (see “Device port” on page 8), of the KVM ACCESS server that will manage the device.

VPNs

A VPN (virtual private network) is a private network that uses a public network (usually the Internet) to connect several sites. It typically includes several WANs. Many companies create their own VPN to provide a secure network connection between two sites. While the VPN network is secure, it can be slow.

Firewalls

When several KVM ACCESS servers are located behind separate firewalls, the following service ports must be specified on the servers, and the corresponding ports must be opened on the firewall.

1. The KVM ACCESS server's HTTPS port
2. The KVM ACCESS Proxy port.

KVM ACCESS Proxy Function

The KVM ACCESS Proxy function relates to KVM ACCESS servers located behind a firewall. In order for KVM ACCESS Client Workstations outside the firewall to access KVM and Serial devices managed by KVM ACCESS servers inside the firewall, the KVM ACCESS Proxy function must be enabled on those servers, and the port specified as the proxy port must be opened on the firewall.

Note: 1. While a KVM ACCESS Client Workstation outside the firewall can open a web browser session with a KVM ACCESS server inside the firewall when the proxy port has not been specified and opened, viewers for the KVM and Serial Console devices managed by that KVM ACCESS server cannot be opened.
2. If the Proxy function is not enabled, to access the devices you must open all of the service ports on the firewall required by the devices.

Name, Description, and Range Parameters

Note: Unless otherwise specified, field entries can be input in any supported language.

Category		Length/Range	Default
Users	Login name	Up to the equivalent of 16 English alphanumeric characters. The minimum number is base on the account policy settings. The following characters may not be used: / \ [ ] : ; | = , + * ? < > @ “ ‘	
	Screen name	Up to 32 Bytes. The following characters may not be used: “ ‘	
	Password	The equivalent of 0 - 16 English alphanumeric characters. The minimum number is based on the account policy settings. 0 means no password authentication.	
	Description	Up to 256 Bytes.	
	Session Timeout	1 - 99 minutes	3 minutes
	Unexpected disconnection timeout	2 - 10 minutes	2 minutes
	Email	Up to 256 Bytes. From: 0 - 64 To: 0 - 128 Subject: 1 - 128	
Groups	Name	2 - 32 Bytes. The following characters may not be used: “ ‘	
	Description	Up to 256 Bytes.	
User Type	Name	2 - 32 Bytes. The following characters may not be used: “ ‘	
	Description	Up to 256 Bytes.	
Authentication Server	Server name	2 - 32 Bytes. The following characters may not be used: “ ‘	
	Description	Up to 256 Bytes.	
	Browser Method	Unlimited for Username and Password. **Note:** KVM ACCESS performance is adversely affected if too many characters are used.	
KVM ACCESS Authentication	Username Minimum	Up to the equivalent of 16 English alphanumeric characters. The minumum number is based on the account policy settings. The following characters may not be used: / \ [ ] : ; | = , + * ? < > @ “ ‘	6
	Password Minimum	The equivalent of 0 - 16 English alphanumeric characters. The minimum number is based on the account policy settings. 0 means no password authentication.	6
	Password Expires	No limit on the number of days.	
Devices	Name	0 - 32 Bytes.	
	Description	Up to 256 Bytes.	
	Contact name	No limit on the number of Bytes.	
	Telephone	No limit on the number of Bytes.	
	Email notification	No limit on the number of Bytes.	
Aggregate devices	Name	0 - 32 Bytes.	
	Description	Up to 256 Bytes.	
Folders	Name	0 - 32 Bytes.	
	Description	Up to 256 Bytes.	

Departments/ Locations	Name	0 - 32 Bytes.	
	Description	Up to 256 Bytes.	
Tasks	All Tasknames	No limit on the number of Bytes.	
	Master Database Backup Password	0 - 8 Bytes. 0 means no password authentication.	
	Export Device Log Pattern	No limit on the number of Bytes.	
KVM ACCESS Log Options	By Period	7 - 90 days	
	By Record	1000 - 100,000	
	Records per page	10 - 100	
Log Notification Settings	Subject	1 - 128 Bytes.	
	Mail from	Up to 64 Bytes.	
	Send to	Up to 128 Bytes.	
Preferences: Web options	Display screen name	0 - 32 Bytes.	

Trusted Certificates

When logging into the device from your browser, a Security Alert message opens to inform you that the device's certificate is not trusted, and asks if you want to proceed.

The certificate can be trusted, but the alert is triggered because the certificate's name is not found on the Microsoft list of Trusted Authorities. You can ignore the warning and click **Yes** to go on.

Note: To avoid going through the certificate acceptance prompt each time, use a third party certificate authority (CA) to obtain a signed certificate. See “Importing a Signed SSL Server Certificate” on page 80, for details.

Troubleshooting

Problem	Resolution
After installing KVM ACCESS, the message: **Error 1067** appears a few minutes later.	The error message is generated by the Operating System, it indicates that the KVM ACCESS service is unable to run. To resolve the problem try: 1. Rebooting the computer. 2. Checking that your computer meets the minimum requirements to run KVM ACCESS (see “Server Requirements” on page 3). 3. Uninstalling and reinstalling KVM ACCESS. If there was a previous version of KVM ACCESS, and you are installing this version as a new installation rather than as an upgrade, this may indicate that you did not remove all files from the older version (see “Uninstalling KVM ACCESS Software” on page 12).
I entered the IP address for the KVM ACCESS website, but I can't bring up the KVM ACCESS login page.	1. KVM ACCESS only allows HTTPS requests. HTTP requests from a browser are automatically redirected to HTTPS requests. The default port for HTTP is 80. The default port for HTTPS is 443. If either of these ports has been renamed by the administrator, the port number must be entered as part of the URL string. **Example:** If KVM ACCESS' IP address is 10.10.10.10, and the SSL port has been set to 8443, then the URL string entered in the browser should be: https://10.10.10.10:8443. 2. Other services running on the KVM ACCESS server are using the default ports. Use the “KVM ACCESS Utility” on page 110 to change the port settings. 3. Make sure that KVM ACCESS is running. If you are running Windows, see “Post-installation check” on page 9 if you are running Linux, see “Post-installation Check” on page 11.
The language of the login dialog box is not the language I have set in my KVM ACCESS Preferences.	The login page first looks at the language that your browser is set for, and next looks at your OS language. After you have logged in, KVM ACCESS will display in the language you have set in Preferences. See “Web options” on page 17 for details.
I cannot log in to KVM ACCESS.	Make sure your Username and Password are correct.
When I try to log in, I get the following message: "Login failed. You are attempting to log in from a computer that already has a browser session open."	Netscape and Firefox (as well as other Mozilla-based browsers), share the same session ID for multiple connections to the same server. KVM ACCESS will deny a login request once there is a session open with the same session ID. Either: 1. End the currently open session and log in again, 2. Log in from a different computer, or 3. Log in with a non-Mozilla based browser. **Note:** This condition occurs in some versions of IE running on Windows98, as well.
When I log in, the browser generates a CA Root **certificate is not trusted**, or a **Certificate Error** response.	The certificate's name is not found on Microsoft's list of Trusted Authorities. The certificate can be trusted. See “Trusted Certificates” on page 106, for details.
After logging in to KVM ACCESS, there is no Port Access tab or Port Access page.	You have not been authorized to access any ports. Check with your KVM ACCESS administrator to get authorization to access the ports for which you are responsible.
After logging in to KVM ACCESS, I cannot open the page for the device I want to access.	Check with your KVM ACCESS administrator to find out whether you are authorized to access that device.
When I log in to KVM ACCESS, the System Management tab page opens with only two menu entries: **This Server** and **License**.	A license conflict has occurred. See ,“If all the licenses are in use, only if a currently unlocked port is locked, or if an aggregate device is deleted, freeing up the license it was using, can a locked port (or new aggregate device) use that license.” on page 82 for details on resolving the problem.

Troubleshooting, continued

I am not receiving email notifications of event trap situations.	1. Check that the email server settings have been specified correctly in the KVM ACCESS Manager. 2. Check that the email address in the related device's settings is correct. 3. Check that the event trap settings for the related device has been specified correctly.
When I try to access my Generic device from the Tree View nothing happens.	Generic devices are accessed directly from the device's IP address. If the IP address has changed, then clicking the old IP address will not connect to the device. Change to the device's new IP address.
The device I want to add cannot be found.	1. Make sure the KVM ACCESS Manager is running and all services have started successfully. 2. Make sure that Management has been enabled and specified correctly in the device's ANMS settings.
When adding a Cat5e KVM switch, can I add all the ports at the same time?	Yes, provided all the ports have KVM Adapters attached and their devices are on line. See the note on page 48, for details.
The icon for my port indicates the port is online, but the icon for the device it belongs to indicates it is offline. I am unable to access the device or port.	This indicates that the device's firmware does not support this version of KVM ACCESS. Update the device's firmware to the latest version.
My APC device is not recognized by KVM ACCESS.	1. The device may not be supported by the KVM ACCESS. See “Compatible Products” on page 103, for a list of supported devices. 2. Upgrade to the device's latest firmware version to be recognized by KVM ACCESS.
I set the KVM ACCESS for "No timeout" operation, but it timed out anyway.	The change doesn't take effect until the next time you log in.
After making a setting change and clicking Save, an HTTP Status 500 - error page opens.	A mistake was made when the setting was entered. This is an Apache Tomcat error message that appears whenever it receives an invalid setting. To recover, select any other tab then come back to make your change. Be sure to enter a valid setting.

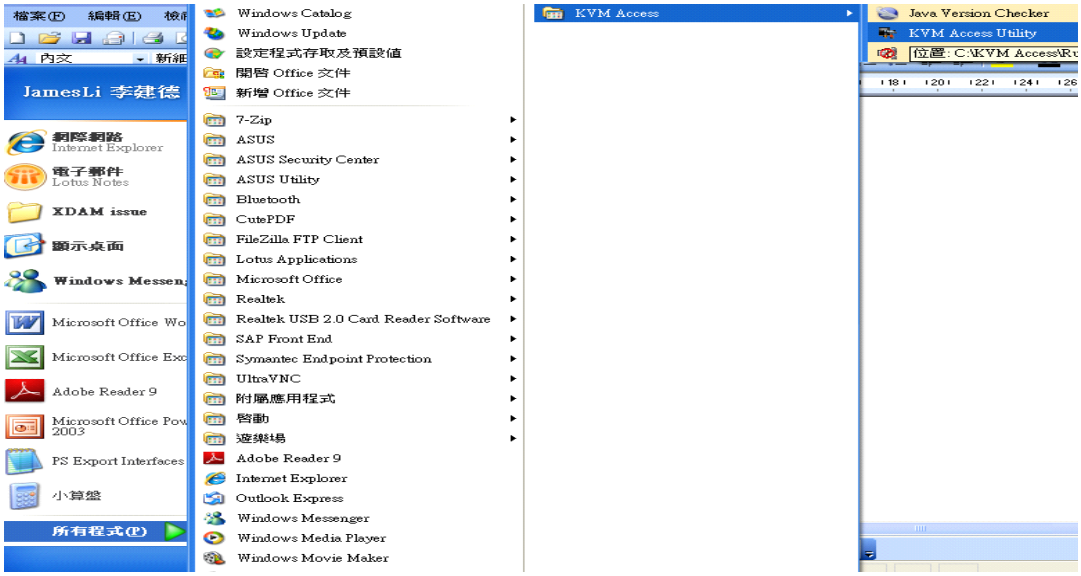
When a viewer is opened, the web page does not display or work correctly, and an error message displays.	Reset the Internet Explorer security settings to enable Active Scripting, ActiveX controls, and Java applets. By default, Internet Explorer 6 and some versions of Internet Explorer 5.x use the High security level for the Restricted sites zone. Microsoft Windows Server 2003 uses the High security level for both the Restricted sites zone and the Internet zone. To enable Active Scripting, ActiveX controls, and Java applets: • Start Internet Explorer. • On the Tools menu, click **Internet Options**. • In the Internet Options dialog box, click **Security**. • Click **Default Level**. • Click **OK**. Verify that Active Scripting, ActiveX, and Java are not blocked. If some computers work but others do not, verify that Internet Explorer or another program on your computer such as an anti-virus program or a firewall are not configured to block scripts, ActiveX controls, or Java applets. Verify that your anti-virus program is not set to scan the Temporary Internet Files or Downloaded Program Files folders. Delete all temporary Internet-related files. To remove temporary Internet-related files from your computer: Start Internet Explorer. • On the Tools menu, click **Internet Options**. • Click the **General** tab. • Under Temporary Internet files, click **Settings**. • Click **Delete Files**. • Click **OK**. • Click **Delete Cookies**. • Click **OK**. • Under History, click **Clear History**, and then click **Yes**. • Click **OK**. Make sure that you have the latest version of Microsoft DirectX installed. For information about installing the latest version of Microsoft DirectX, visit the following Microsoft Web site: http://www.microsoft.com/windows/directx/default.aspx?url=/windows/ directx/downloads/default.htm Make sure that you have the latest version of the Java JRE installed. For information about how to install the latest version of the JRE visit the Java Web site: www.java.com

KVM ACCESS Utility

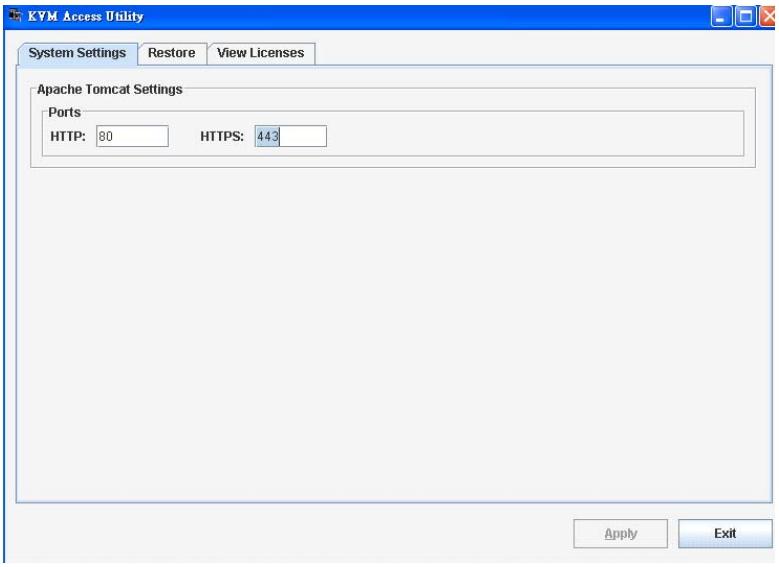
Overview

The KVM ACCESS Utility is installed as part of the installation procedure. It allows configuration of a number of KVM ACCESS' parameters from the desktop of the computer that KVM ACCESS runs on without invoking the browser GUI.

In Windows, to run the program, open the Start menu; navigate to KVM ACCESS (Programs > KVM ACCESS), and select KVM ACCESS Utility:



In Linux, as root, go to the /home/KVM ACCESS/Runable directory, and run the KVM ACCESS_Utility file.



The Utility offers System Settings, Restore, and View Licenses.

System Settings

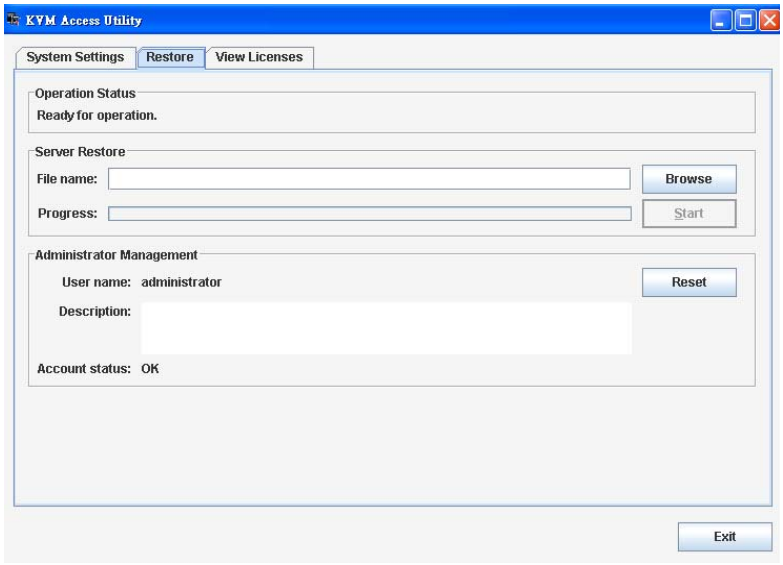
The program that serves the KVM ACCESS' web pages is Apache Tomcat. KVM ACCESS' installation program asks you to specify the ports that Apache Tomcat monitors for web requests.

- The HTTP port is the regular port that Apache Tomcat monitors. The default is 80. If you use a different port, specify the port number in the URL of the browser.
- The HTTPS port is the secure port that Apache Tomcat monitors. The default is 443. If you use a different port, specify the port number in the URL of the browsers.

If a port conflict occurs and prevents the web page from opening, use this utility to change the port settings. After making your settings, click **Apply** to save the changes.

Restore

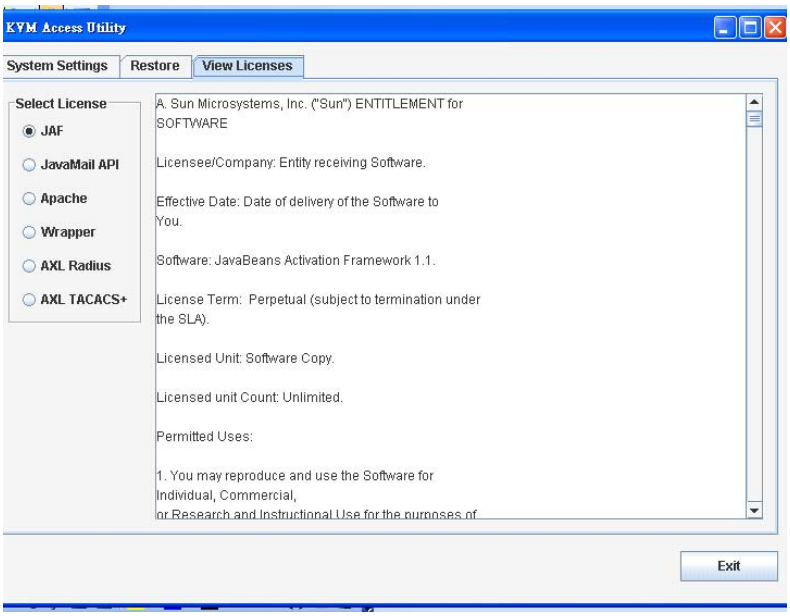
Click the **Restore** tab to open the dialog box.



Panel	Description
Operation Status	Used to check that the KVM ACCESS service is up and running normally.
KVM ACCESS Restore	Used to restore the KVM ACCESS' master server database to a previously saved version (see “Backup the Server Database” on page 84). Click **Browse** to navigate to the location of the file. Select the file and return to the dialog box then click **Start** to begin the operation. The progress of the operation is indicated in the Progress field.
Administrator Management	Clicking Reset returns the default System Administrator's account to the default (apc / apc). If this account has been Locked (see “Lockout Policy” on page 94) it is automatically Unlocked.

View License

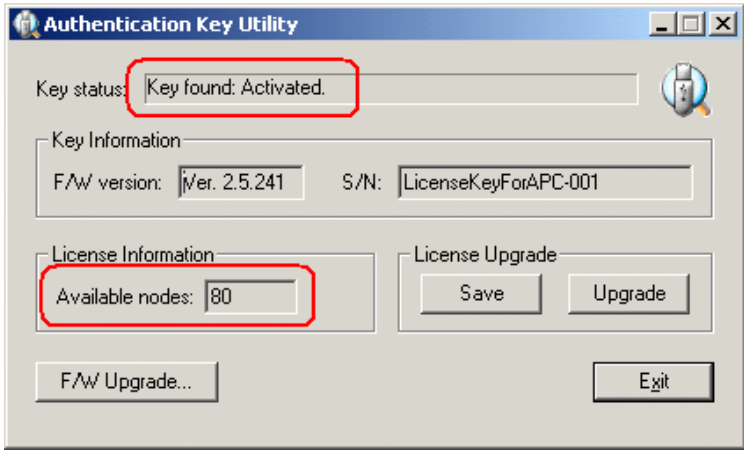
View the licenses related to KVM ACCESS. To view a license, click its radio button.



Authentication Key Utility

Overview

The Authentication Key Utility (AuthKeyStatus.exe), is a Windows-based utility for accessing and updating the information and data contained in the KVM ACCESS Authentication Key. AuthKeyStatus.exe, can be found on the KVM ACCESS CD.



Key Status Information

The dialog box is described in the table below:

Section	Purpose
Key Status	Indicates whether the key has been recognized and accepted as valid or not.
Key Information	Displays the key's current firmware version and serial number.
License Information	Displays the number of nodes the key is licensed for.
License Upgrade	These buttons are used when performing an Offline license upgrade.
F/W Upgrade	This button is used to upgrade the authentication key's firmware.

Key Utilities

The License Upgrade and F/W Upgrade sections offer utilities that allow you to upgrade the key's firmware (F/W Upgrade), and to upgrade the number of servers and nodes authorized by the license (License Upgrade).

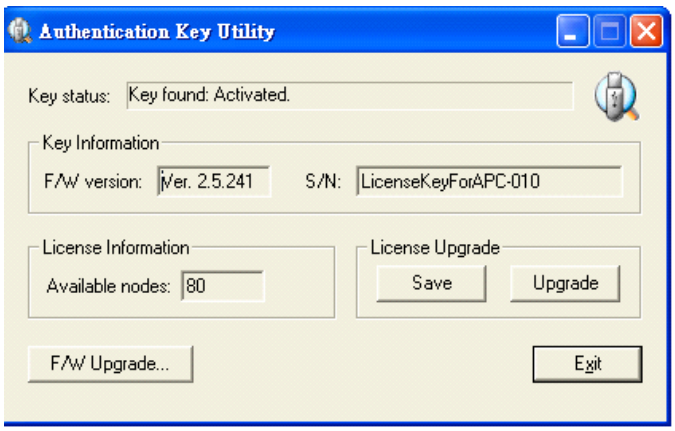
Key Firmware Upgrade

As new revisions of the KVM ACCESS Authentication Key's firmware are released, the upgrade files are posted on **www.apc.com**. Check the web site regularly to find the latest files and information.

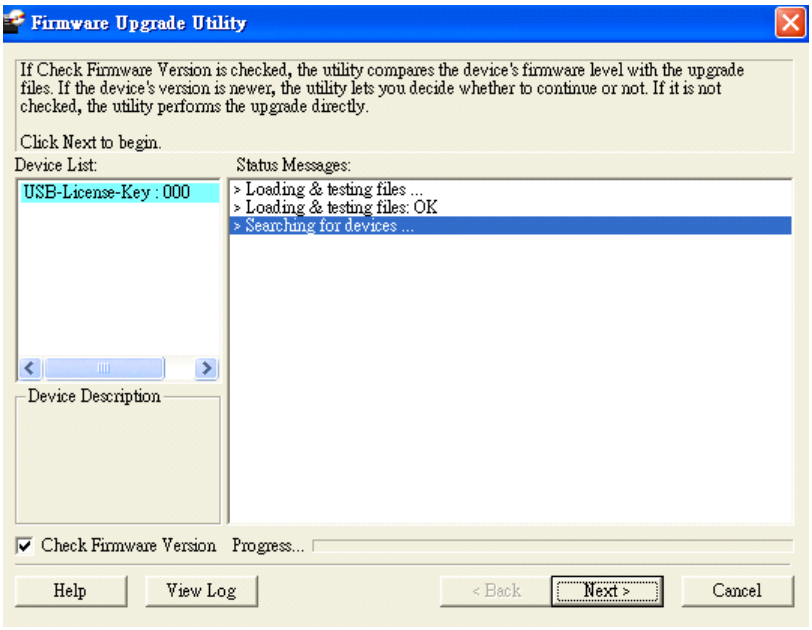
Starting the Upgrade

1. Go to **www.apc.com** to download the new firmware file to your computer.
2. With the authentication key plugged in, run the Key Status Utility (AuthKeyStatus.exe).

   Note: 1. AuthKeyStatus.exe only runs under Windows.
   2. Firmware version 2.1.204 or higher is required for KVM ACCESS authentication keys to support the license upgrade function.
   3. KeyStatus.exe, can be found on the KVM ACCESS CD and copied to your computer.
3. In the screen that opens, click **F/W Upgrade**.
4. In the File Open dialog box that opens, select the firmware upgrade file, then click **Open**.
5. Read and Agree to the License Agreement (click the **I Agree** radio button).



6. The utility finds your device, and lists it in the Device List panel. Click **Next** to continue.

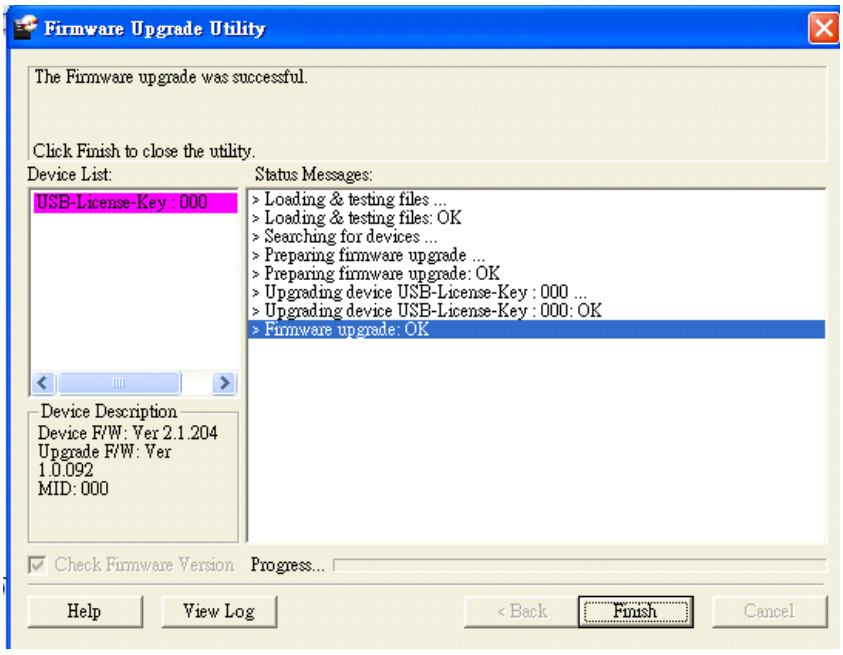


Note: Check Firmware Version compares the device's firmware level with the upgrade files. If the device's version is higher than the upgrade version, a dialog box opens giving you the option to Continue or Cancel. If you don't enable Check Firmware Version, the Utility installs the upgrade files without checking them.

Upgrade Succeeded

When the upgrade has completed, a screen opens to inform you that the procedure was successful.

Click **Finish** to close the Firmware Upgrade Utility.



Key License Upgrade

Overview

KVM ACCESS allows ecustomers to update their authentication keys to reflect an increase to their number of licenses. Contact APC to purchase the 1024 key license upgrade (SEKVM1024N).

Note: A separate order must be processed for each key.

To upgrade the key:

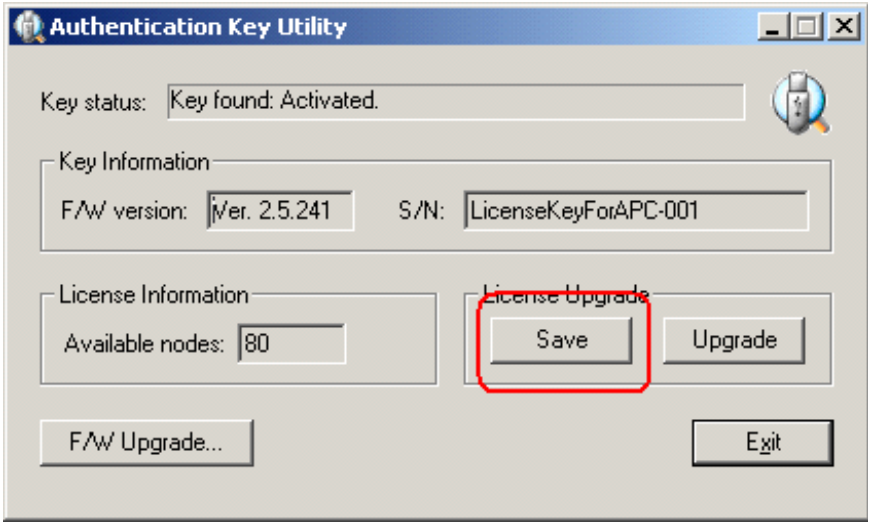
- A Windows-based Key Status Utility is used to extract the key's information and write it to a Key Information Data File. The key information data file is then used in a a browser session to generate a license upgrade file. After the license upgrade file has been generated, the Key Status Utility is used again to write the upgrade file's information to the license key.
- The customer provides APC with the key information data file (extracted with the Key Status Utility) which the APC uses to generate the customer's key license upgrade file. APC then returns the key license upgrade file to the customer which the customer uses with the Key Status Utility to upgrade the Authentication Key's license information.

Upgrade Procedure

An upgrade procedure can be performed by APC. The customer must email the key information data file to the APC (KVMAccessUpgrade@schneider-electric.com) to receive a key upgrade file in return.

Preliminary Steps. To perform the upgrade, the customer must create a Key Information Data File.

1. 1. With the authentication key plugged in, run the Key Status Utility (AuthKeyStatus.exe).
2. 2. In the License Upgrade panel of the dialog box that opens, click **Save** to create a Key Information Data File (KeyUpload.dat).



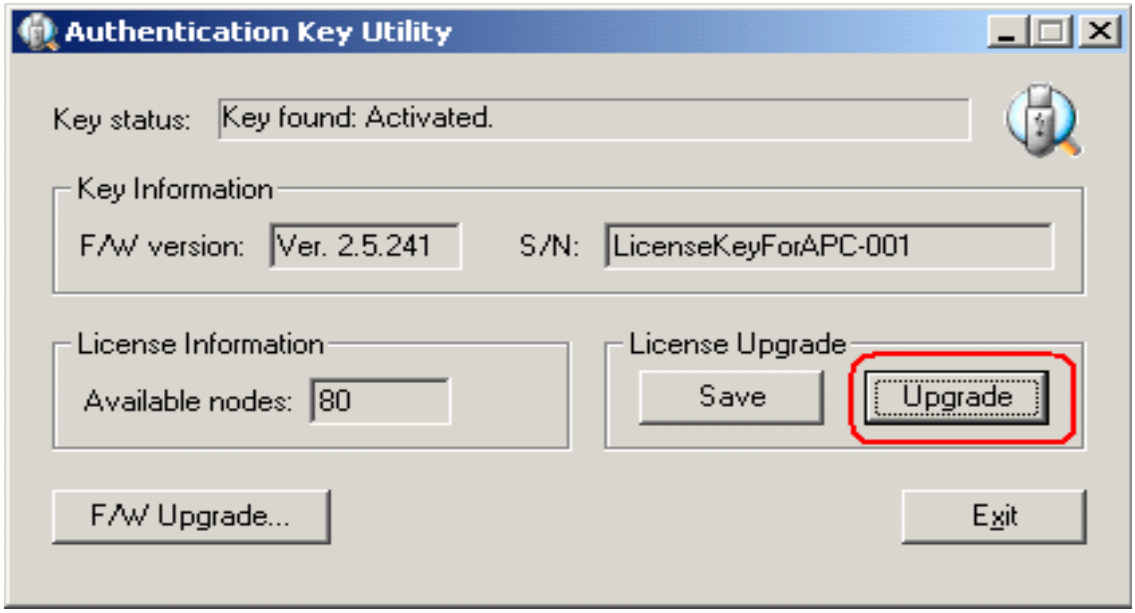
Note: The Key Information Data File is created in the same directory in which the Key Status Utility resides.

After the Key Information Data File is created, send a copy to APC.

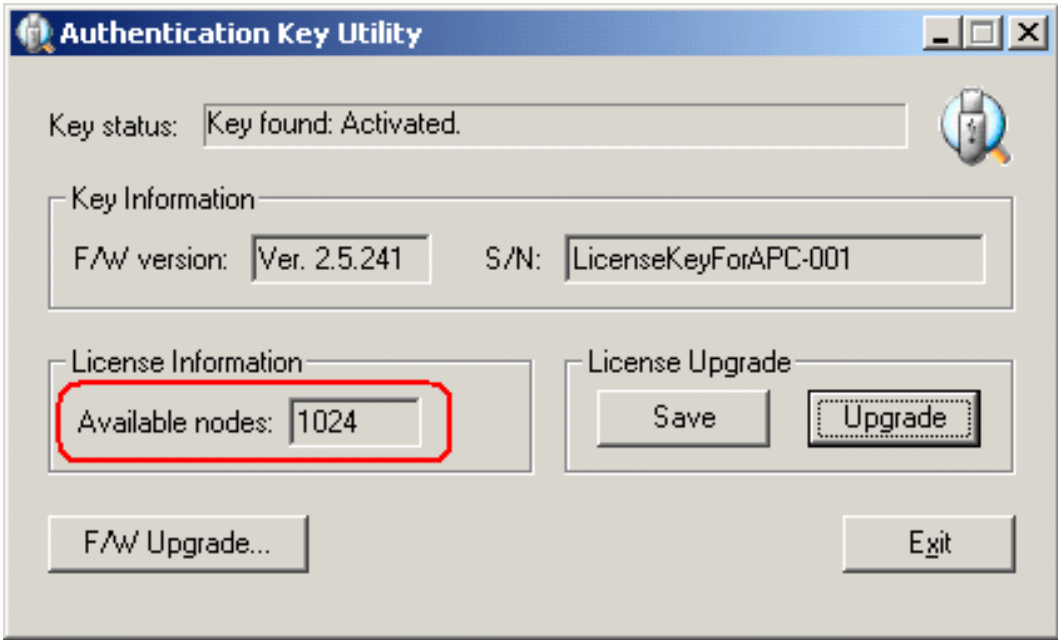
Performing the Upgrade. After the upgrade process is finished, an "Upgrade File" will be sent to allow you to upgrade your license key.

To upgrade license key:

1. Run the Key Status Utility again.
2. In the License Upgrade panel, click **Upgrade**.



3. In the dialog box that opens, select the upgrade file (KeyUpgrade.dat).
   – Click **Open**. A window opens stating that the upgrade was successful.
   – The figure for the number of licenses in the License Information panel changes to reflect the upgrade.



External Authentication Services

Overview

In addition to its own internal Username / Password authentication procedure, KVM ACCESS supports authentication from external, third party authentication services. If a third party service has been specified for a user, KVM ACCESS transfers the login information to the appropriate service for authentication using an encrypted HTTPS (SSL) connection. The KVM ACCESS supports the following third party external authentication servers: LDAP, Active Directory, RADIUS, TACACS+, and Windows NT Domain.

Approved Services

The following services have been tested and approved for use with KVM ACCESS:

- AD Server: Microsoft Windows Server 2003
- LDAP: Microsoft Windows Server 2003; OpenLDAP
- RADIUS: Microsoft IAS for Windows Server 2003; FreeRADIUS
- TACACS+: Microsoft Windows Server 2003 (ClearBox)
- Microsoft Windows NT Domain

LDAP/LDAPS - OpenLDAP Setting Example

In this example, the external server uses OpenLDAP; its IP address is 192.168.10.100; its service port is 389, and the server administrator has created a file named: KVMAccessldap.ldif in the OpenLDAP directory.

– dn: cn=KVM ACCESS,ou=software,dc=apc,dc=com

– objectclass: top

– objectclass: person

– objectclass: organizationalPerson

– cn: KVM ACCESS

– sn: KVM ACCESS

– userPassword: password

The LDAP administrator can check the LDAP definition with LDAP Browser.

The KVM ACCESS Administrator gets this information to use in the Adding an External Authentication Server procedure (see “LDAP” on page 46). In this example, the fields would be filled in as follows:

- IP: 192.168.10.100
- Port: 389
- BaseDN: dc=apc,dc=com
- UserRDN: ou=software
- Key attribute: cn
- Object class: person
- Full name attribute: sn

After the LDAP Authentication server has been added, the KVM ACCESS Administrator can use the Browse button to browse all the user names in the software directory.

Active Directory Settings Example

In this example the external server is Active Directory on Windows Server 2003 system. Its IP address is 192.168.10.100. Configure Active Directory in Windows Server 2003 as follows:

1. Open **Start > Control Panel > Administrative Tools > Active Directory Users and Computers > Domain > Users**.
2. The KVM ACCESS Administrator gets this information to use in the Adding an External Authentication Server procedure (see Active Directory, page 46).
   In this example, the fields are filled in as follows:
   - IP: 192.168.10.100
   - UserRDN: cn=users

After the Active Directory Authentication server has been added, the KVM ACCESS Administrator can use the Browse button to browse all the user names in the Users directory.

RADIUS Settings Example

In this example the external server is RADIUS: Microsoft IAS for Windows Server 2003. Its IP address is 10.0.0.100. Configure RADIUS as follows:

1. Open Start > Control Panel > Administrative Tools > Internet Authentication Services.
2. In the screen that comes up, right click on RADIUS Client.
3. Select New RADIUS Client.
4. In the screen that opens, enter the Friendly name. For example: KVM ACCESS-10.0.0.131, then click **Next**.
5. In this example, the KVM ACCESS's IP is 10.0.0.131. The Client-Vendor is RADIUS Standard. For the Shared secret, use **password**.
6. After clicking **OK**, you return to the Internet Authentication Services screen. In the left panel, click **Remote Access Policies**, in the main panel right click **Use Windows authentication for all users** and select Properties.
7. In the screen that opens, click the **Edit Profile** button, then select the Authorization tab.
8. In this example we use CHAP for encrypted authorization.

   The KVM ACCESS Administrator gets this information to use in the Adding and External Authentication Server procedure (see “RADIUS and TACACS+” on page 46).
   In this example, the fields would be filled in as follows:

   – IP: 10.0.0.100

   – Authentication type: CHAP

   – Shared secret: **password**

After the RADIUS Authentication server has been added, when the KVM ACCESS Administrator adds user accounts, he must use the names that were configured on the RADIUS server under Open Start > Control Panel > Administrative Tools > Computer Management > Local Users and Groups > Users for the Login names.

TACACS+ Settings Example

In this example the external server is TCACS+: Microsoft IAS for Windows Server 2003 (ClearBox). Its IP address is 10.0.0.100. Configure TCACS+ as follows:

1. Open Start > All Programs > ClearBox RADIUS TACACS+ Server > Server Manager.
2. In the screen that comes up, click **Connect**.
3. Enter the password that you set when you installed the ClearBox RADIUS TACACS+ Server.
4. In the ClearBox Server Configurator screen, select the Server Settings tab.
5. In this example, the TACACS+ service port is 49.
6. Open Start > All Programs > ClearBox RADIUS TACACS+ Server > Configurator.
7. In the screen that opens in the left panel, select **Realms > def**, then select the Authentication tab.
8. Click the **Allowed Protocols...** button.
9. In this example we use MS-CHAP for the allowed authentication protocol.
10. You are returned to the ClearBox Server Configurator screen. In the left panel select **Data Sources > users**.
11. In the main panel of the screen that opens, there is an MS Access entry field with a path specifying the general.mdb file. Accounts contained in this file are generated through MS Access.

    The KVM ACCESS Administrator gets this information to use in the Adding an External Authentication Server procedure (see “RADIUS and TACACS+” on page 46).
    In this example, the fields would be filled in as follows:

    – IP: 10.0.0.100

    – Port: 49

    – Authentication type: MSCHAP

    – Shared secret: the password that you set when you installed the ClearBox RADIUS TACACS+ Server

After the TACACS+ Authentication server has been added, when the KVM ACCESS Administrator adds user accounts, the names that were configured in the TACACS+ server's general.mdb file must be used.

NT Domain Settings Example

In this example the external server is Microsoft Windows NT Domain; its Server IP is QA_NT_SERVER. Configure NT Domain as follows: Open Start > Programs > Administrative Tools (Common) > User Manager for Domains to open a screen.

The KVM ACCESS Administrator gets the information to use in the Adding an External Authentication Server procedure. In this example, the fields would be filled in as follows: Server IP: QA_NT_SERVER

After the NT Domain server has been added, when the KVM ACCESS Administrator adds user accounts, he must use the names that were configured under User Manager for Domains.

LDAP Group Authorization Setting Examples

Example 1. In this example the external server is OpenLDAP on Windows Server 2003 as shown in the “LDAP/LDAPS - OpenLDAP Setting Example” on page 118.

1. Under the KVM ACCESS User Manager tab, select Authentication Services > Authentication Servers.
2. Select the OpenLDAP server, then click Group Authorization.
3. Click the Group has Member attribute radio button.
4. Click **Add** (at the top-right of the panel).
5. In this example add the **groups1** group.

The OpenLDAP administrator uses this name (**groups1** in the example) to create a group under OpenLDAP with the same name as the one just created on the KVM ACCESS server, as follows:

1. Open the core.schema file. The default settings we are interested in are as follows:

   attributetype (2.5.4.31 NAME 'member'

   DESC 'RFC2256: member of a group'

   SUP distinguishedName)

   objectclass (2.5.6.9 NAME 'groupOfNames'

   DESC 'RFC2256: a group of names (DNs)'

   SUP top STRUCTURAL

   MUST (member $ cn)

   MAY (businessCategory $ seeAlso $ owner $ ou $ o $ description))

2. Edit the kvmaccessldap.ldif file to add a definition for groups1 and have KVM ACCESS user accounts fall under **groups1**, as follows:

   dn: cn=groups1,ou=groups,dc=apc,dc=com

   objectclass: groupofnames

   member: cn=kvmaccess,ou=software,dc=apc,dc=com

   cn: groups1

   Note:1. The entry after dn: cn= should be the name of an actual group created under Group Authorization (see Group Authorization, page 72) on the KVM ACCESS server.
   2. The entry after objectclass: should be consistent with the name that was entered for the Object class when the group was created on the KVM ACCESS server. Change the default entry in this file to match.
   3. The entry after member: cn= should be an actual user login name.

3. You can check the group definition with LDAP Browser.
4. The above example has added a member, **kvmaccess**, to the **groups1** group. To add additional members to the group, edit the file to include them. For example:

   member: cn=kvmaccess-1,ou=software,dc=apc,dc=com

   member: cn=kvmaccess-2,ou=software,dc=apc,dc=com

Once these procedures are completed, KVM ACCESS users who are authenticated through the LDAP/LDAPS server, are authorized according to the permissions assigned to the group.

Example 2. By default OpenLDAP only supports the Group has Member attribute setting for the group related schema. This was the setting used in Example 1. An alternative setting used by other LDAP servers, User has Member Of attribute, is also supported under OpenLDAP by extending the schema.

In this example the external server is OpenLDAP on Windows Server 2003 as shown in the “LDAP/ LDAPS - OpenLDAP Setting Example” on page 118.

1. Under the KVM ACCESS User Manager tab, select Authentication Services > Authentication Servers.
2. Select the OpenLDAP server; then click **Group Authorization**.
3. Click the **User has Member Of attribute** radio button.
4. Click **Add** (at the top-right of the panel).
5. In this example add the **groups1** group.

The OpenLDAP administrator uses this name (**groups1** in the example) to create a group under OpenLDAP with the same name as the one just created on the KVM ACCESS server, as follows:

1. Open the core.schema file. Extend the schema as follows:

   attributetype (1.2.840.113556.1.2.102

   NAME 'memberof'

   DESC 'RFC2256: member of a group'

   SUP distinguishedName)

   objectclass (1.2.840.113556.1.5.9

   NAME 'person'

   SUP organizationalPerson

   STRUCTURAL

   MUST (cn)

   MAY (userPassword $ description $ sn $ mail $ memberof))

2. Edit the kvmaccessldap.ldif file to add a user account to the **groups1** group as follows:

   dn: cn=kvmaccesstest,ou=software,dc=apc,dc=com

   objectclass: top

   objectclass: person

   objectclass: organizationalPerson

   cn: kvmaccesstest

   sn: kvmaccesstest

   memberof: cn=groups1,ou=groups,dc=apc,dc=com

   userPassword: apc

Note: 1. The entry after dn: cn= should be an actual user login name.
2. The entry after objectclass: should be consistent with the name that was entered for NAME in the extended schema.
3. The entry after memberof: cn= should be the name of an actual group created under Group Authorization (see Group Authorization, page 72) on the KVM ACCESS server.

3. Check the group definition with LDAP Browser.
4. Repeat step 2 for each user account that you want to add to the group.

Once these procedures are completed, KVM ACCESS users who are authenticated through the LDAP/LDAPS server, are authorized according to the permissions assigned to the group.

Active Directory Group Authorization Setting Example

In this example the external server is Active Directory on Windows Server 2003 as shown in the “Active Directory Settings Example” on page 119.

1. Under the KVM ACCESS User Manager tab, select Authentication Services > Authentication Servers.
2. Select the Active Directory server, then click **Group Authorization**.
3. In this example add the KVMACCESSGP group.

The Active Directory administrator uses this name (KVMACCESSGP in our example) to create a group under Active Directory with the same name as the one just created on the KVM ACCESS server, as follows:

1. Open Start > Control Panel > Administrative Tools > Active Directory Users and Computers > Domain (CA-QA.com in our example).
2. In the left panel, right click Domain Controllers. Select **New**. Select **Group**.
3. In the dialog box that opens, enter the name of the group (KVMACCESSGP in our example).
4. In the right panel, right click KVMACCESSGP. Select **Properties**. Select **Members**.
5. Click **Add**.

The dialog box that opens lets you add members to the group. The members are selected from the accounts found in the Users folder (see the left panel of the original screen).

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 the APC Customer Support Center by telephone or e-mail.
  - Local, country-specific centers: go to **www.apc.com/support/contact** for contact information.

For information on how to obtain local customer support, contact the APC representative or other distributors from whom you purchased your APC product.