Simply Better Connections

CC2000

Centralized Management Software

User Manual

User Information

Online Registration

Be sure to register your product at our online support center:

International	http://eservice.aten.com

Telephone Support

For telephone support, call this number:

International	886-2-8692-6959
China	86-400-810-0-810
Japan	81-3-5615-5811
Korea	82-2-467-6789
North America	1-888-999-ATEN ext 4988 1-949-428-1111

User Notice

All information, documentation, and specifications contained in this manual are subject to change without prior notification by the manufacturer. The manufacturer makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties as to merchantability or fitness for any particular purpose. Any of the manufacturer's software described in this manual is sold or licensed *as is*. Should the programs prove defective following their purchase, the buyer (and not the manufacturer, its distributor, or its dealer), assumes the entire cost of all necessary servicing, repair and any incidental or consequential damages resulting from any defect in the software.

The manufacturer is not responsible for any damage incurred in the operation of this system if the correct operational voltage setting was not selected prior to operation. PLEASE VERIFY THAT THE VOLTAGE SETTING IS CORRECT BEFORE USE.

Package Contents

Check to make sure that all components are in working order. If you encounter any problem, please contact your dealer.

The CC2000 package consists of:

1 CC2000 USB License Key

1 software CD

Product Information

For information about all ATEN products and how they can help you connect without limits, visit ATEN on the Web or contact an ATEN Authorized Reseller. Visit ATEN on the Web for a list of locations and telephone numbers:

International	http://www.aten.com

Contents

*Chapter 3.*Web Console Overview

*Chapter 4.*Dashboard and Basic Operation

*Chapter 5.*Device Management

Chapter 6. User Management

*Chapter 7.*System

Chapter 9. Asset Management

Appendix A—Technical Information

Appendix B—The CC2000 Utility

Appendix C—Authentication Key Utility

Appendix D—External Authentication Services

Appendix E—SSO HTML Sample Codes

Appendix F—CC2000 MIB Reference

About this Manual

This manual is provided to help you get the most out of your CC2000 system. It covers all aspects of the software, including installation, configuration, and operation. An overview of the information found in the manual is provided below.

Chapter 1, Introduction, introduces you to the CC2000 System, with its purpose, features, and benefits described.

Chapter 2, Server Installation and Utilities, provides step-by-step instructions for installing the CC2000 on both a Windows and Linux system.

Chapter 3, Web Console Overview, explains how to log into the CC2000 with a browser, and describes how to use the CC2000's browser GUI interface.

Chapter 4, Dashboard and Basic Operation, explains the dashboard of the CC2000 server and goes over the basics of using the interface.

Chapter 5, Device Management, explains how to access, control, add, configure, and organize the devices that will be managed over the CC2000 network.

Chapter 6, User Management, describes how to add, modify, and delete user accounts; create user groups and assign users to them; specify device access rights for users and groups; and specify the user authentication method.

Chapter 7, System, provides an overview of the CC2000 organizational concept, and demonstrates how to deploy, configure, and manage the CC2000 primary and secondary servers on your installation.

Chapter 8, Logs, explains the CC2000's logging function and how to access, filter, and search the various logs that are kept by the CC2000.

Chapter 9, Asset Management, provides information on how to create 2D representations of the managed data centers that allow you to manage assets from a remote site.

***Appendix A Technical Information*,** provides technical as well as troubleshooting information.

Appendix B The CC2000 Utility, shows how to configure a number of the CC2000's parameters from the desktop of the computer that the CC2000 runs on, without having to invoke the browser GUI.

Appendix C Authentication Key Utility, describes how to access and update the information contained in the CC2000 Authentication Key.

Appendix D External Authentication Services, discusses the use of authentication via external third-party services. It also provides examples and configuration suggestions for setting up these authentication services.

Appendix E SSO HTML Sample Codes, provides sample codes for the Single Sign-On function.

Appendix F CC2000 MIB Reference , documents the MIB objects and SNMP traps supported by CC2000. It provides detailed information required for integration with network management systems, automated monitoring, and event handling.

Note:

- Read this manual thoroughly and follow the installation and operation procedures carefully to prevent any damage to the unit or connected devices.
- ATEN regularly updates its product documentation for new features and fixes. For an up-to-date CC2000 documentation, visit http://www.aten.com/global/en/

Conventions

This manual uses the following conventions:

Monospaced	Indicates text that you should key in.
[ ]	Indicates keys you should press. For example, [Enter] means to press the **Enter** key. If keys need to be chorded, they appear together in the same bracket with a plus sign between them: [Ctrl+Alt].
1.	Numbered lists represent procedures with sequential steps.
◆	Bullet lists provide information, but do not involve sequential steps.
>	Indicates selecting consecutive options (such as on a menu or dialog box). For example, Start > Run means to open the *Start* menu, and then select *Run*.
⚠	Indicates critical information.

Chapter 1
Introduction

Overview

ATEN's CC2000 Centralized Management Software provides IT Teams in every industry with a comprehensive solution that enables central management of their IT infrastructure locally and worldwide through a single portal. The software consolidates the management of all ATEN KVM over IP switches, serial console servers, ATEN PDUs and third-party devices such as embedded service processors, blade servers, and physical and virtual servers for in-band and out-of-band management. The brand new CC2000 provides an easy-to-use yet robust interface – making system management more efficient and productive.

Featuring concise and intuitive HTML 5-based web interface, the CC2000 delivers a better user experience and advanced usability. By utilizing consolidated data, task-based navigation, and simplified menus, administrators can access, configure, and manage all of the IT equipments with ease.

The CC2000 also features a consolidated portal, the Dashboard, to help IT staff quickly attain a full grasp of all the important information and to complete monitoring tasks with minimal effort and time. The Dashboard displays an at-a-glance overview of device status, device events, task results, online users, and licensed nodes usage. With the device status and device events sections, administrators can be immediately notified about the condition of the connected devices, as well as quickly receiving the generated critical logs. The task results section delivers vital messages about operation success or failure. Administrators can also view details of currently logged-in users and terminate suspicious user sessions. The Dashboard's enhanced notification functionality helps users to promptly handle issues and fix problems efficiently.

With the asset management functions, CC2000 enables users to quickly gain access to the specifications, appearance, installed location of the managed assets, providing complete control over floor space, rack space, IT equipment, power, and connectivity. Users can easily find assets with previously created tags and export all equipment details, simplifying the asset verification process. Featuring a floor map, CC2000 provides users the flexibility to observe the status of installed equipment from a location level down to the device level in both 2D and 3D images, facilitating comprehensive capacity planning and meticulous capacity management. It empowers users to assess,

optimize, and allocate resource, ensuring efficient utilization of infrastructure resources in alignment with organizational goals and requirements.

By integrating ATEN SN11XX series, PDU series, and Energy Box, the CC2000 supports real-time environment and power monitoring. This allows users to recognize potential hot spots in racks, , monitor power status of connected PDUs, and inspect other important info through the system dashboard, ensuring 24/7 availalbility of IP equipment.

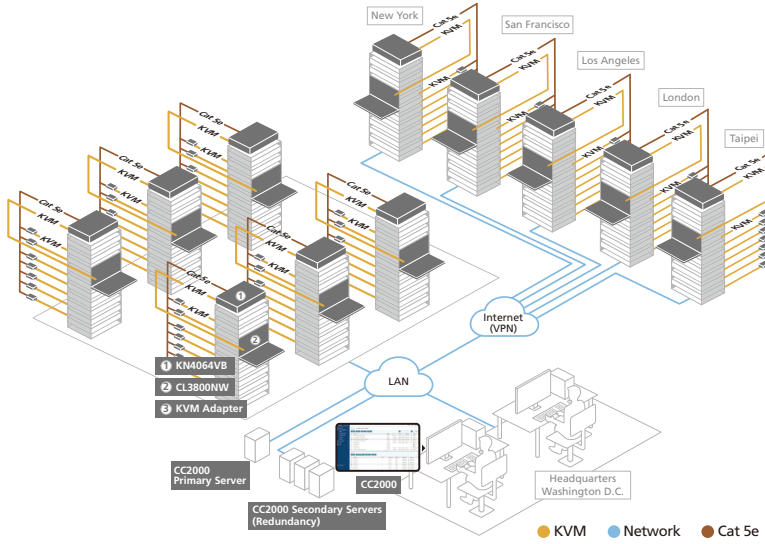
When monitored figures exceed their configured thresholds, users will get real-time alerts through Dashboard, message center, email, SNMP trap, and Syslog. IT administrators can get actionable insights about server room's temperature, humidity, air pressure, voltage, current, and power dissipation from the trend chart.

The CC2000's patented Panel DynaArray mode lets administrators view the output of multiple ports in individual panels on the same screen. The panel configuration can combine the ports from different over-IP KVM devices and give administrators a flexible choice to select which devices they wish to monitor and how the ports appear on the screen. Ports can be accessed and managed simply by clicking on the panel it is displayed in.

The CC2000 Centralized Management Software uses Primary-Secondary architecture to offer service redundancy. When the Primary CC2000 server goes down, the CC2000 management system will keep functioning since one of Secondary units can provide the required management services until the Primary unit is back online. This feature ensures that you are able to access all your devices whenever required.

With the help of the CC2000, users can promptly handle issues and fix problems efficiently. As a secure and centralized system management solution, the CC2000 software meets the requirements of IT administrators in centralized management and easy monitoring, putting them in complete control of their data centers, server rooms and branch offices wherever they are deployed.

Deployment Example:



Features

- Asset management – effortlessly view the specifications, appearance, location, and configuration of every asset in the data center, enabling users to improve the efficiency and reliability of data center operations.
- Visualized floor map – allows users to view the layout of server rooms and the configuration of server racks in 2D or 3D floor maps, providing insights on the overall the capacity and status of the infrastructure.
- Environment and power monitoring — monitors temperature, humidity, air pressure, voltage, current, power dissipation, water leakage and door entry for server rooms and data centers
- Real-time notification — for ensuring 24/7 availability of critical alerts, CC2000 notifies users when monitoring data exceed a user-configured threshold
- Trend charts and auditing — allow users to gain insight, analyze findings, and take strategic actions
- Single sign-on to consolidate the management of ATEN's KVM over IP switches, serial console servers, intelligent PDUs, and third party devices such as embedded service processors, and physical and virtual servers
- Intuitive User Interface with HTML5 to deliver friendly user experience
- At-a-glance Dashboard portal to display an overview of device status, device events, task results, online users, and licensed nodes usage
- Flexible remote access to service processors including Redfish (iDRAC8/iLO5), Dell iDRAC5/6/8, IBM RSA II, HP iLO2/3/5, Dell CMC, IBM AMM, HP OA, IPMI, IMM, or to IT equipment using RDP, VNC, SSH or Telnet IP tools
- Supports access and control to virtualized environment over VMware vSphere 6.0/6.5/6.7/7.0/8.0, Windows Server 2008, 2012 & 2016, or Citrix XenServer 6.5
- Supports management of APC PDUs (AP79xx, AP89xx, and AP86xx)
- Supports LDAP, AD, Kerberos, RADIUS and TACACS+ for centralized authentication and authorization ·
- Centralized role-based policy for user access privilege control
- Military level encryption (AES 256-bit) for secure end-to-end node access
- Access control to grant or restrict user access by IP or MAC address, and SAS 70 compliance for configurable failed login attempts and lockout
- Supports certificates signed from third-party authorities (CA)

- TLS v1.3 data encryption and RSA 2048-bit certificates to secure user logins from browser
- Supports strong user password policy to enhance the security of user accounts
- Consolidates logs from ATEN's KVM over IP switches, serial console servers, and other devices through syslog protocol for audit trail
- Universal virtual media support for easy software deployment (mount ISO image, boot, or upgrade the device remotely)
- Event notification support through Dashboard, message center, email, SNMP (v1, v2c, v3), and Syslog
- Task scheduling for backing up CC2000 database and configuration, exporting logs, and controlling power on/off on PDU devices
- Message Box — shows internal system messages or critical logs that can be viewed in full detail with just one simple click.
- Panel Array Mode – allows administrators to monitor multiple video outputs of remote servers in one screen
- Mouse DynaSync – automatically synchronizes the local and remote mouse cursors
- Delivers server redundancy through primary/secondary architecture for service availability
- Quick device access and management – go to **Recent** and **My Favorite** side menus to see and manage a list of recently visited and bookmarked devices, respectively
- Online Chat – Instant communication and collaboration between users (e.g. for quick problem troubleshoot)
- Supports MOTP (Mobile One Time Password) and two-factor authentication to provide an additional layer of protection against account hijacks.

Requirements

Server Requirements

Systems that the CC2000 server will be installed on should meet the following requirements:

- Hardware Requirements

	Small Installation (< 100 devices)	Medium or Large Installation (> 100 devices)
CPU	Intel Core i3 2+ GHz or above	Intel Core i5 3+ GHz or above
Memory	4 GB or above	8 GB or above
Hard Drive	20 GB or above	40 GB or above
Ethernet	At least 1 Ethernet adapter (100 Mbps or above) — Giga LAN recommended	

- Operating System Requirements

JRE 8	OpenJDK 8
Windows: ◆ Server 2019 ◆ Server 2016 ◆ Server 2012 ◆ Server 2008 ◆ 10 ◆ 8	Windows: ◆ Server 2019 x64 ◆ Server 2016 x64 ◆ 10 x32/x64
Linux ◆ Red Hat Enterprise Linux V. 4 ◆ Novell SUSE Enterprise Server 9 and 10 ◆ Ubuntu 15.10 x64 ◆ Ubuntu 15.10 x86 ◆ Debian 8.2 x64 ◆ Fedora 23 x64 ◆ Fedora 23 x86 ◆ OpenSUSE 13.1 x64 ◆ CentOS 7 x64	Linux ◆ Ubuntu 16.04 x64 ◆ Ubuntu 20.04 x64 ◆ Fedora 32 x64 ◆ Red Hat Enterprise 8.1 x64 ◆ CentOS 8.1 x64

Client Requirements

Hardware Requirements

- CPU: We recommend that the computers used to access the switch should have at least a Pentium 4 2GHz processor, with a 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 Web Start (JNLP) Viewer, the latest version of Java Runtime Environment (JRE) 8 or OpenJDK 8, with IcedTea-Web must be installed. To download IcedTea-Web, go to https://azul.com.
- At least 205MB of memory must be available for accessing the first viewer after logging in from the browser, and another 100MB for each additional viewer that is opened thereafter.

Operating Systems

- Supported operating systems for client workstations connecting to the CC2000 are listed below:

OS		Version
Windows		8 or later
Linux	Red Hat	7.1 or later
	Fedora	Core 2 or later
	SuSE	9.0 or later
	Mandriva (Mandrake)	9.0 or later
UNIX	AIX	4.3 or later
	FreeBSD	4.2 or later
	Sun	Solaris 8 or later

- Supported operating systems for CC2000 users include:
  - Windows 2000 or later
  - Platforms running OpenJDK 8
  - Platforms running Java Runtime Environment (JRE) 8

Browsers

Supported browsers for users logging into the CC2000 include the following:

Browser		Version
Edge		42 or later
Chrome		56 or later
Firefox	Windows	60 or later
	Linux	60 or later
	Sun	52 or later
Safari	Mac	10 or later
Opera		57 or later

Device Requirements

All ATEN KVM IP products must be at a firmware level that contains the CC Management function, and the CC Management function must be enabled. Download and install the latest version of the relevant firmware from our Website, if necessary. For details on upgrading the firmware, see *Update & Restore* on page 145.

Note:

- Devices must be configured to communicate on the same port that as the CC2000's Device Port (see *Device port*, page 15).
- For a list of supported devices, refer to the ATEN website.

Licenses

The CC2000 license controls the number of secondary servers and nodes permitted on the CC2000 server installation. License information is contained on the USB License Key that came with your CC2000 purchase.

Licensing Policy

- Upon completion of the CC2000 server software installation, a default license for one primary (no secondaries), and 16 nodes is automatically provided.
- To add anything more (secondary servers and nodes), you must upgrade the license. For detailed information, see *License* on page 244.
- A maintenance license is required for updating the system from v3.3 to v4.0 or later. With an expired maintenance license, the CC2000 can still operate normally. However, updates will be limited to minor fixes, for example, from v4.0.109 to v4.0.201.
- For more details on our licensing policy, please go to: https://eservice.aten.com/eServiceCx/Common/FAQ/view.do?id=19915&lang=en_US

Note:

- When an expired maintenance license is renewed, the passed period of time will also be counted toward the purchased period of time.
- To purchase or update a maintenance license, contact your local sales representative for more information.
- An order of two maintenance license (e.g. CCMA512, a license supporting up to 512 nodes) is an equivalent of a two-year license.
- To apply a renewed maintenance license to the CC2000 system, see *License* on page 244.

Nodes

- A node can either be an aggregate device or a physical port (e.g. KVM port on a KVM device, serial port on a Serial Console Server, or a sensor/ outlet port on a PDU). Each node requires a license.
  - Aggregate devices can be created when a device (router, server, Ethernet switch, etc.,) managed through the CC2000 is capable of being accessed through several ATEN device ports*. By consolidating

those ports into a single Aggregate Device, the Aggregate Device counts as a single node, and only requires a single license.

Note: Maximum of 2 KVM ports, 4 serial ports and 8 outlet ports.

- Ports on ATEN devices, when not part of an aggregate device, must be unlocked (see *Locking / Unlocking Devices*, page 124) 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.
- Group Devices do not count as nodes. They are made up of unlocked physical ports that are grouped together. The same physical port can be added to more than one Group device, but it only requires one node license no matter how many Group devices it is added to.
- Blade Server & Host VM: takes N+1 node license (N = number of Blades / Virtual Machines)

Note: See *By Devices - General Operations* on page 68 for detailed information on each of the device categories.

Secondaries

The license specifies how many secondaries you can register with the primary CC2000. See *CC2000 Secondary Servers*, page 25 for details on registering a Secondary with the Primary.

Chapter 2
Server Installation and Utilities

Overview

Recognizing the increasing prominence of Linux systems in server environments, the CC2000 Centralized Management Software system has made its management services available on both Windows and Linux platforms. This chapter describes how to install the CC2000 server on each.

Windows Version Installation

Before You Begin

Before installing, make sure OpenJDK 8 or Sun's Java Runtime Environment (JRE) 8 has been installed on your system. If not, download and install it first.

You can find the latest version of JRE here:

```
http://java.com
```

You can find the latest version of OpenJDK here:

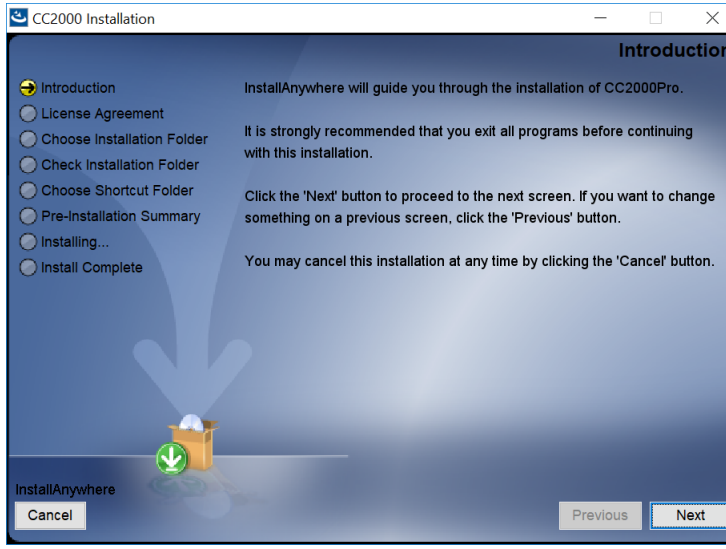
```
http://www.azul.com/
```

After OpenJDK or JRE has been installed on your system, you can start installing the CC2000 program.

Starting the Installation

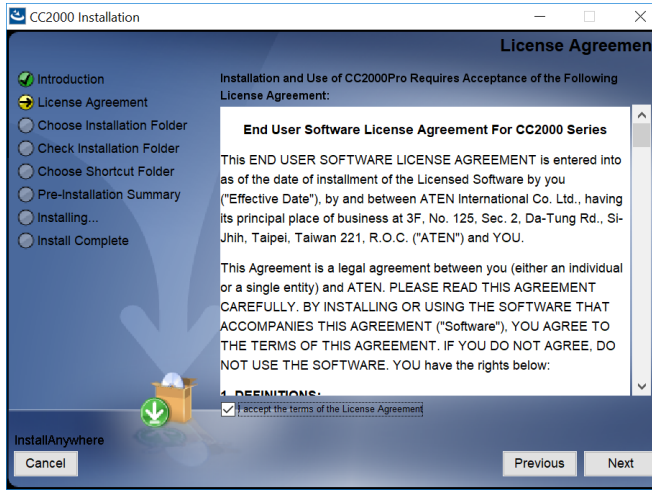
To install CC2000 on a Windows system, do the following:

1. Put the software CD that came with your package into the computer's CD or DVD drive.
2. Go to the folder where the installation file (e.g. *CC2000_Setup_V3.0.0_ForWindows.exe*) is located and execute it. The installer will appear as shown below:

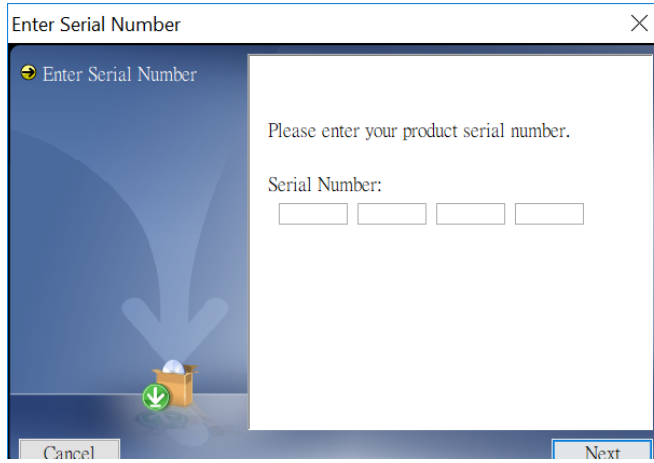


Click **Next** to continue.

3. The installer will display the License Agreement. Read it and should you accept, click to check *I accept the terms of the License Agreement*. Click *Next* to continue.



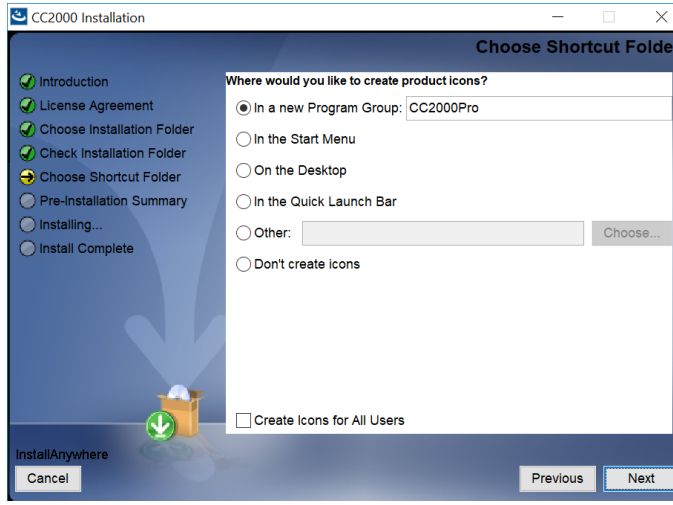
4. The installer will prompt you to enter a serial number. Key in the CC2000's software serial number (the serial number can be found on the CD case) and click *Next* to continue.



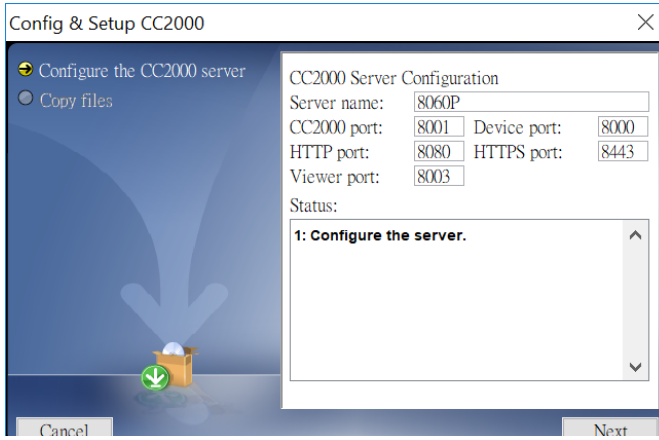
Note: We recommend that you save your software serial number in a safe place in case you need to use it for re-installation.

5. The installer will bring you to the *Choose Installation Folder* page and ask you to specify the CC2000's installation directory. If you don't want to use the default entry, click **Choose...** to browse and select a location. Click *Next* to continue.

6. In the *Choose Shortcut Folder* dialog box, click the radio buttons to specify where you would like to create software shortcuts. Click *Next* to continue.



7. In the Configuration dialog box, fill in the fields according to the information provided in the table below.



Heading	Explanation
Server name	The dialog box presents the default name of the server – as defined in the Windows *Computer Name* setting. You can define a name to identify the server on the CC2000 installation, if you wish. The name can be of 2–32 bytes in any supported language. **Note:** 1. The following characters may not be used: **" ' ** 2. This name is only for CC2000 server purposes – it doesn't change the actual computer name.
CC2000 port	The port that the CC2000 server uses to communicate with other CC2000 servers. The default is 8001. **Note:** 1. This is the **CC2000 Port** referred to on the *Redundant Servers* web page (see *Redundant Servers*, page 269). 2. Although each CC2000 server on the system can use its own port setting, for ease of management, we recommend that all CC2000 servers use the same port setting.
Device port	The CC2000 server uses this port to communicate with the connected devices (ATEN/Altusen IP products) on the installation. The default is **8000**. Each CC2000 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 CC2000 server uses for web communication. The default is 8080. If you use a different port, users must specify the port number in the URL of their browsers.

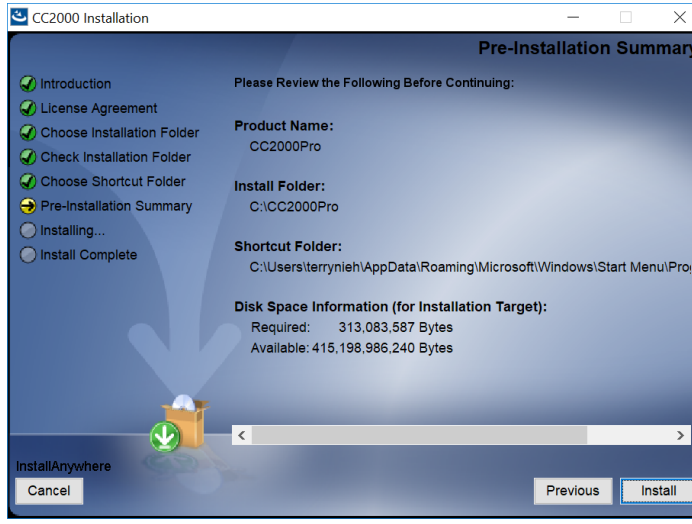
Heading	Explanation
HTTPS port	The port that the CC2000 server uses for secure web communication. The default is 8443. If you use a different port, users must specify the port number in the URL of their browsers.
Viewer Port	The default is 8003.

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

Note: You can still change any of these settings following the installation. See *System Info*, page 215, for details.

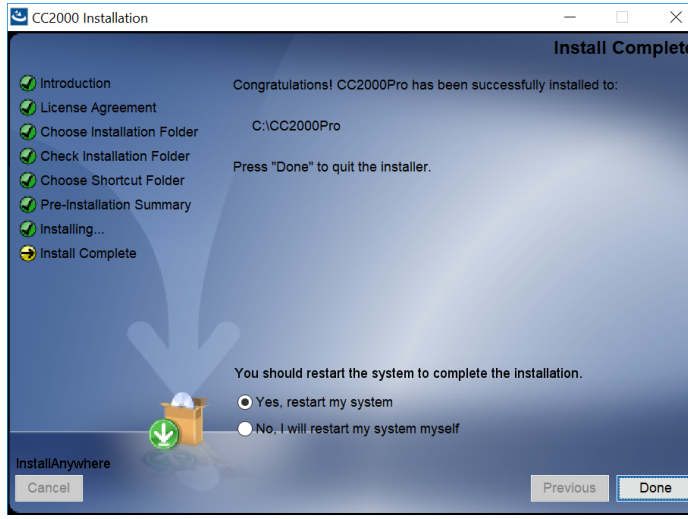
9. The dialog box changes to inform you that files are being copied to the installation folder. Once the files have been copied, click *Continue* to move on.

10. The *Pre-Installation Summary* screen appears:

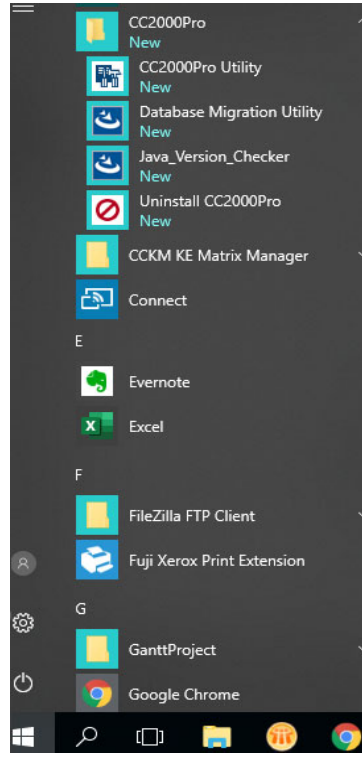


If you wish to change anything, click *Previous* to go back, If the information is correct, click *Install*.

11. When completed, the installer will ask you whether to restart the system to complete the installation or not. Click **Done** to exit the installer and restart the system. Choose *No, I will restart my system later* if you do not wish to restart your system.



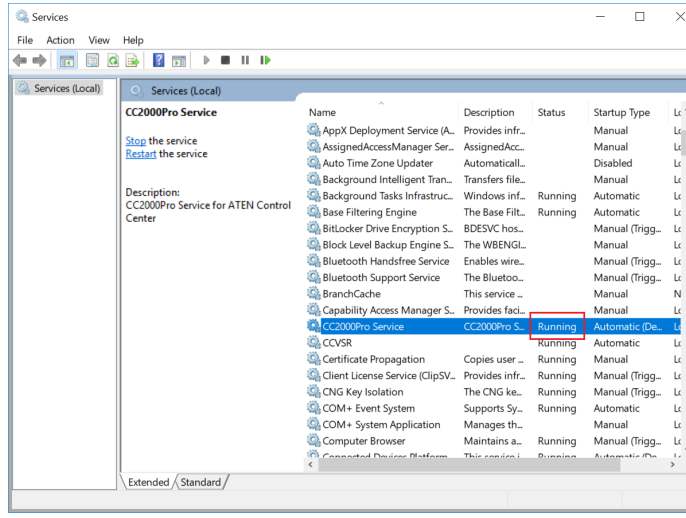
12. A CC2000Pro entry is created in the Windows *Start* menu.



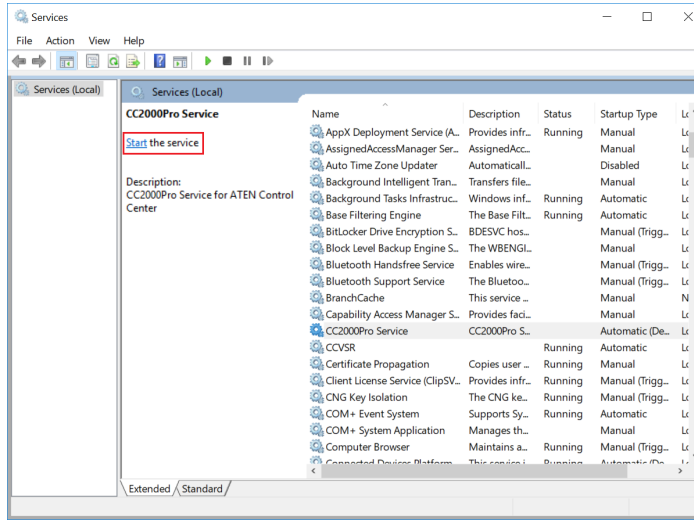
Post-installation Check

After the installation, the CC2000 program starts automatically (and starts automatically upon Windows startup).

To check that the CC2000 has started, go to the Services desktop app and see if *Running* is shown under the Status column.



If *Running* is not shown, you can click *Start* to start the service.



Linux Version Installation

Before you Begin

The procedure for installing CC2000 on a Linux system is similar to that of Windows, but with Java considerations to take note of before starting.

- If Java isn't already installed on your system, you will need to download it from the Java web site:

  ```
  http://java.com
  ```

  Installation instructions are provided on the Java download page.

- CC2000 program requires the system to run OpenJDK 8 or JRE 8. Some Linux distributions may have different versions of JRE installed. To find out your Java version, open a terminal and enter the following:

  ```
  java -version
  ```

IMPORTANT: Both the OpenJDK and CC2000 must be installed using the Linux's root user, otherwise certain functions may not work properly.

  If the version displayed does not fit the system requirement, please make sure you have OpenJDK 8 or JRE version 8 installed. (See the previous point regarding downloading and installing Java.)

- Make sure your 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
  ```

- Even after you install an appropriate Java version and set the new PATH and JAVA_HOME environment variables, the distribution may still not recognize the new version and continue to use its original version of Java. If this problem occurs, correct it by doing the following:

  1. Copy the CC2000*Setup_Linux.bin* file from the distribution CD to a folder on your hard disk.
  2. Open a terminal and go to the directory where the CC2000*Setup_Linux.bin* file is located.
  3. Enter the following commands:

     ```
     export LAX_DEBUG=1
     sh CC2000-Setup-ForLinux.bin
     ```

Note: If the installation program starts, cancel it.

4. In the screen output, look for the line (it will be in bold) that starts with:

   ```
   Using VM.........
   ```

   to see which Java your distribution is defaulting to.

5. If the *Using VM* entry shows a path to a file named *java* in the old Java version directory, go to that directory and either delete the *java* file or rename it.

6. Log out and log back in.

Installing

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

1. Put the software CD that came with your package into the computer's CD or DVD drive.

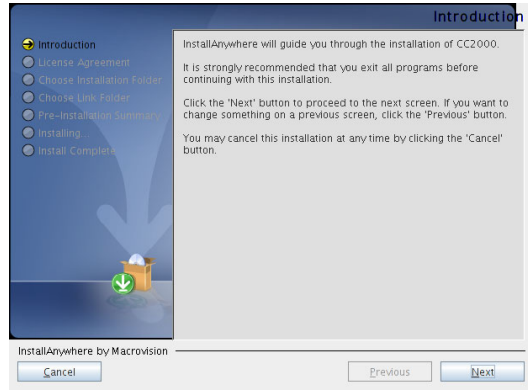
2. Go to the folder where the installation file (e.g. *CC2000_Setup_V3.0.0_ForLinux.exe*) is located and execute it.

IMPORTANT: Both the OpenJDK and CC2000 must be installed using the Linux's root user, otherwise certain functions may not work properly.

Note: 1. Make sure that the installation file has executable permissions

2. For some versions of Linux, the program must be run in a terminal.

A screen, similar to the one below, appears:



Click **Next** to move on.

3. From here, the installation procedure is the same as that of Windows. Refer to the Windows installation procedure (see page 11) for details.

Post-installation Check

- After the installation completes successfully, the CC2000 program starts automatically (and starts automatically upon every startup).

  To check if the CC2000 has started, or to start, stop, or restart the service, issue the following commands (as root) from a terminal console.

Purpose	Command
To start the service	/root/CC20000pro start#
To stop the service	/root/CC20000pro stop#t
To restart the service	/root/CC20000pro restart#
To check the service status	/root/CC20000pro status#

  If the above commands fail, try commands that use legacy paths:

Purpose	Command (Legacy Path)
To start the service	/etc/init.d/cc2000service start#
To stop the service	/etc/init.d/cc2000service stop#t
To restart the service	/etc/init.d/cc2000service restart#
To check the service status	/etc/init.d/cc2000service status#

- To check on the Java version your system is running, do the following:
  1. Open the *Start* menu.
  2. Navigate to the CC2000 entry (Programs → CC2000), and select **Java Version Checker**.

Post-Installation Setup

The CC2000 software comes with a default demo license that allows the server to be a primary server with no secondaries and 16 nodes (all of which must be on the same network as the server). For anything beyond this minimum, you will need a purchased license key that allows secondary servers and additional nodes.

Once the software is installed on the server, the next step is to specify whether the server will be a Primary or Secondary.

- If this server is going to be a Primary, insert the CC2000's USB license key into a USB port; log into the server (see *Logging In*, page 30); go to the *License* page, and click **Upgrade** (see *To update the license, contact your dealer to purchase a license key for the number of Secondaries and nodes desired. After receiving your purchased USB license key, you can update the license of the CC2000 through one of the two following methods:* on page 245, for details). The number of Secondaries and nodes allowed depends on your license key purchase.

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

- If this installation is going to be a secondary server, there is no need to insert a license key – you simply need to register it with the primary. See *View Properties* on page 270, for details.

Uninstalling the CC2000

Uninstalling from a Windows System

To uninstall the CC2000 from a Windows system, do the following:

1. Open the *Start* menu.
2. Navigate to the CC2000Pro entry (Programs → CC2000Pro), and select *Uninstall* CC2000*Pro*.

Note: The removal program does not remove a number of the CC2000 files and folders that were created during operation. For a complete removal (necessary if you plan on reinstalling), you must remove them yourself from the location that the CC2000 was installed at (the default folder is C:\CC2000Pro).

Uninstalling from a Linux System

To uninstall the CC2000 from a Linux system, as root, execute the following command:

```
/install-path/Uninstall_CC2000Pro/Uninstall_CC2000Pro
```

Where */install-path/* represents the path and directory that you specified for the CC2000's location during installation.

Note: The removal program does not remove a number of the CC2000 files and folders that were created during installation. For a complete removal (necessary if you plan on reinstalling), you must remove them yourself. The default is /home/CC2000Pro.

Updating the CC2000

To update CC2000 from v3.0 to v4.0 or later, follow the steps below.

1. Purchase a maintenance license and upgrade the USB key.
   For more information, see *Key License Upgrade*, page 382.
2. Apply the license to CC2000 v3.x using one of the following methods:
   - *Upgrade License with USB Key* (page 246)
   - *Upgrade License with License File* (page 247)
3. Update CC2000 v3.x to v4.0 using the CC2000-Upgrade program:
   - CC2000Upgrade_Win.exe (for Windows)
   - CC2000Upgrade_Linux.bin (for Linux)

Note: When you update, you must update the primary and each of the secondaries.

New versions of the Upgrade Program are put on our website for download as they become available. Check the website to get the most up-to-date version.

Preliminary Steps

These steps make sure that the installation database is indeed most up-to-date across all of the CC2000 servers. Should a problem occur after the update, you can use the backup to restore the database to its latest working level.

We recommend you take the following backup steps on each CC2000 server before you begin.

1. Replicate the database of each of the secondaries; use *Run Now* for the schedule setting (See *Replicate Database* on page 266).
2. After replication completes; go back and set the schedule to a time that will not take place during the update time (next week, next month, etc.).
3. On the primary unit, do a Database Backup.

Once you have finished these preliminary steps, you can update the primary and each of the secondaries. When you run the upgrade program, simply follow the Installation Wizard to complete the procedure.

CC2000 Secondary Servers

A complete CC2000 installation can comprise of 1 Primary and up to 31 secondary servers, located anywhere throughout the world. The primary server is automated to be designated at the server where you updated the license of your CC2000 software. See *License*, page 244, for details.

Once the primary server has been set, you can then register each of the other CC2000 server as a Secondary with the *Register* function. See *View Properties*, page 270, for details.

CC2000 Redundant Secondary Servers

To provide CC2000 server redundancy, at least a secondary CC2000 server must be installed.

Should the primary server fail (due to network failure, CC2000 failure, etc.), one of the secondary servers will act as the deputy primary server, maintaining the connected devices and normal operation. However, administrators will not be able to configure any of the settings until a primary server is present (fixed or newly assigned).

Refer to *Redundant Servers* on page 269 on how you can appoint one of the secondary servers as the redundant server.

Database Migration Utility

For system updates from version 2.8 to version 3.2 or any later version, use database migration utility to migrate your system database. For system updates from version 3.2 to any later version, the server will automatically migrate the database. The database migration utility is a pure Java utility and can be used on Windows and Linux systems.

Before you begin

Make sure the CC2000 server you are trying to *migrate from* is version 2.8.271 (or later). If not, download the update file from the "CC2000 3.0" product page on the ATEN website and install it.

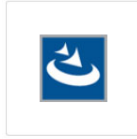
Make sure the CC2000 server you are trying to migrate to is version 3.2.312 (or later). If not, download the update file from the CC2000 3.0 product page on the ATEN website and install it.

Note: To update the CC2000 server from v2.x to v2.8, download the installer from ATEN eSupport or contact ATEN Tech Support for further assistance.

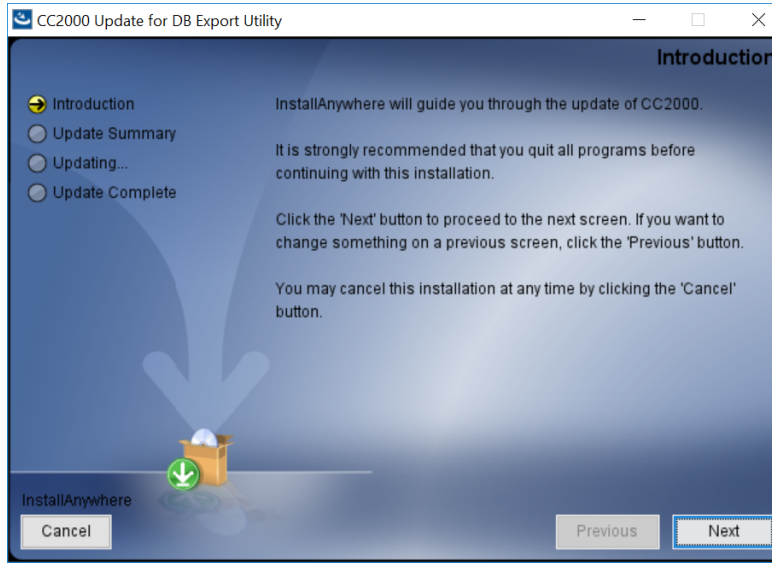
Migrating the System Database

Follow the procedures below to migrate the database:

1. On the computer running CC2000 v2.8, download the DB Migration Utility installer from the "CC2000 v3.0" product page on the ATEN website.

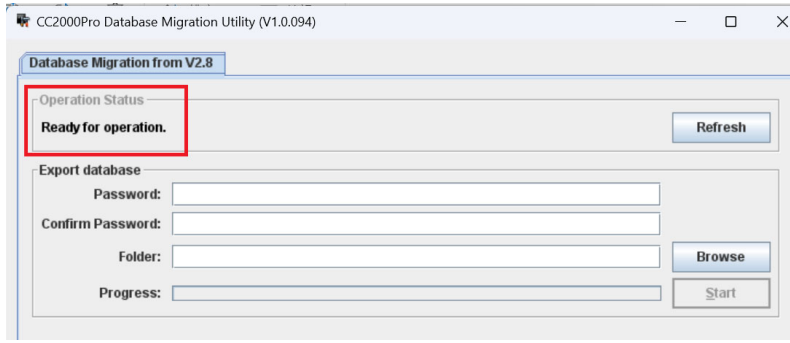


2. Run the installer and follow the on-screen instructions.



3. Use DB Migration Utility to export the system database.

Note: Make sure CC2000 v2.8 is running, with the **Operation Status** appear connected. If not, click **Refresh** to refresh the status.



a) Enter the password, and click **Browse** to select a destination folder.

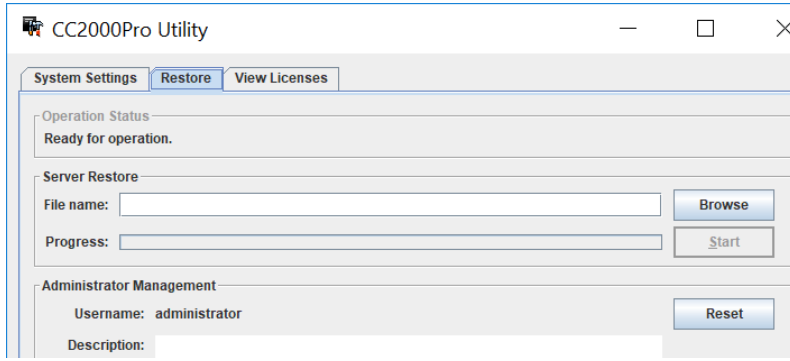
b) Click **Start** to begin the export. A database backup file (*.cbk) and a log file (*.log) appear in the destination folder.

4. After the export process, stop the CC2000 v2.8 server.

5. Copy the *.cbk file to the computer running the CC2000 v3.2 (or a later version).

Note: Make sure that this server is a primary server and that it is running.

6. Launch the CC2000Pro utility and go to the **Restore** tab.



c) Click **Browse** and select the *.cbk file. The utility prompts you to enter the password.

d) Enter the password and click **Start** to begin the import (restore) process.

7. After the import process:
   - Log into the CC2000 v3.2 (or a later version) server to check:
     - the export log file to see the affected items (authentication server, user type, user account, notifications, etc.)
     - the device connection settings (CC management settings, server IP, device port, etc.).
   - Find the secondary CC2000 servers originally on the CC2000 v2.8 server and re-register them to the primary CC2000 v3.2 server.

Notes About the Migration

- User Types: Some user types are remapped and user-created user types will be renamed without any roles. Review and reconfigure where necessary.
- Folder: All folders will be removed during the migration and the devices under these folders will be moved to the device root.
- Events: Some events have been changed or removed in CC2000 v3.2and related events will also be changed or deleted. The corresponding logs will be kept and available for display.
- Notifications: Some event types have been removed in CC2000 v3.2 and their notifications will also be removed.
- Detached Devices: This function is not supported in CC2000 v3.2 or any later versions and will be removed during the migration.
- Maintenance setting: Due to setting range changes, some maintenance settings (log options, device log options, serial console history options and SNMP trap options) may be changed, refer to the corresponding section for the updated ranges.

Chapter 3
Web Console Overview

To ensure multi-platform operability, access to the CC2000 is available through most standard web browsers and supports several authentication methods. This chapter provides details on the login procedures and an overview of the CC2000 web console.

Logging In

CC2000 accounts require only a username and password for login. To improve security, consider implementing additional authentication methods. For full information, see *Authentication Services*, page 191.

Logins through Account Credentials

To log in the CC2000 web console using account credentials (username and password), follow the steps below.

1. Open a browser and specify the IP address of the CC2000 in the browser's URL location bar.

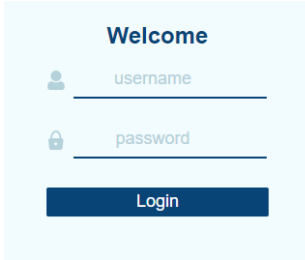
   If you created a shortcut on the desktop, opening the shortcut will bring you to the URL on your default browser.

   Note: If the system administrator has configured the HTTP or HTTPS port setting as something other than the default ports 8080 and 8443, you must include **http://** or **https://** before the IP address, and specify the port number along with the IP address. For example:

   ```
   https://192.168.1.20:8443
   ```

   Where *8443* is the https port number, with a colon separating it and the IP address.

2. If any Security Alert dialog boxes appear, accept the certificate – it can be trusted. See *Trusted Certificates*, page 359 for details. After a moment, the Login page appears:

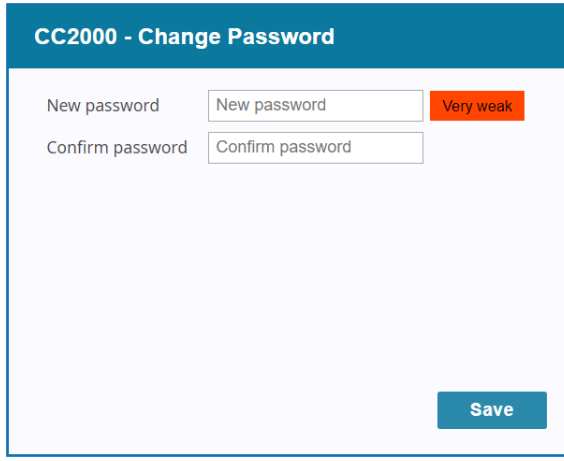


Note: If you are using MOTP authentication or Dual authentication, refer to *Logins through MOTP Authentication* and *Logins through Dual Authentication*.

3. Enter your CC2000 username and password, and then click **Login**.

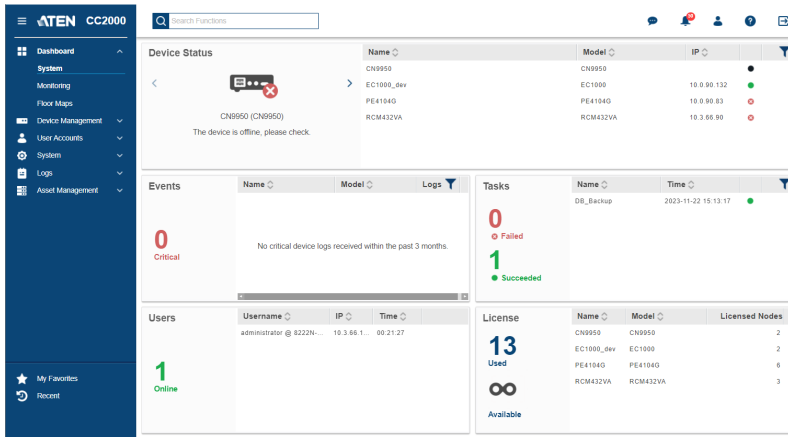
Note: The administrator account's default username is "administrator" with the default password being "password".

The system immediately prompts you to change the login password.



4. Enter a new password, confirm the password again in the next field, and click **Save**. A maximum of 32 English alphanumeric characters is allowed.

   The system will bring you to the Dashboard.



Logins through MOTP Authentication

If you have chosen to use MOTP authentication, the login page only requires you to enter the username. Upon entering your username, a MOTP authentication dialog window appears. Follow the on-screen instructions to log in via MTOP authentication.

For more information on the different types of MOTP authentication, refer to *Two Factor* on page 201.

Logins through Dual Authentication

If you have chosen to use Dual Authentication, you will need to enter the username and password of a CC2000 user, followed by the MOTP authentication.

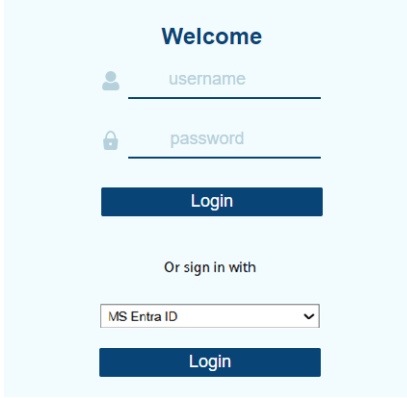
For information related to MOTP or Dual authentication, refer to the MOTP or Dual authentication sections in *Authentication Services* on page 191.

Logins through Single Sign-On (SSO)

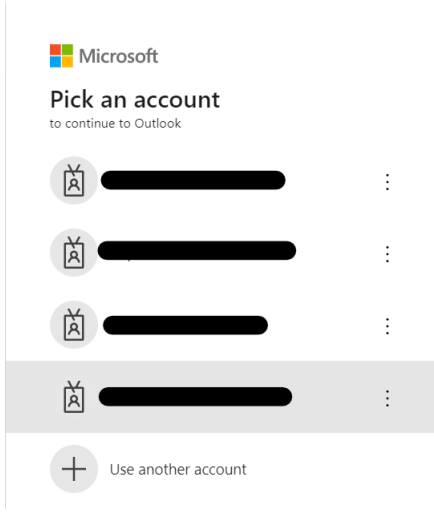
Logins through SSO require a series of configuration on Entra ID and CC2000. For a suggested procedure, see *Single Sign-On Using Microsoft Entra ID*, page 202.

To log in an account via SSO:

1. In a web browser, enter the URL of the CC2000 web console. This screen appears.

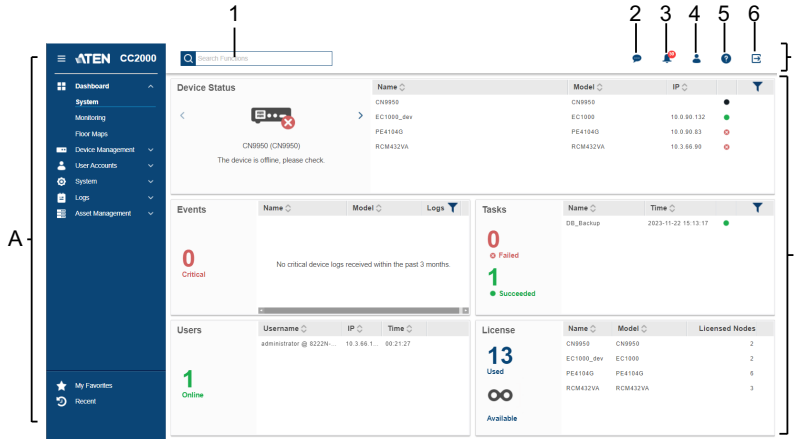


2. From the drop-down menu, select the Entra ID service and click **Login**.
3. Select an account or click **Use another account** to log in. The account can be a standalone user or a user that belongs to a group.



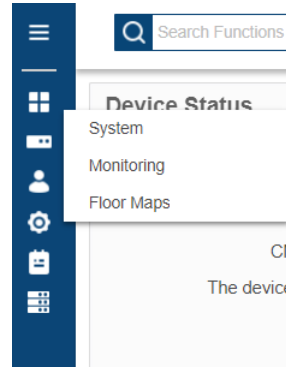
The Interface

The general interface of CC2000 and its components (sections and items) are shown below:



Screen Components

The screen components are described in the table below:

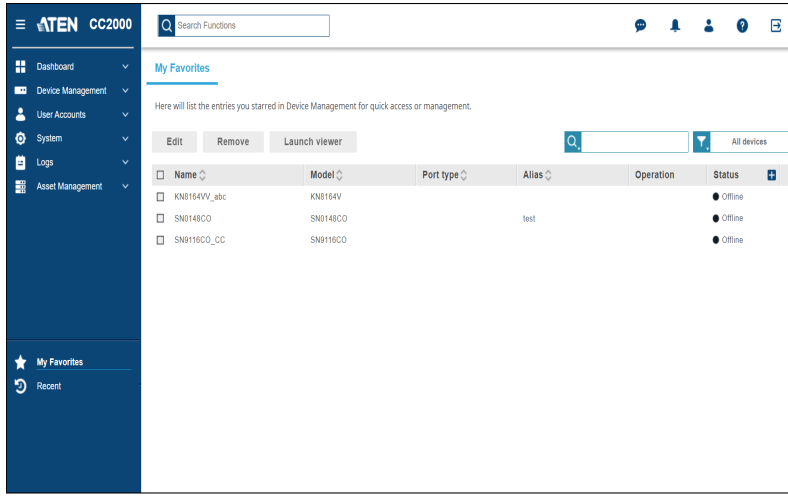
No.	Item	Description
A	Sidebar Menu Section	◆ The sidebar menu section is the main selection menu. Click to select the menu you wish to view/configure. Clicking the menu may expand submenus for further configurations. ◆ To collapse the menu, click ≡. The sidebar menu becomes collapsed as illustrated:  With a collapsed menu, click on any of the icons to open its submenu. For example: 
B	Task Bar Section	The task bar section contains function search, notifications, personal settings (language & password), help and logout.
C	Interactive Display Panel Section	This section is your main work area. The screens that appear reflect your menu choices and submenu item selection. The use of this panel is discussed later in this chapter.

No.	Item	Description
1	Function Search	You can use this item to search for functions in the CC2000 browser GUI. For example, if you wish to find “SNMP”, enter it into the search bar. All the SNMP related functions will be displayed (shown below). Click the desired search result and CC2000 will bring you to the function’s configuration. 
2	Online Chat	Clicking this icon will bring up a chat window. Refer to *Chat* on page 43 for more information.
3	Notification	If there are notifications, the bell icon will have a number displayed on it. The information displayed here will depend on the user’s permission. Clicking this icon will display the 50 newest notifications. These include, from newest to the oldest, critical logs, warning logs and system messages. Click *Clean all* to clear all notifications. Click *View logs* to go to System Logs (see *System Logs*, page 277). Click *View message box* to open message box window. Refer to see *Message Box*, page 39 on how to use message box.
4	Personal	Clicking this icon to see or access the following settings: ◆ The username of this session ◆ The time the user last logged in ◆ User preferences Click this option to change the interface language or to resume to the previous logout status. ◆ Change password ◆ Two-factor authentication
5	About	Clicking this icon to view CC2000 information. Click *Help* for the CC2000 user manual. Click *About* for information of your CC2000.
6	Logout	Click this icon to log out of your CC2000 session.

My Favorites

The *My Favorites* page is similar to bookmarks. Devices and ports that you frequently access can be marked as favorites and you can come to this page to quickly access them. Simply open this page and select the device/port instead of hunting for devices and ports in the *Devices* submenu. This feature is especially handy on large, crowded installations.

Clicking **My Favorites** will bring you to the page shown below:

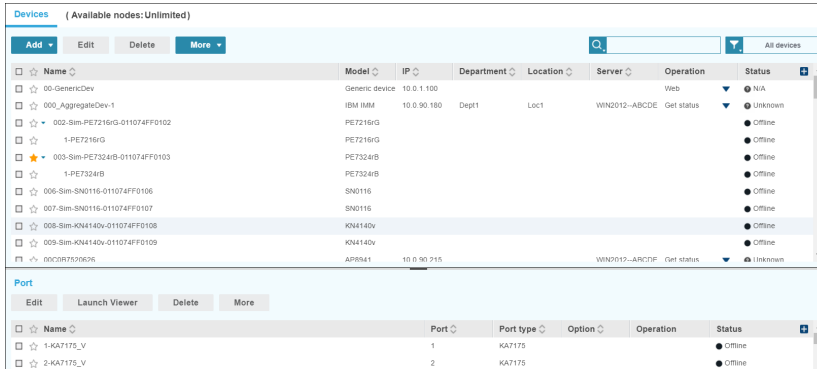


Note: Editing and operations are the same as those in the Devices submenu. Refer to *By Devices - General Operations* on page 68 for more information.

Add Favorites

Follow the steps below to add a favorite.

1. Go to the Devices submenu (**Device management** > **Devices**).



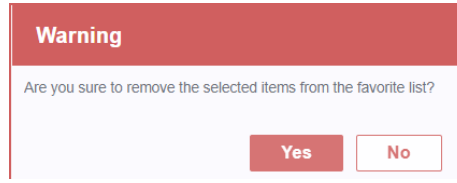
2. Find the device/port you wish to add to My Favorites in the device/port list.

3. A star icon ☆ should be visible on the left of the device/port name, click it.

4. The star icon will change to an orange star ★ to indicate you have successfully added the device/port to My Favorites.

Remove Favorites

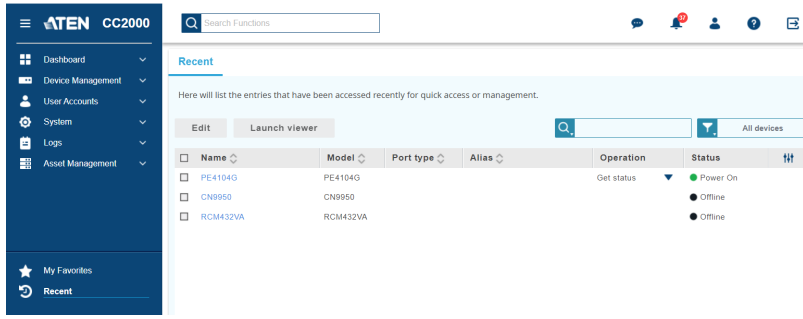
To remove a device/port from My Favorites, check the check box of the device/port and click **Remove**. The system will ask if you would like to remove the device/port, click **Yes** to continue.



Recent

The *Recent* page is similar to history. Devices and ports that you have previously accessed are listed here (up to 100 recent devices/ports) and you can come to this page to quickly access them. Simply open this page and select the device/port instead of hunting for devices and ports in the *Devices* submenu. This feature is especially handy on large, crowded installations.

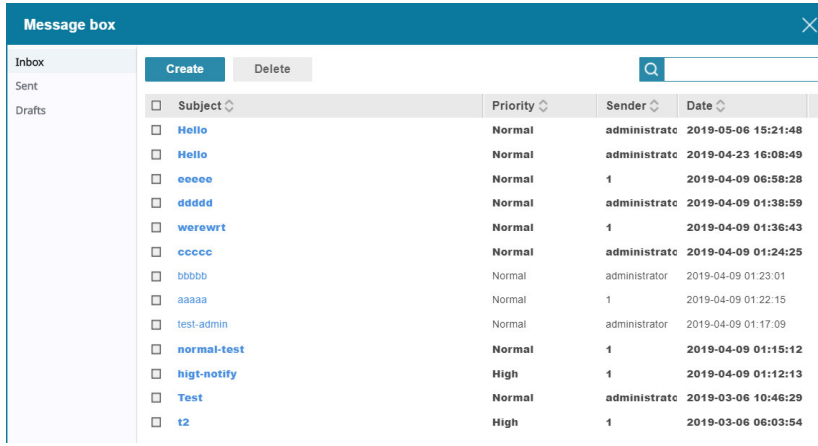
Clicking **Recent** will bring you to the page shown below:



Note: Editing and operations are the same as those in the Devices submenu. Refer to *By Devices - General Operations* on page 68 for more information.

Message Box

Go to the Message Box by clicking the notification icon followed by **View message box**.



Note: The Sent and Draft options are Administrator-only function.

You can select **Inbox**, **Sent** or **Drafts** folders to respectively find incoming messages, messages you have sent, or unsent messages.

Use the search option on the upper-right corner to filter the messages.

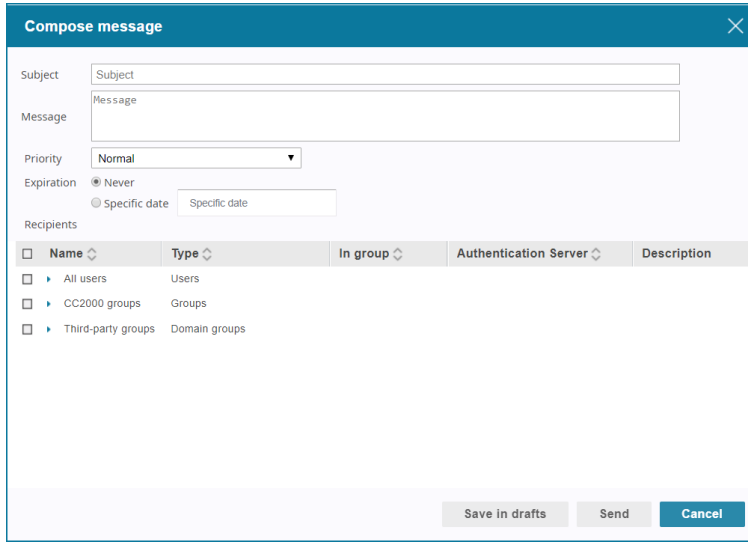
Click the column headings to sort the order of display.

Inbox

■ Create Notification

Follow the steps below to create a notification:

1. Click **Create** for the following pop-up window:

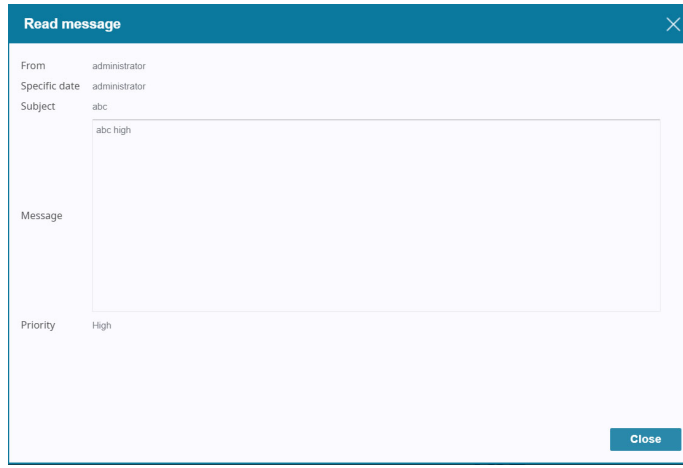


2. Fill in the **Subject** and **Message** fields.
3. Select a priority type using the **Priority** drop-down menu.
4. Select the **Expiration** option: Never or Specific date. Set the date for the system message to expire if Specific date is selected.
5. Select the **Recipients** by checking the check box(es). You can expand recipients in the Name column by clicking the arrowhead to select individual users.

6. Click **Save in drafts** or **Send**.

   Messages are respectively copied into the Drafts or Sent items folder in the sidebar.

Note: 1. High priority messages appear on the first page when a user logs in as shown below:



2. Normal priority messages will appear with a notification in the Notification icon as shown below:

■ Delete Notification

To delete a notification(s), check the check box(es) of the notification(s) and click **Delete**. A confirmation message will be shown, click **Yes** to confirm.

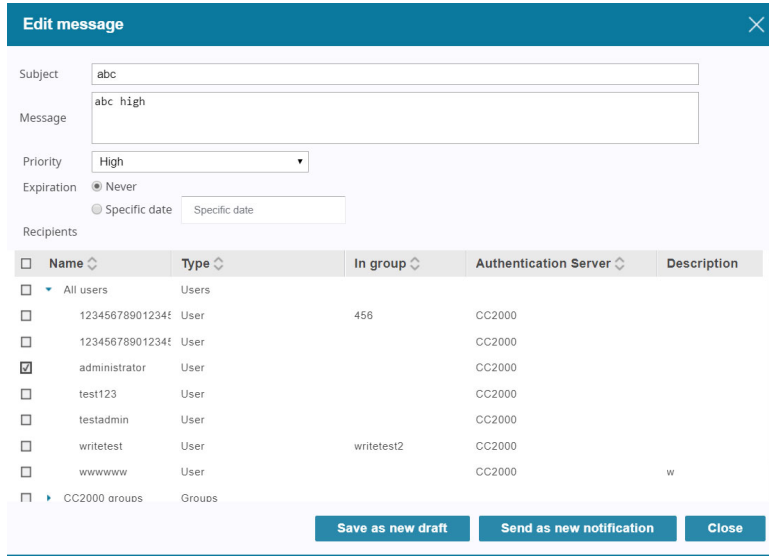
Sent

Clicking this folder allows you to edit and delete sent notifications.

■ Edit Sent Notification

Follow the steps below to edit a notification:

1. Check the check box of the notification and click **Edit**.



2. Make your desired changes and click **Save as new draft** or **Send as new notification**.

■ Delete Sent Notification

To delete a sent notification(s), check the check box(es) and click **Delete**. A confirmation message will be shown, click **Yes** to confirm.

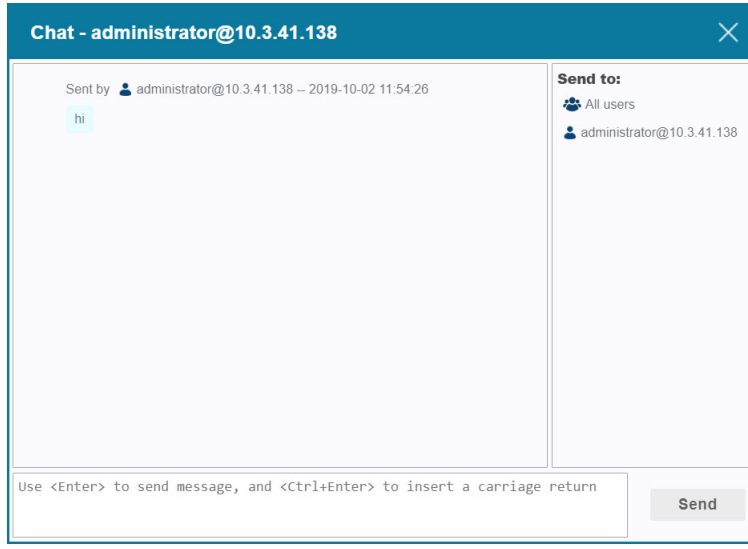
Drafts

Clicking this folder allows you to edit and delete unsent notifications.

Note: The Edit and Delete options works similar to the ones described in the Sent folder. Refer back to page 41 where necessary.

Chat

Click the chat icon to bring up the Chat panel. An example is shown below:



Send to lists the users currently online. Click to select the user you wish to send the chat to. You can select multiple users, or click “All users” to send to all. The selected user(s) will be highlighted.

Click the X icon (top right) of the panel to exit the Chat function.

Chapter 4
Dashboard and Basic Operation

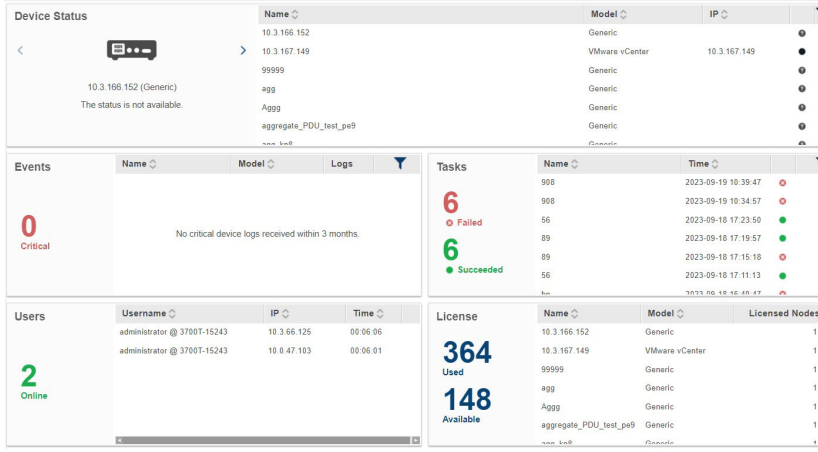
Overview

Dashboard provides a visual summary of the system and monitored ports and equipment. It provides an overview of the current system status and draws your attention to critical events that need intervention. For more information, refer to the following sections.

- System Dashboard (page 44)
- Monitoring Dashboard (page 48)
- Floor Maps Dashboard (page 54)

System Dashboard

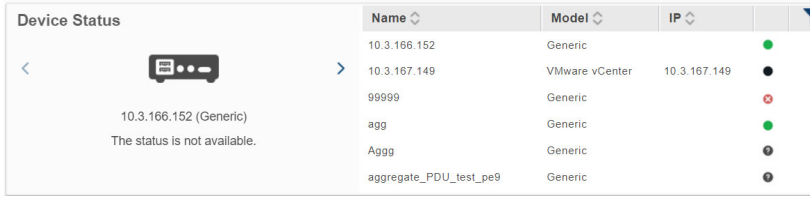
The system dashboard page displays status overview regarding added devices, events and tasks executed, online users, and license usage.



Note: Dashboard page access is only for Super Administrators and System Administrators.

Device Status

The Device Status panel lists and displays the status of all added devices. Those that may require intervention, for example, devices that are detected with abnormality or are offline, are shown on the left of the panel, as illustrated below:



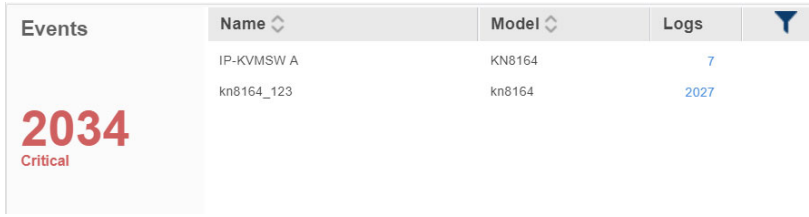
- To check out devices that are detected with abnormality, unknown status, or are offline, click the left or right arrow on the left of the Device Status panel to cycle through these devices.

Note: If the environment information is turned on for KN and SN devices, abnormal temperature or fan operation will also be displayed here.

- To filter the displayed entries by status, click and select from the pop-up menu.
- To sort the order of display, click the column headings of the table.
- The last entry of the table is a visual status display of the device.
  - represents normal.
  - represents offline.
  - represents abnormal.
  - represents unknown.

Events

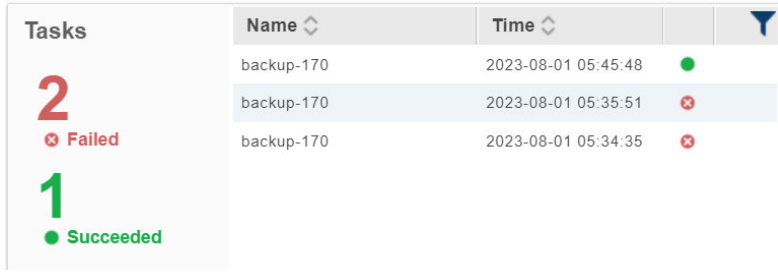
The Events panel displays critical device logs of the past 3 months.



- The number on the left is the total number of critical logs collected.
- To filter the displayed critical events by duration (e.g. for the past two months), click and select from the pop-up menu.
- Click the number in the last entry column for the logs of a particular device. A window will pop-up displaying the detailed logs. An example is shown below:

Tasks

This panel displays the scheduled tasks of the past 3 months and the status of the tasks.



- The red number on the left is the number of failed scheduled tasks.
- The green number on the left is the number of successful scheduled tasks.
- To filter tasks by duration, click and select from the pop-up menu.

Users

This panel displays which user(s) is currently online. An example is shown:

The number on the left shows how many users are currently online.

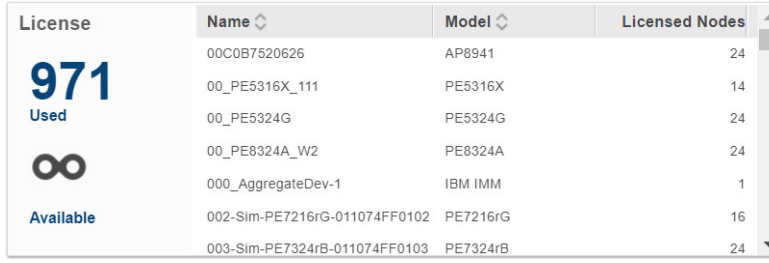
The table gives you the details of the users currently online.

The second to last entry column includes a “kill this session” icon . Click it to log this user out.

The last entry column includes a “Disable User Account” icon . Click it to disable this user account. To reactivate the user account, refer to *Reactivate Disabled Users* on page 180.

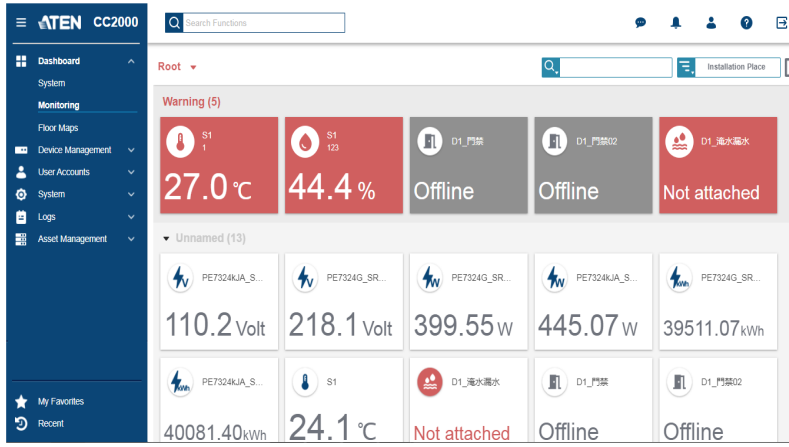
License

This panel displays the number of used and available nodes. An example is shown:

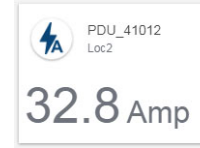


Monitoring Dashboard

The Monitoring dashboard provides a graphical summary of monitored ports and equipment (*Creating a Monitoring Rule* on page 159).

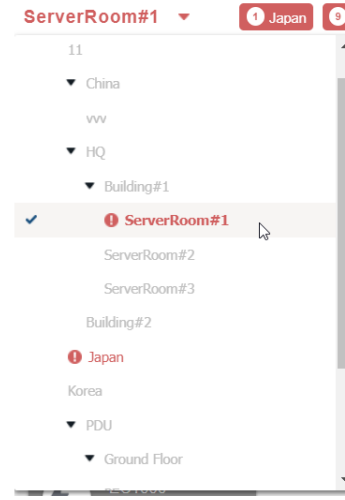


The status and value of each monitored port/equipment is represented using a card. For example:



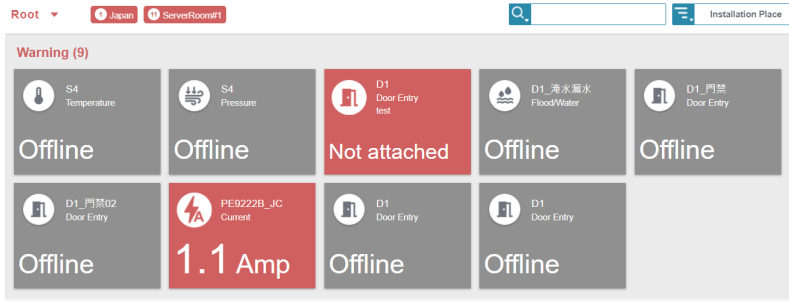
Use the drop-down menu to navigate between different levels and folders of the Monitoring dashboard.

The displayed levels and folders are based on the organization of added folders in the Monitoring Settings page. To configure the organization, see *Adding a Folder*, page 160.



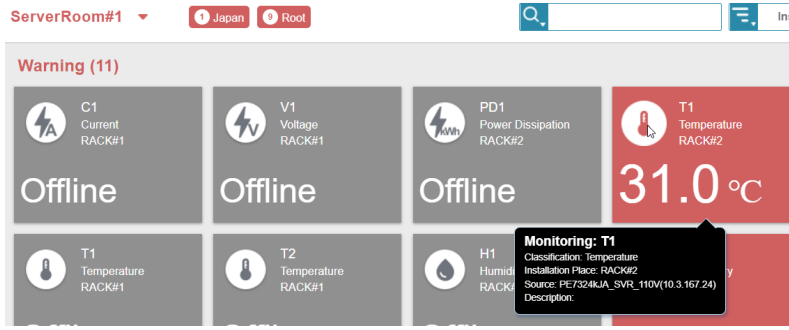
Warning Events

When monitored equipment or ports exceed its threshold or warning status (such as a door opened), the system will identify it as a warning event and indicate it using banners on top of the dashboard and changing the card to red. For example:



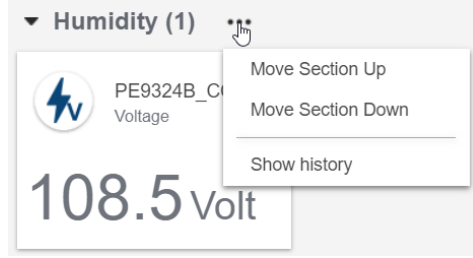
A banner indicates the total number of warning events and the folder name which contains these events. For example, the banner below shows that there are 11 warning events in the ServerRoom#1 folder.

To check out the current status of warning events, you can click on the banner to bring the dashboard view to these equipment/ports, and mouse over any card to show more information.



Re-arranging Cards

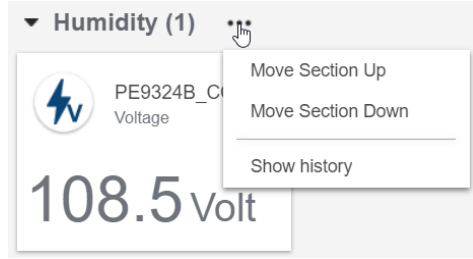
To re-arrange a section of cards, click on the dots and select **Move Section Up** or **Move Section Down**.



To re-arrange a card *within* a section, click on the card to drag-and-drop it to a new place.

Viewing Analysis Chart

To see trend charts of a group of monitored equipment/port, click the dots icon and select **Show History**. The trend charts appears. For more information about trend charts, see *Viewing Charts of Monitored Equipment*, page 164.

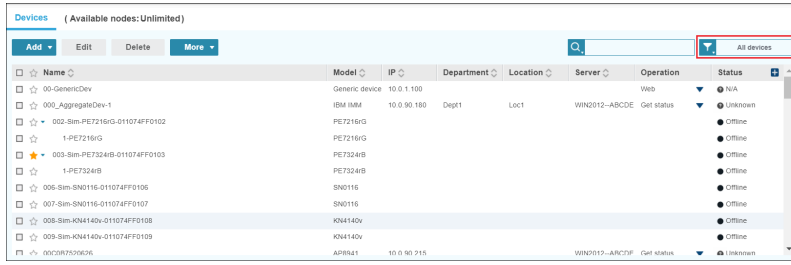


Basic Operations

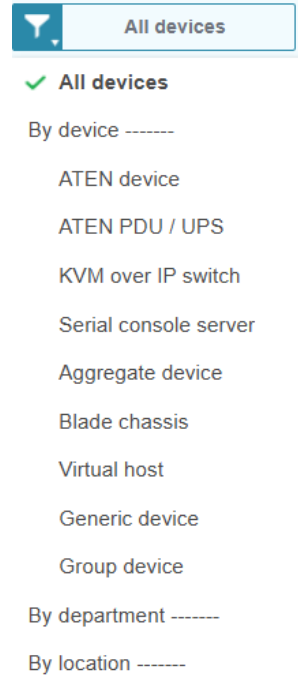
A number of basic operations can be seen throughout the CC2000 interface and are explained in the following sections.

■ Filter

Filter allows you to refine the number and the type of items being displayed. Filter for a particular table is located at the top right-hand corner above the table:



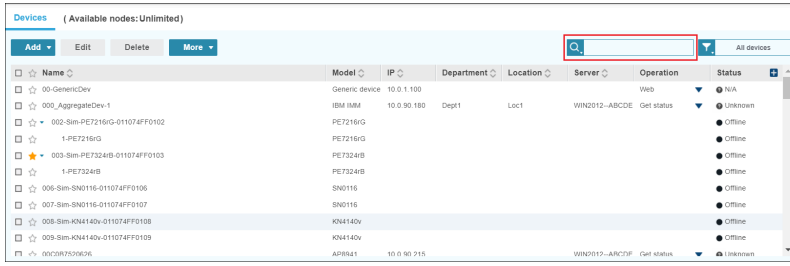
Click the filter bar for a drop-down menu that includes different filter options. An example is shown:



Click to select any of the filter to control which items are being displayed. The table will be updated to reflect your filter selection.

■ Search

Search allows you to search for items using keywords relating to the search options. Search for a particular table is also located at the top right-hand corner above the table:

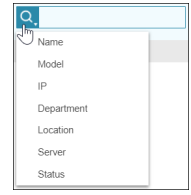


In the blank field, enter the keyword you wish to search for and press *Enter*.

The table will be updated to reflect your search result. An example is shown:

You can click the X icon to cancel your search, the table will also be updated accordingly.

To refine your search, you can click the magnifying glass for a list of search options:



Click the search options (multiple selections available) to check the categories you wish to search for. For the example shown here, you can check *Model*, *Location*, and enter something in the blank field to search for something in the *Model* and *Location* categories.

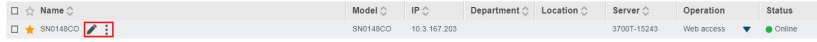
■ Table Headings

Click the table column headings to sort the display priority.

Note: The headings at the top of the table don't all appear for each view. Click the + icon to select the headings you wish to view.

■ Edit / Further Options

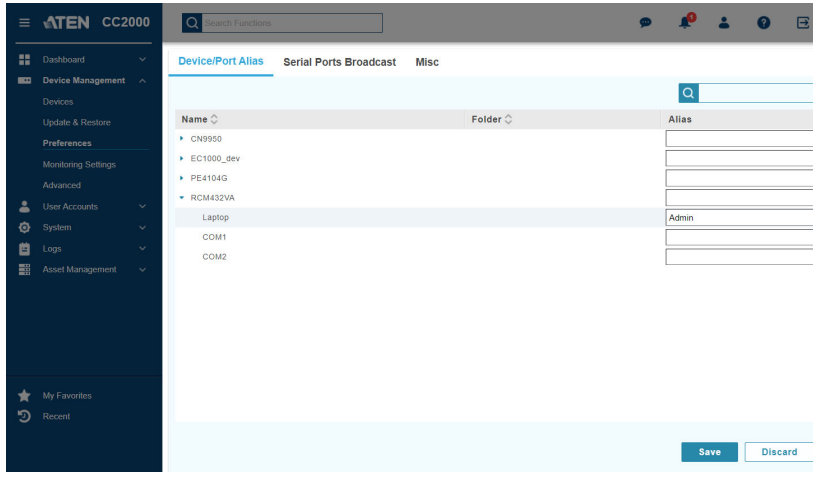
As an alternative to the *Edit* or *More* options, you may move your cursor over an item and a pencil icon and/or option icon will appear. An example is shown below:



Click one of the icons for a drop-down menu and click to select what you wish to configure. For information on these options, refer to *Editing Devices* on page 111 or on page 119.

■ Modifications on Interactive Display Panel

When editing a page on the interactive display panel, some background areas will turn gray (as shown in the example diagram below), this is to remind that any modification has not been saved.

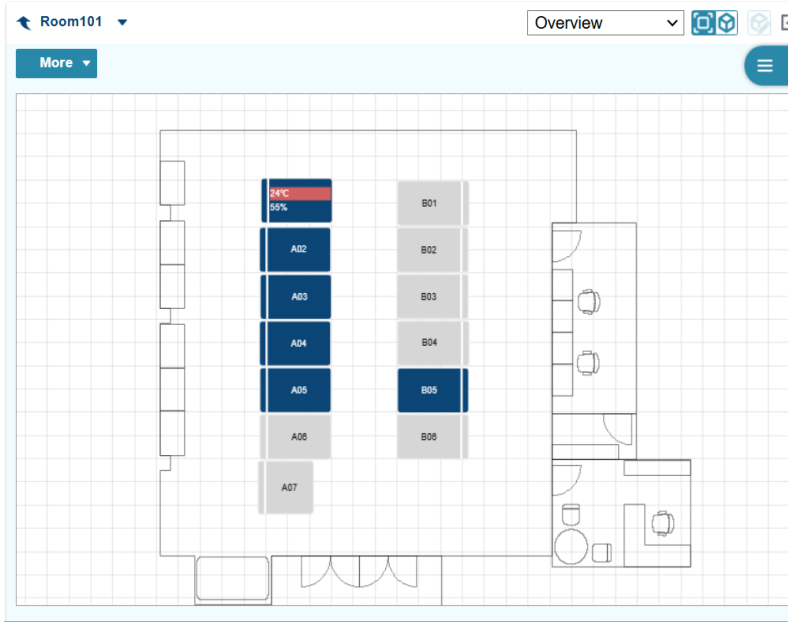


Floor Map Dashboard

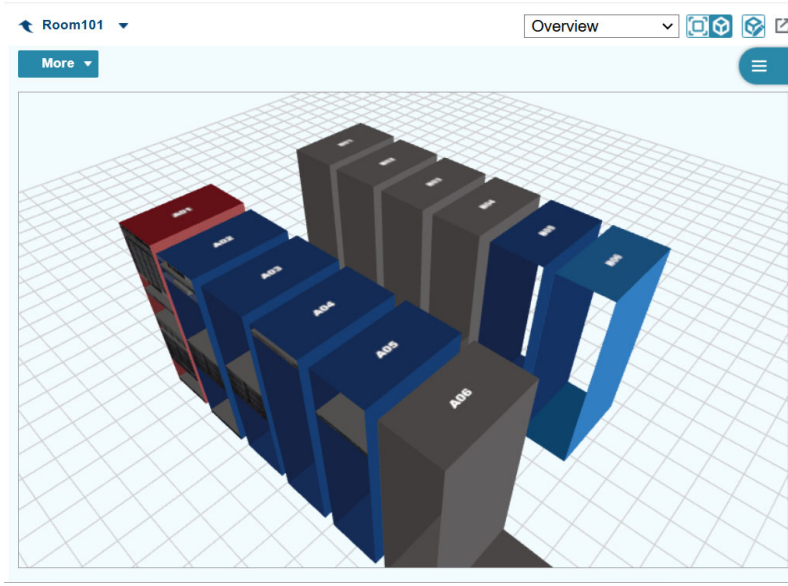
Overview

The *floor map dashboard* provides status information of monitored assets, such as available rack space, rack temperature, environment humidity, device voltage, and power etc., in 2D and 3D images, as shown below.

Floor Map Dashboard (2D)



Floor Map Dashboard (3D)

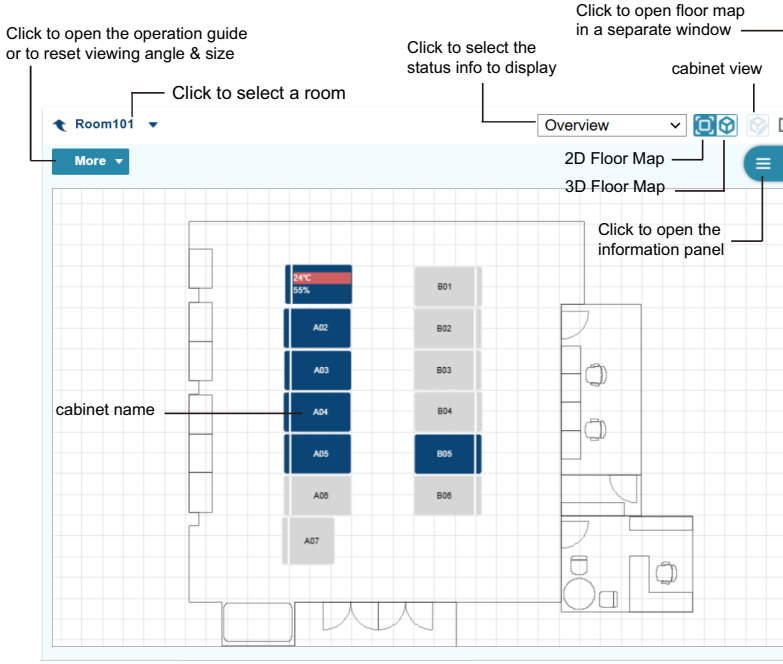


Note: To create a floor map, go to **Asset Management** > **Floor Maps**. For more information, see Chapter 9, Asset Management.

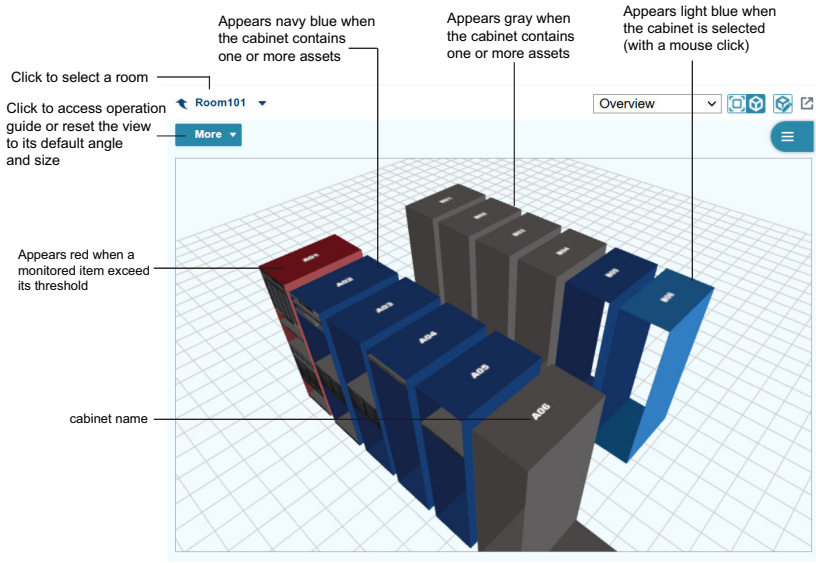
Basic Controls and Operations

- To access the floor map dashboard, go to **Dashboard** > **Floor Maps**.
- Refer to the illustrations below for an overview of the controls on 2D and 3D floor map dashboard:

2D Floor Map

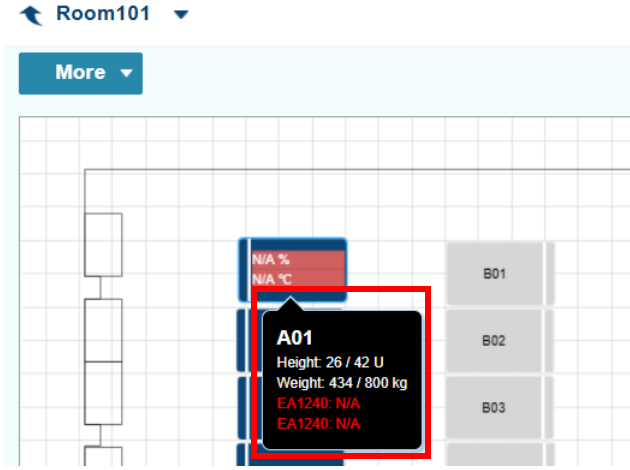


3D Floor Map



Monitor from 2D Floor Maps

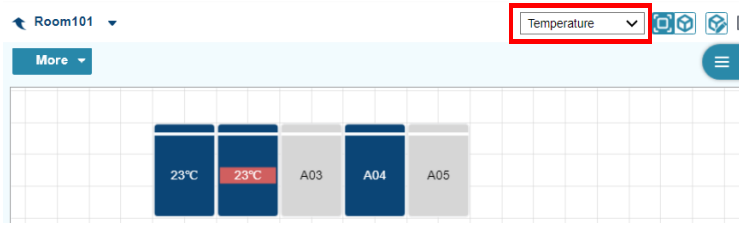
- To switch the dashboard view to 2D, click from the dashboard tool bar.



  - Status information is indicated on the cabinet icon. Mouse over a cabinet or asset to display more information.

- When a monitored item exceeds its threshold, the info is displayed in red.
- Blue icon indicates that the cabinet contains one or more assets; gray indicates that the cabinet is empty.

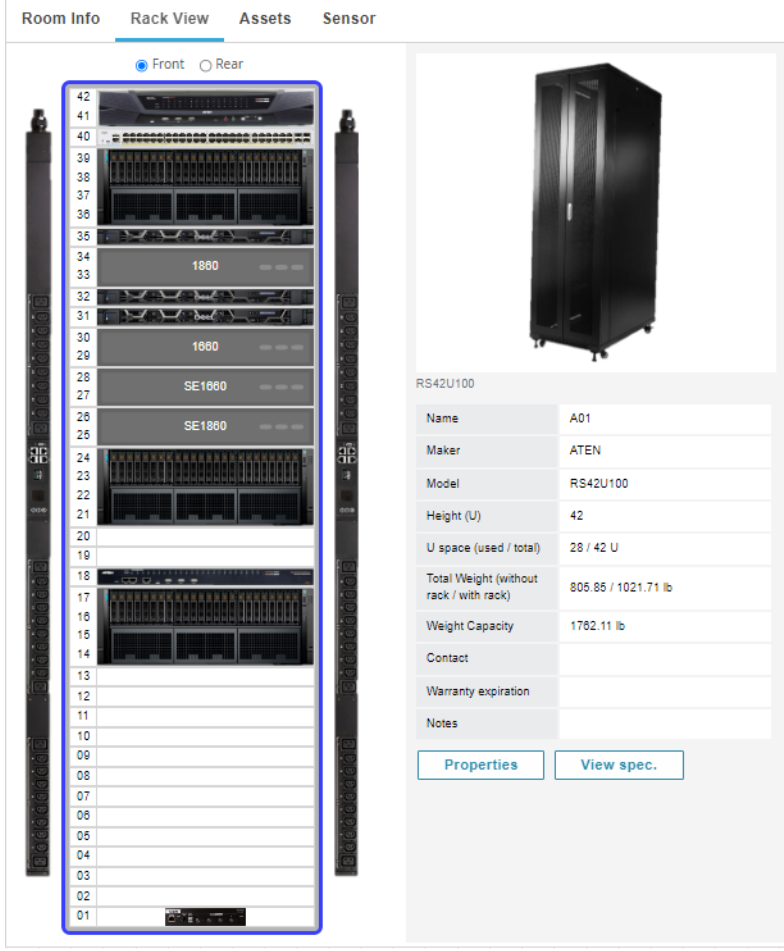
- To change the displayed information, click the drop-down menu from the top-right corner.



  - **Overview:** displays height, weight, humidity and temperature information, provided that the required sensors are also installed.
  - **Weight:** displays (total asset weight/maximum allowed weight).
  - **Space:** displays (total occupied unit space/total allowed unit space).
  - **Temperature, Humidity, Air Pressure, voltage, Current, Power, Power Dissipation:** displays detected values.

- To view detailed information of a specific cabinet, double-click on the cabinet icon to open the information panel, or click on a cabinet and then

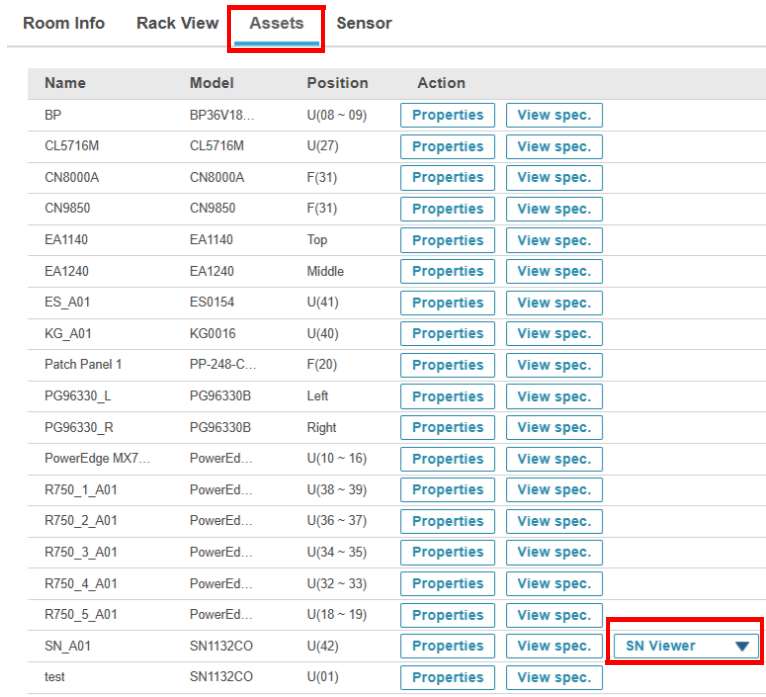
click . An information panel may contain up to 4 tabs, as illustrated below.



- **Rack View tab**
  - This tab shows a front and rear view of the cabinet. To switch views, click the **Front** or **Rear** radio button
  - To see the properties and specifications of an installed asset, click the asset from the rack photo (on the left), the photo and specs of the asset appear on the right. Click **Properties** or **View spec** to view more information.

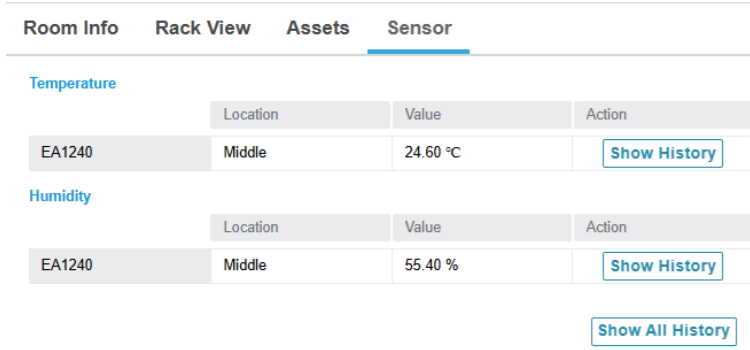
- **Assets tab**

  This tab shows a summary of assets installed to this cabinet.

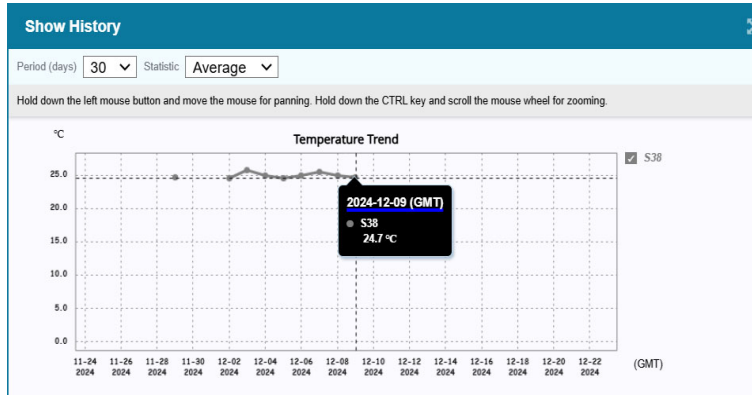


  - To see detailed asset information, click **Properties** or **View spec**.
  - Remotely access SN Viewer / Web console of ATEN KVM, serial consoles, or PDUs using the drop-down list (as shown above). To allow this access, make sure to select **Enable operations in Dashboard > Floor Maps** in device properties.

- **Sensor Tab**



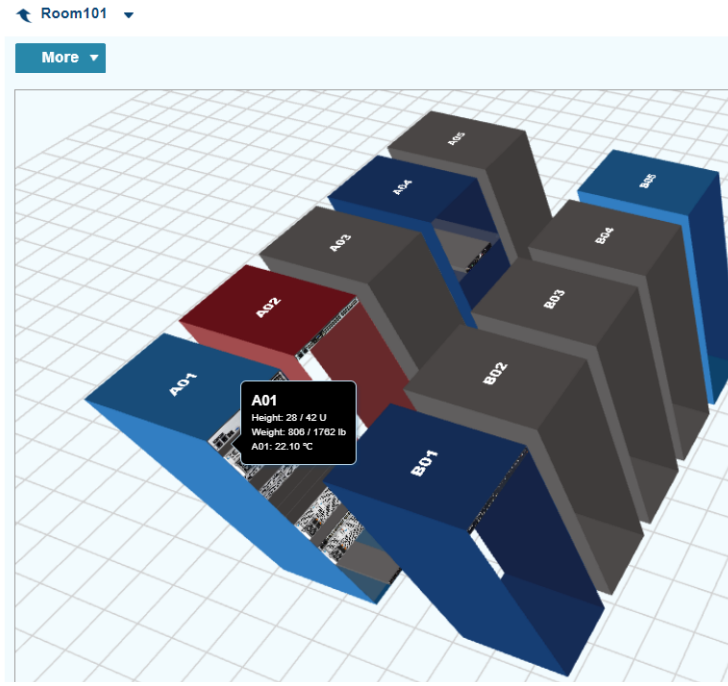
This tab shows the current detected value and historical values for all the sensors installed to this cabinet. To see history values, click **Show History**. To see historical values for all sensors, click **Show All History**. For example:



- Use the drop-down lists to apply a time period and value type (average, minimum, or maximum value) to the displayed data.
- Mouse over the dots on the chart to see detected values for specific dates.

Monitor from 3D Floor Maps

To switch the dashboard view to 3D, click  from the dashboard tool bar.



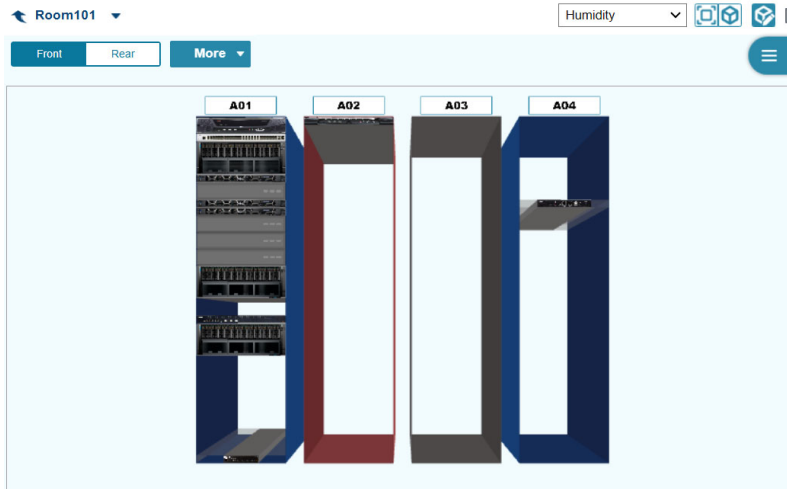
- Status information is indicated on the cabinet icon. Mouse over a cabinet or asset to display more information.
- When a monitored item exceeds its threshold, the cabinet is displayed in red. Blue icon indicates that the cabinet contains one or more assets; gray indicates that the cabinet is empty.
- To change the displayed information when a cabinet or asset is moused over, click the drop-down menu from the top-right corner.

  - **Overview:** displays height, weight, humidity and temperature information, provided that the required sensors are also installed.
  - **Weight:** displays (total asset weight/maximum allowed weight).
  - **Space:** displays (total occupied unit space/total allowed unit space).
  - **Temperature, Humidity, Air Pressure, voltage, Current, Power, Power Dissipation:** displays detected values.

- To view detailed information of a specific cabinet, double-click on the cabinet icon to open the information panel, or click on a cabinet and then click . For more information, see *Monitor from a Cabinet View* on page 63.

Monitor from a Cabinet View

You can view the cabinets in a direct front or rear view, as illustrated below.



To access this view:

1. To access the floor map dashboard, go to **Dashboard** > **Floor Maps**.
2. Click to select a cabinet or multiple cabinets by holding the **Ctrl** button.
3. Click . The selected cabinets appear in a cabinet view.

For example:

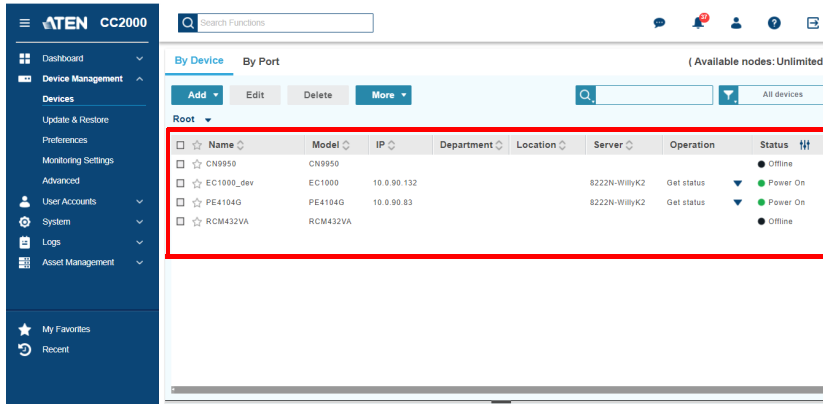
- To view detailed information of a specific cabinet, double-click on the cabinet icon to open the information panel, or click on a cabinet and then click . For more information, see *Monitor from a Cabinet View* on page 63.
- Click the **Front** or **Rear** tab to switch views.

Chapter 5
Device Management

Overview

The *Device Management* menu is used to add, configure, and organize the devices that will be managed over the CC2000 network.

Clicking *Device management* will bring you to the *Devices* submenu, which shows a **device list**:



Note: The Device Management page access is for Super Administrators, System Administrators, Device Administrators and Auditors. Auditors can only view the items in this menu. Users with device access right can also access parts of this page.

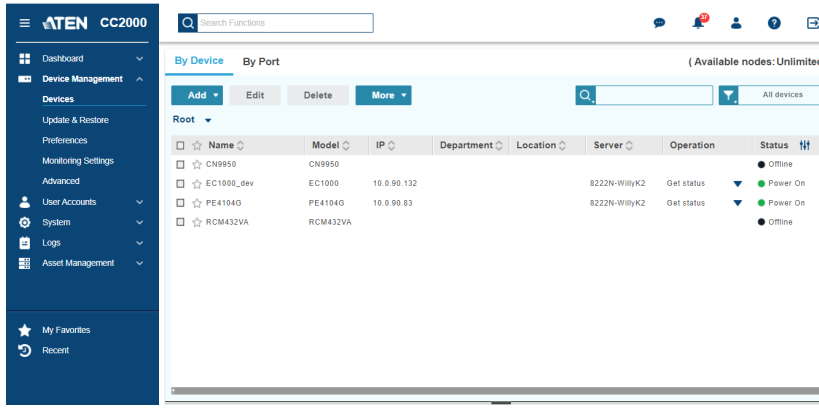
The Interactive Display Panel for *Devices* is divided into an upper and lower screen.

In the upper screen, 2 tabs are available: **By Device** and **By Port**.

All devices that have been configured for use on the CC2000 server and have been added into its database are listed in the upper screen under the **By Device** tab. An example is shown above.

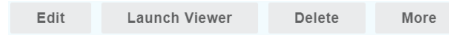
The buttons at the upper-left corner are the general operations of the **By Device** tab, as shown below. Refer to *By Devices - General Operations* on page 68 for more information.

All the ports/outlets of the added devices are listed under the **By Port** tab. An example is shown below.



The lower screen also lists the ports/outlets of the selected device. Click to highlight a device in the upper screen to display its ports/outlets in the lower screen.

The general operations for the **By Port** tab and the lower screen is shown below:



Refer to *Ports* on page 140 for more details.

Preliminary Procedures

Before devices can be managed, they must first be added into the system, which is done through four basic steps:

1. Connecting the devices to a network segment which can be reached by CC2000. You must do this for the Primary and each of the Secondaries.
2. Once the devices have been connected to an accessible network segment, the CC2000 managing that segment must be made aware of them. This can be done either by enabling the *CC Management* function on the device's ANMS page (see *Device ANMS Settings* on page 352), or with the *Initialize devices IP/Port* function in System Broadcast (see *System Broadcast* on page 169). Each of the Secondaries, then notifies the Primary of the devices connected to it.

   Note:

   - On the *Devices* page of the Primary, clicking the **Add → Auto Discovery** lists all the available devices including all of the ones connected to its Secondaries.
   - Devices that already have been added to the CC2000 management system do not show in the list of available devices.

3. From the Primary CC2000 unit, the devices recognized in step 2 must be added to the CC2000's management system (see page 77).
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 *Adding an Aggregate Device*, page 100, for details.

Using VPN

In some installations, you may prefer to use a VPN (virtual private network) environment for your CC2000 management functions. In this configuration, it is not necessary for the device to be recognized by the CC2000 that manages its network segment. It can be recognized directly by the Primary unit. This is accomplished by enabling the CC Management function (on the device's ANMS page – see page 352) and keying in the IP address of the CC2000 Primary you want the device to be recognized by. See *VPNs*, page 353, for details.

By Devices - General Operations

Introduction

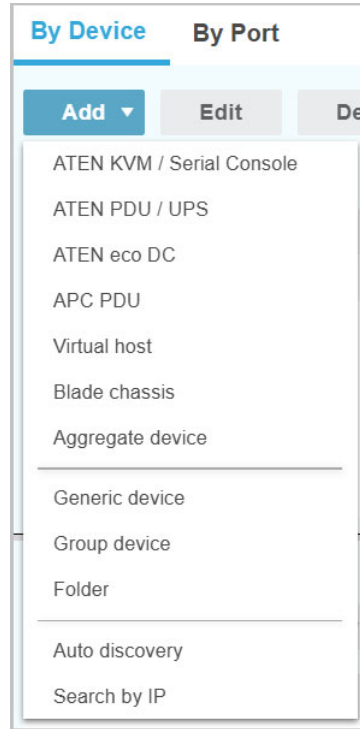
Device Table Column Headings

An explanation of the column headings is provided in the table below.

Heading	Explanation
Name	The name given to the port when it was added to the CC2000 installation.
Model	The model of the device.
IP Address	For physical devices – the device's IP Address is displayed.
MAC Address	For physical devices – the device's MAC Address is displayed.
Alias	If you gave the port an alias, the alias name appears here.
Department	The department category of the device.
Location	The location category of the device.
Server	The server the device is connected to.
Operation	The default action for accessing the device appears in this cell. ◆ Click the arrow at the right of the table cell to see what other actions are available. ◆ Click your choice to open a session for the device. The various device operation choices are described in *Operation* on page 125.
Type	The type category of the device.
Status	◆ For KVM devices, indicates whether the port is online or offline. ◆ For Serial devices, indicates whether the port is online or offline. ◆ For PDU devices, indicates whether the outlet port's power socket is On or Off. ◆ For Blade chassis, indicates whether the port is online, offline or unknown.

Device Types

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



The device types and an explanation of their purposes are described in the following table:

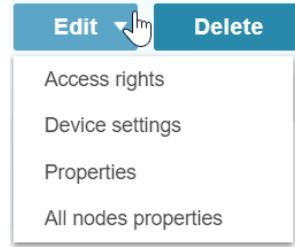
Type	Purpose
ATEN KVM / Serial Console	Select this type to add ATEN KVM devices into the CC2000 management system. CC2000 supports CN, CS, KG, KH, KL, KN, PN, SN and PE series devices. The “PE series” here only refers to the ARM-based products. If you want to add PE series products that are not ARM-based, see *Adding an ATEN PDU / UPS*, page 82, for details. **Note:** When devices are added, all of their ports are locked by default and must be unlocked. See *Transfer Settings*, page 120, for details. This allows you to add devices containing ports beyond the number allowed by the license. You can then select specific ones to unlock – thereby gaining access to critical ports while remaining within the license restrictions.

Type	Purpose
ATEN PDU / UPS	Select this type to add PE Series Energy Intelligence PDUs or UPS into the CC2000 management system. **Note:** The “PE series” here excludes ARM-based PE series products. If you want to add PE series products that are ARM-based see *Adding an ATEN KVM or Serial Console Device*, page 77, for details.
ATEN eco DC	Select this type to add eco DC into the CC2000 management system. eco DC by itself is a web-based GUI allowing users to manage and control PDUs through a web browser. To add an ATEN eco DC, refer to *Adding an ATEN eco DC* on page 85.
APC PDU	Select this type to add an APC Power Distribution Unit (PDU) into the CC2000 management system. The CC2000 supports simple device configuration, WebSSO, and power management for the following models: AP79xx, AP89xx, AP86xx. See *Adding an APC PDU*, page 89.
Aggregate Device	Select this to create a logical device consisting of ports selected from ATENKVM devices and some SPMs (e.g. IPMI, HP iLO2/3/5, IBM RSA II, Dell DRAC 5/6/8, Redfish-enabled device) that have been added to the CC2000 management system. This type of device 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 what the physical license restrictions permit. See *Adding an Aggregate Device*, page 100, 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 this to add a blade chassis.
Virtual host	Select this to add a VMware / Hyper-V / Citrix virtual host.

Type	Purpose
Generic Device	Generic devices (routers, switches, etc.) can be any third-party 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 CC2000, and are not part of the CC2000's single sign on configuration. Generic devices do not occupy device node licenses. There is no proxy support for these devices (see page 355) When you select this type of device, the CC2000 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 licensed nodes.
Group Device	Up to 64 ports can be added to a group device. Group devices are also created as a composite of ports that exist on actual ATEN/KVM devices. The differences between Group and Aggregate Devices are as follows: Once a physical port is added to an Aggregate device, it cannot be used by 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 how many Group Devices it is added to. 3. Group devices and the added ports are related to the display of panel array, please see *Panel Array Mode* on page 135.

Refer to *Adding a Device* on page 75 for details on how to add a device.

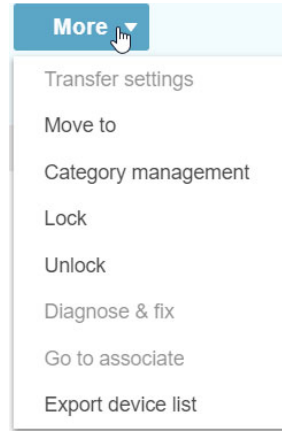
If you wish to edit a device, check the device and click *Edit* for the drop-down menu:



Refer to *Editing Devices* on page 111 for details on how to edit a device.

If you wish to delete device(s), check the device(s) and click *Delete*.

More configuration options are available here. Click *More* for the drop-down menu as shown:



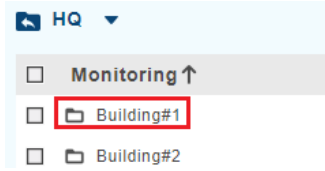
Refer to on page 119 for the option details within **More**.

Navigating the Device List

When devices and folders are organized into multiple levels with folders and sub-folders, you may need to navigate to and from different levels and folders in the device list while making configurations. The CC2000 offers a few ways to help you navigate the device list to a specific level or folder.

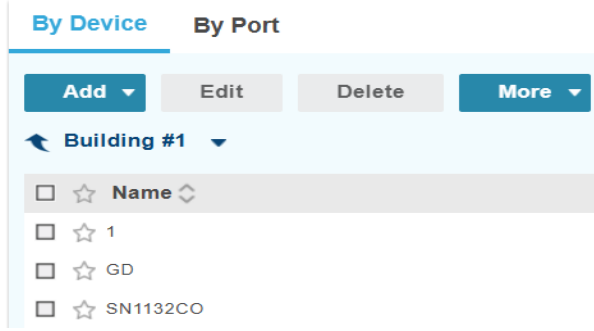
■ **To navigate to a specific level or folder:**

- Double-click the target folder directly from the device list.

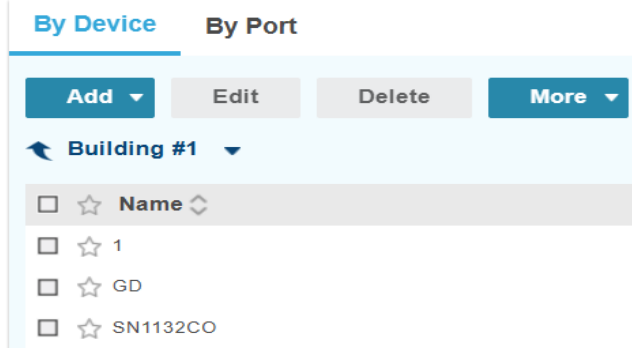


- Use the device tree drop-down menu to select the target folder/level.

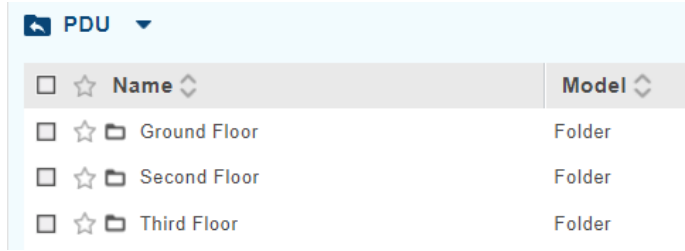
  1. In the **By Device** tab, click the **Root** drop-down button to open the device tree. A menu appears.



  2. Click to select a level. For example:

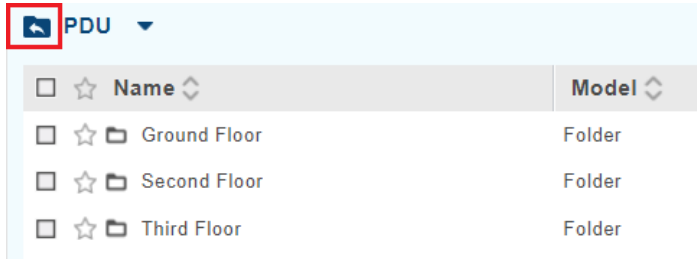


3. The view switches to the selected folder.

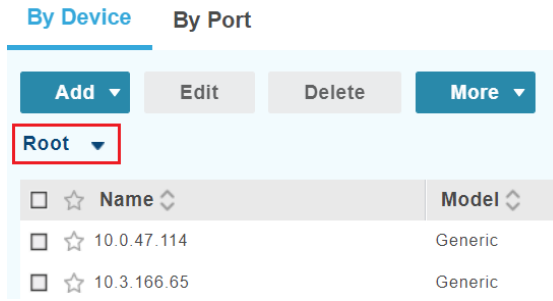


■ **To return to a previous level:**

- Click the return icon.



- Click the device tree drop-down menu and select a level/folder.



Adding a Device

Follow the steps below to add a device. Optionally create folders first before add devices into the created folders. For detailed instructions, see *Adding a Folder* on page 76.

1. Go to **Device Management** > **Devices**.
2. Click **Add** for a drop-down menu.

3. Click to select the type of device you would like to add from the list. A window pops up. The interface of the window depends on your selection. For more details on adding each device type, refer to the following sections:
   - *Adding an ATEN KVM or Serial Console Device* on page 77
   - *Adding an ATEN PDU / UPS* on page 82
   - *Adding an ATEN eco DC* on page 85
   - *Adding an APC PDU* on page 89
   - *Adding a Virtual Host* on page 92
   - *Adding a Blade Chassis* on page 96
   - *Adding an Aggregate Device* on page 100
   - *Adding a Generic Device* on page 105

Adding a Folder

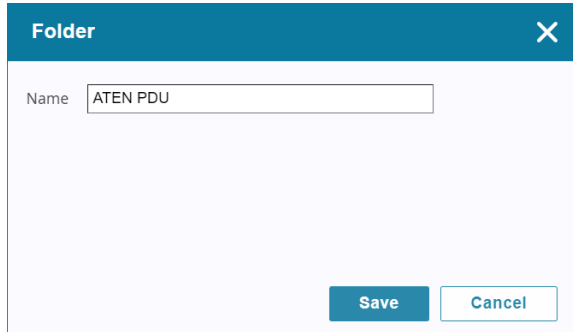
You can create folders and sub-folders to help you organize added devices by type, location, or product series, depending on your needs. To add a folder, use one of the following method.

■ Using the add + button.

1. In the devices list page, mouse over the target folder.
2. Click + to open a selection menu and then select **Folder**.

■ Using the navigation menu

1. In the devices list page, navigate to a level or folder where you wish to add a folder.
2. Click **Add** ▾.
3. In the pop-up menu, click **Folder**. This screen appears.



4. Name the folder and then click **Save**.

   To edit a folder name, mouse over the target device, click ✎ and then select **Properties**.

Adding an ATEN KVM or Serial Console Device

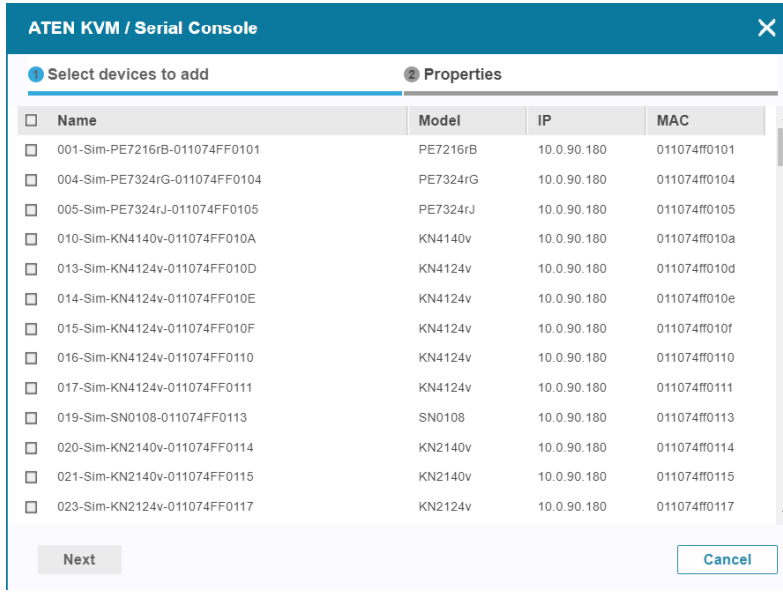
This item refers to adding ATEN KVM / Serial Console device into the CC2000 management system. CC2000 supports CN, CS, KG, KH, KL, KN, PN, SN and ARM-based PE series devices.

To add PE series products that are not ARM-based see *Adding an ATEN PDU / UPS*, page 82, for details.

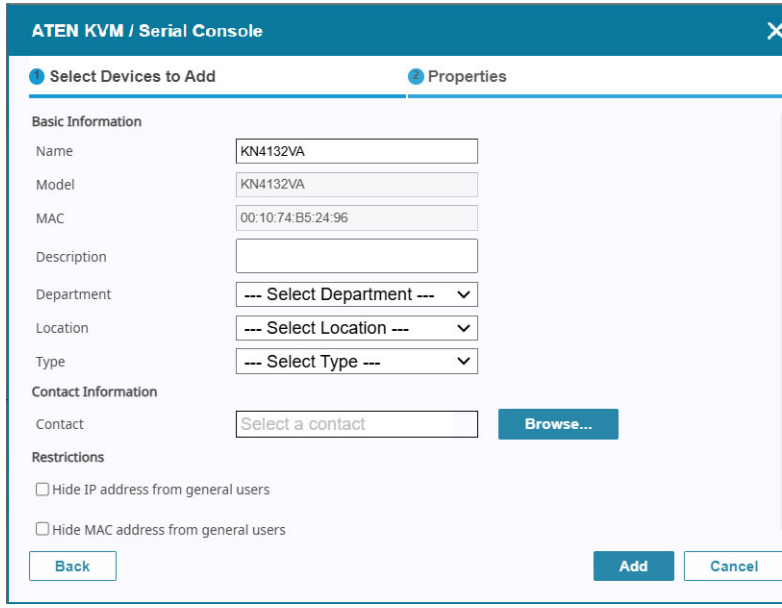
Note: Before attempting to add an ATEN KVM device to the CC2000 server, make sure it has been recognized. See *Preliminary Procedures*, page 67, for details.

To add an ATEN KVM:

1. Select **ATEN KVM / Serial Console** from the drop-down menu. A window pops up listing all the online devices that can be added.



2. Click to check the checkbox of the device you wish to add and click **Next**. This window appears.



3. Fill in the fields according to the information provided in the table below:

Field	Information
Basic Information	**Name**: Provide a name of 1-48 characters 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 CC2000 database. The name on the original configuration remains the same. **Model**: The CC2000 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 is displayed here. **MAC Address**: The CC2000 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 (you have previously created – see *Category Management* on page 122), and click on the one you want the device to belong to. **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 (you have previously created – see *Category Management* on page 122), and click on the one you want the device to belong to. **Type:** For organization purposes, specify the device type. If you wish to do so, drop down the list of types (you have previously created – see *Category Management* on page 122), and click on the one you want. **Description**: If you wish to provide extra information to describe the device, enter it here. This field is optional.
Contact Information	Click **Browse** to add a contact. This field is optional. To create a new contact, go to **System** > **Contacts**.

Field	Information
Restrictions	**Hide IP Address from general users:** This is an added security measure. Enable this setting to prevent the device's IP address from appearing in the Device List when users log in via their browser. **Hide MAC Address from general users:** This is an added security measure. Enable this setting to prevent the device's MAC address from appearing in the Device List when users log in via their browser. **Enable operations in Dashboard > Floor Maps:** Select this setting to allow remote operations of a selected device via SN Viewer or Web browsers from dashboard floor maps (page 60). Note that this setting is only available for super administrators, system administrators, and device administrators.
CC2000 Options	**Allow users to access the device through viewer or its web login page**As an added security measure. If this feature is not enabled, the device will only accept logins through the CC2000. While the device is connected to the CC2000 system, users cannot log in to the device using the device's own authentication system, and they can only manage the device through the CC2000's interface. **Note:** 1. If the device becomes disconnected from the CC2000 system, users will be able to log into the device using its own authentication system. 2. If the checkbox is checked, it means that other authentication is enabled and users can log into the device using its own authentication system. **Enable device logs to be sent to CC2000**If this feature is enabled, the CC2000 acts as the device's log server – receiving and storing the device's tick event information, and having it available for retrieval. **Disable PDU local schedule:** Checking this option will disable the PDU's local schedule. **Device session timeout**A web-accessed session to a device will time out if the session receives no input for a duration. Set the timeout duration by entering a number (2-99 minutes) in the field here. If 0 is entered, the session will never time out.

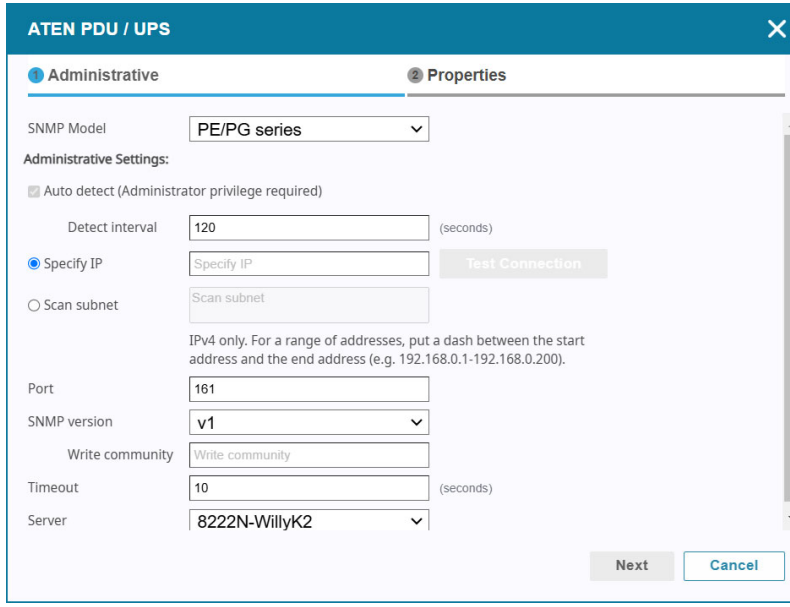
4. When you have finished, click **Add** to complete the procedure.

Note:

- For Cat5 KVM switches, only the ports that have a KVM adapter cable attached and are online can be recognized and 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.
- If you have difficulty adding ARM-based PE series PDU, refer to *Adding ARM-based PE series PDU* on page 360 for more details.

Adding an ATEN PDU / UPS

This item refers to adding ATEN PDU(s) or UPS into the CC2000 management system:

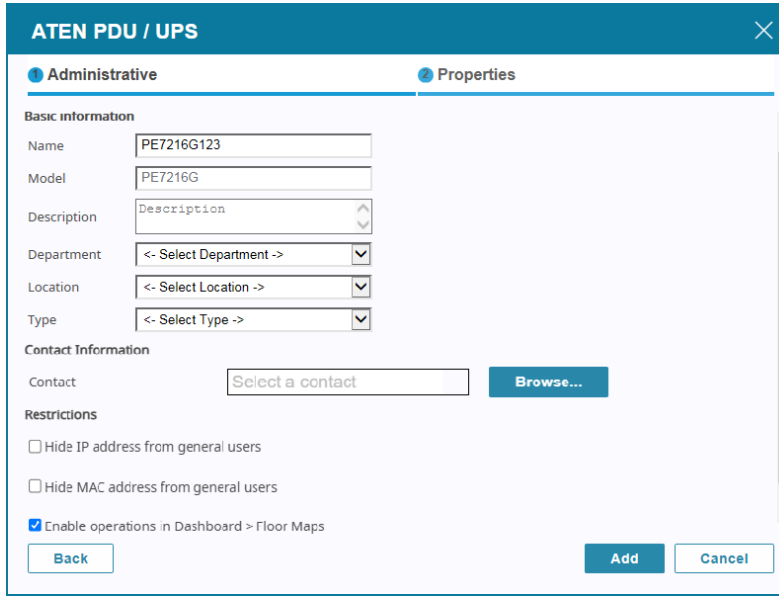


1. Fill in the fields according to the information provided in the table below:

Field	Information
SNMP Model	Use the drop-down menu to select between **PE/PG series** or **OL series**. Note that the “PE series” here refers to Energy Intelligence PDUs that are *not* ARM-based products. **Note:** To add ARM-based PE series products, see *Adding an ATEN KVM or Serial Console Device*, page 77, for details.
Auto detect	Enable this function to allow the system to automatically check if the device is online or not. Only a user with administrator privileges can enable this function. **Note:** For ATEN PDUs, Auto detect is always enabled.
Detect interval	Set the detect interval by entering a value between 30 and 300 seconds. This sets how often the system shall automatically check if the device is online or not.

Field	Information
Specify IP	Key in the IP address of the device. Click the **Test connection** button to confirm that the IP address has been detected.
Scan subnet	Key in a range of subnet IP addresses that can help search for the device.
Port	Key in the port number used to access the device. The default port is 161.
SNMP version	Select the SNMP version to use: v1, v2c, or v3.
Write community	Key in the community value(s) if required by the SNMP version.
Timeout	Key in the server timeout value. The range is between 10 and 120.
Server	Select a server to use.

2. When you have finished, click **Next**. The Properties page appears.



3. Fill in the fields according to the information provided in the table below:

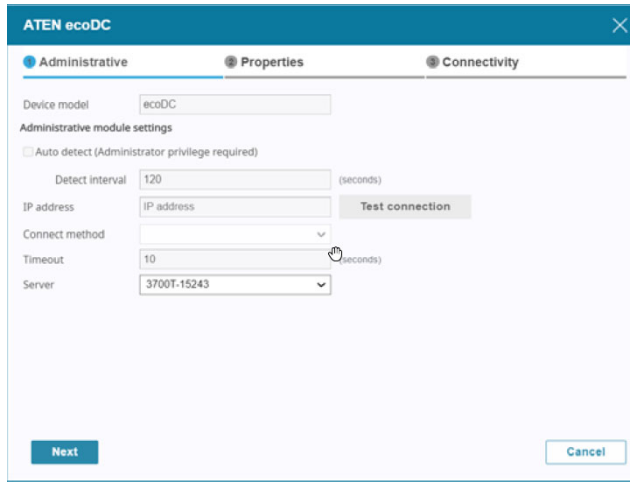
Field	Information
Device Information	**Name**: Provide a name to identify the device. **Model:** The CC2000 recognizes the device model and fills in this field automatically. It cannot be edited. **Description**: If you wish to provide extra information to describe the device, enter it here. This field is optional. **Department**: For organizational purposes, you can establish department categories (R&D, for example), and assign devices to them (see *Category Management* on page 122). If you wish to assign this device to a department, use the drop-down menu of departments (you have previously created) and click the one you want the device to belong to. **Location**: For organizational purposes, you can establish location categories (West Coast, for example), and assign devices to them (see *Category Management* on page 122). If you wish to assign this device to a location, use the drop-down menu of locations (you have previously created) and click the one you want the device to belong to. **Type**: Use the drop-down menu to select the device type.
Contact Information	Click **Browse** to add a contact. This field is optional. To create a new contact, go to **System** > **Contacts**.
Restrictions	**Hide IP Address from general users:** As an added security measure, if this feature is enabled, it prevents the device's IP address from appearing in the Device List when users log in via their browser. **Hide MAC Address from general users:** As an added security measure, if this feature is enabled, it prevents the device's MAC address from appearing in the Device List when users log in via their browser. **Enable operations in Dashboard > Floor Maps:** Select this setting to allow remote operations of a selected device via SN Viewer or Web browsers from dashboard floor maps (page 60). Note that this setting is only available for super administrators, system administrators, and device administrators.

4. When you have finished with this page, click **Add**.

Note: After adding a device, its ports are locked. See *Locking / Unlocking Devices*, page 124.

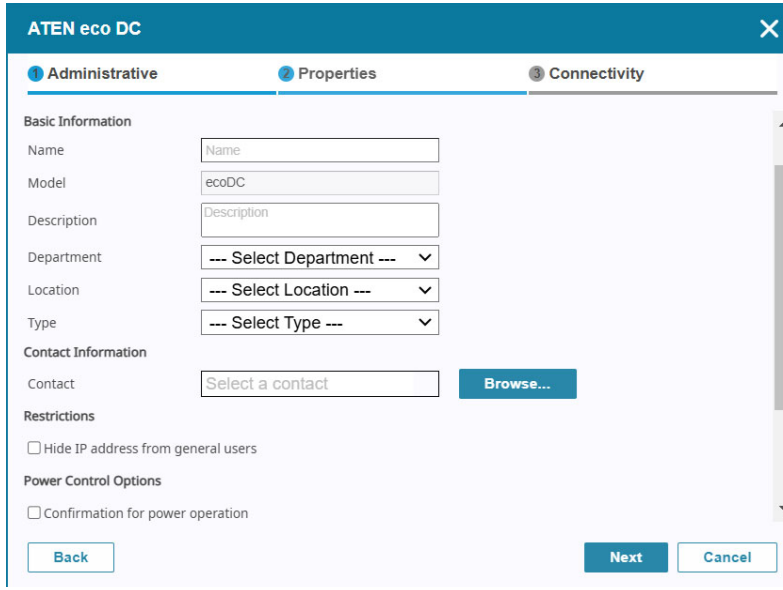
Adding an ATEN eco DC

This item refers to adding an ATEN eco DC to the CC2000 management system:



To add an ATEN eco DC, do the following:

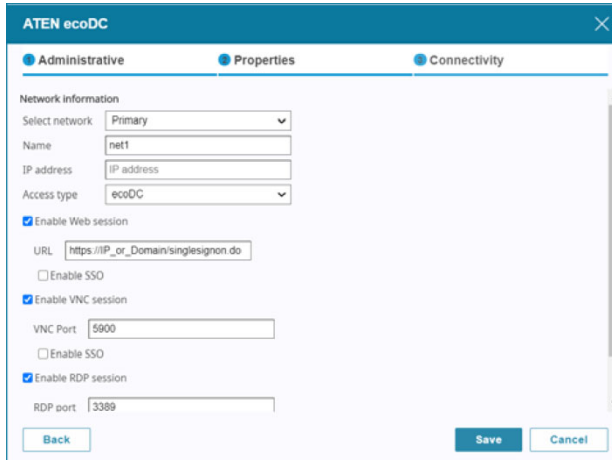
1. Select the Server using its drop-down menu and click **Next**. The Properties page appears.



2. Fill in the fields according to the information provided in the table below:

Field	Information
Basic Information	**Name:** Provide a name to identify the eco DC. **Model:** The CC2000 recognizes the server and fills in this field automatically. It cannot be edited. **Description:** If you wish to provide extra information to describe the server, enter it here. This field is optional. **Department:** For organizational purposes, you can establish department categories (R&D, for example), and assign devices/servers to them (see *Category Management* on page 122). If you wish to assign this server to a department, use the drop-down menu to select the department (you have previously created) you want the server to belong to. **Location:** For organizational purposes, you can establish location categories (West Coast, for example), and assign devices/servers to them (see *Category Management* on page 122). If you wish to assign this server to a location, use the drop-down menu to select the location (you have previously created) you want the server to belong to. **Type:** Use the drop-down menu to select the type of device it is.
Contact Information	Click **Browse** to add a contact. This field is optional. To create a new contact, go to **System** > **Contacts**.
Restrictions	**Hide IP Address from general users:** As an added security measure, if this feature is enabled, it prevents the device's IP address from appearing in the Device List when users log in via their browser.
Power Control Options	Set the Power Control Options as outlined below: ◆ Click the box to enable confirmation for power operation ◆ Click the box to enable delay for power operation, and set the Power on delay / Power off delay / Power restart delay fields in seconds.

3. When you have finished with this page, click **Next**. The Connectivity page appears.



4. Fill in the fields according to the information in the table below:

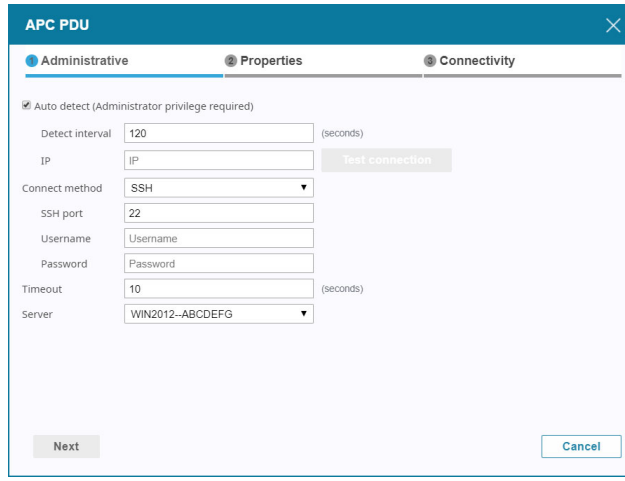
Field	Explanation
Network Information	**Select network:** If the server of the eco DC only has one network interface, select **Primary**. If it has more than one network interface, after you finish configuring the Primary one, come back to choose the additional ones and configure each of them in turn. **Name:** For convenience, each of the network interfaces can be named. **IP Address:** Enter the eco DC's IP address here. **Access Type:** Use the drop-down menu to select the access type.
Web Session	Check to enable web operation. **URL:** To access the eco DC server via the Web, enter the URL that will bring up its management page. **Enable SSO**: Check this box to enable single sign on functionality, and select which credentials to use. ◆ Select *Use login user credentials* to use the same username and password as the CC2000 user account. ◆ Select *Use following credentials* and enter new credentials in the fields below. ◆ **Login name, Password:** Fill in these fields according to the ecoDC server's authentication and authorization procedures.
VNC Session	Check to enable VNC operation. **VNC Port:** Enter the port number for the VNC session **Enable SSO**: Check this box to enable single sign on functionality, and enter the *View only* and *Full control* passwords.

Field	Explanation
RDP Session	Check to enable RDP operation. **RDP Port:** Enter the port number for the RDP session. **Always use local RDP client on Windows platform:** Check the check box to enable this function. **Note:** If this option is checked, SSO will be disabled. **Enable SSO**: Check this box to enable single sign on functionality, and then select which credentials to use. ◆ Select *Use login user credentials* to use the same account username and password as the CC2000 user account. ◆ Select *Use following credentials* and enter new credentials in the fields below.

5. When you have finished with this page, click **Save**. The system will display a list for you to select which devices are to be added to the ATEN eco DC. Check and select the device(s)/port(s) you wish to be associated with the ATEN eco DC.

Adding an APC PDU

This item refers to adding APC PDU into the CC2000 management system:

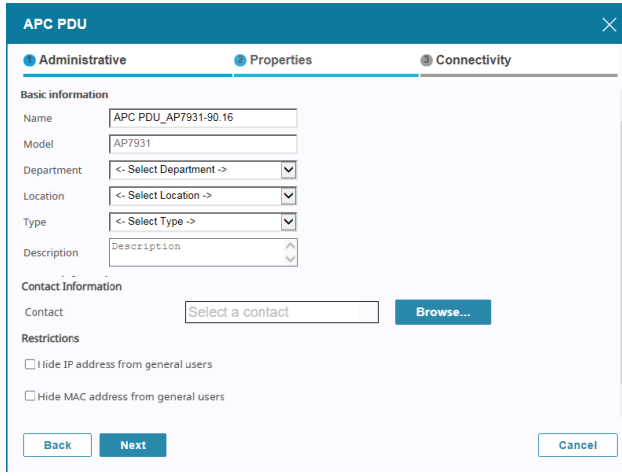


To add an APC PDU, do the following:

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

Field	Information
Auto Detect	Enable Auto detect for the CC2000 to check if the device is online or not. Only a user with administrator privileges can enable this function.
Detect Interval	Set the detect interval by entering a value in seconds. This is how often the system shall automatically check for the online status of the APC PDU.
IP	Key in the APC PDU's IP address. Click **Test Connection** to confirm that the IP has been correctly detected.
Connect Method	Select either SSH or Telnet from the drop-down menu.
SSH Port	Key in the access port used to connect to it (via browser). The default SSH port is 22; Telnet is 23.
Username / Password	Key in a username and password that will be required to access the APC PDU (via Telnet only).
Timeout	The amount of time to wait for a connection request to complete before canceling the request.
Server	Select the CC2000 unit that the APC PDU server is connected under.

2. When you have finished with this page, click **Next**. The Properties page appears.

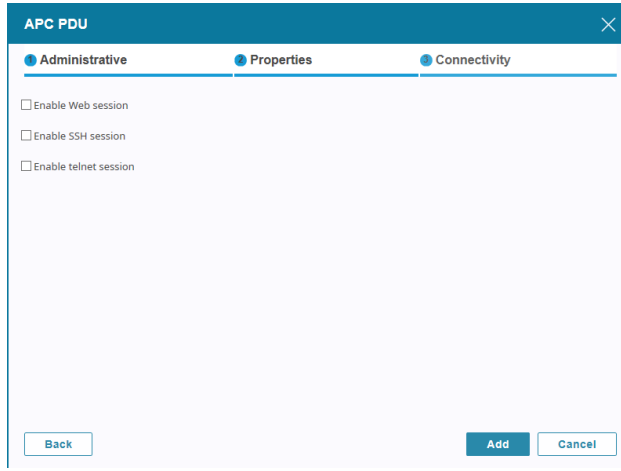


3. Fill in the fields according to the information provided in the table below:

Field	Information
Device Information	**Name:** Provide a name to identify the device. **Model:** The CC2000 recognizes the device model and 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 (see *Category Management* on page 122). If you wish to assign this device to a department, drop down the list of departments (you have previously created), and click on the one you want the device to belong to. **Location:** For organizational purposes, you can establish location categories (West Coast, for example), and assign devices to them (see *Category Management* on page 122). If you wish to assign this device to a location, drop down the list of locations (you have previously created), and click on the one you want the device to belong to. **Type:** Use the drop-down menu to select the type of device it is. **Description:** If you wish to provide extra information to describe the device, enter it here. This field is optional.
Contact Information	Click **Browse** to add a contact. This field is optional. To create a new contact, go to **System** > **Contacts**.

Field	Information
Restrictions	**Hide IP Address from general users:** As an added security measure, if this feature is enabled, it prevents the device's IP address from appearing in the Device List when users log in via their browser. **Hide MAC Address from general users:** As an added security measure, if this feature is enabled, it prevents the device's MAC address from appearing in the Device List when users log in via their browser.

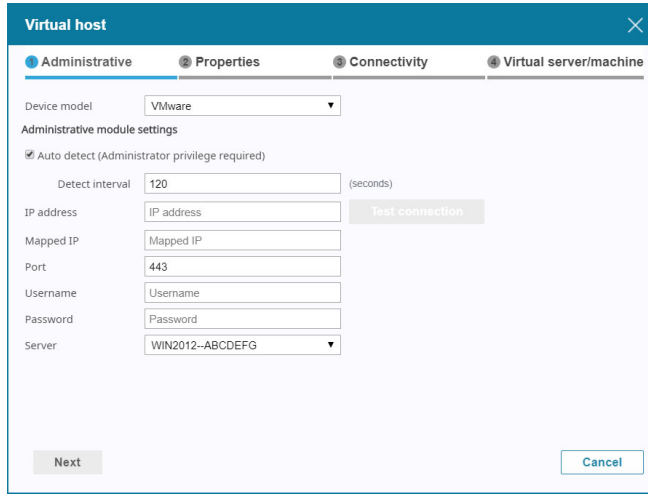
4. When you have finished with this page, click **Next**. The Connectivity page appears. Check to enable web / SSH / Telnet sessions.



5. When you have finished, click **Add** to complete the procedure.

Adding a Virtual Host

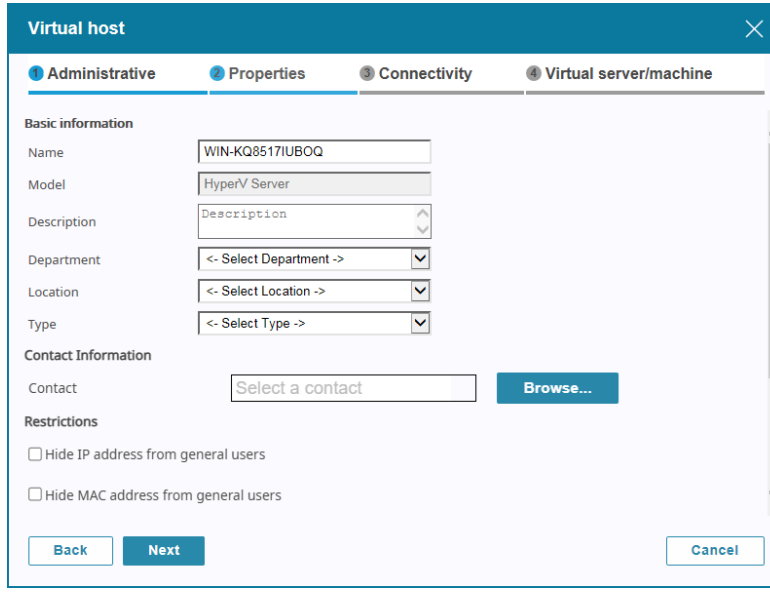
This item refers to adding Virtual Host into the CC2000 management system.



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

Field	Information
Device Model	Select either VMware, Citrix or HyperV from the drop-down menu. **Note:** For CC2000 to manage HyperV hosts, make sure to install CC2000 on Windows 10, 11, or Server 2016/2019/2022.
Auto Detect	Enable this function for the system to automatically check if the virtual machine is online or not. Only a user with administrator privileges can enable this function.
Detect Interval	Set the detect interval by entering a value in seconds. This is how often the system shall automatically check for the online status of the virtual machine.
IP Address / Port	Key in the virtual machine's IP address and the access port used to connect to it (via browser). The default port is 443. Click **Test Connection** to confirm that the IP and port settings have been correctly detected.
Mapped IP	The Mapped IP function is for VMware remote console support (VMRC through router/firewall). To enable the function, enter the virtual host's external IP address in the *Mapped IP* field.
Username / Password	Key in a username and password that will be required to access the virtual machine (via browser).
Server	Select the CC2000 unit that the Virtual Host server is connected under.

2. When you have finished with this page, click **Next**. The Properties page appears.

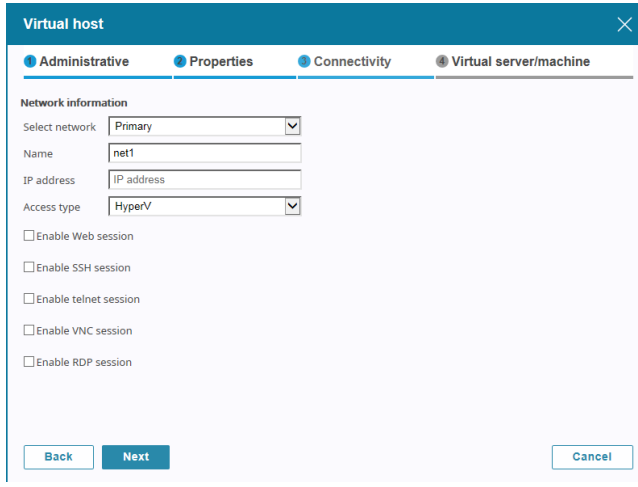


3. Fill in the fields according to the information provided in the table below:

Field	Information
Device Information	**Name:** Provide a name to identify the device. **Model:** The CC2000 recognizes the device model and fills in this field automatically. It cannot be edited. **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 *Category Management* on page 122). If you wish to assign this device to a department, drop down the list of departments (you have previously created), and click on the one you want the device to belong to. **Location:** For organizational purposes, you can establish location categories (West Coast, for example), and assign devices to them (see *Category Management* on page 122). If you wish to assign this device to a location, drop down the list of locations (you have previously created), and click on the one you want the device to belong to. **Type:** Use the drop-down menu to select the type of device it is.

Field	Information
Contact Information	Click **Browse** to add a contact. This field is optional. To create a new contact, go to **System** > **Contacts**.
Restrictions	**Hide IP Address from general users:** As an added security measure, if this feature is enabled, it prevents the device's IP address from appearing in the Device List when users log in via their browser. **Hide MAC Address from general users:** As an added security measure, if this feature is enabled, it prevents the device's MAC address from appearing in the Device List when users log in via their browser.

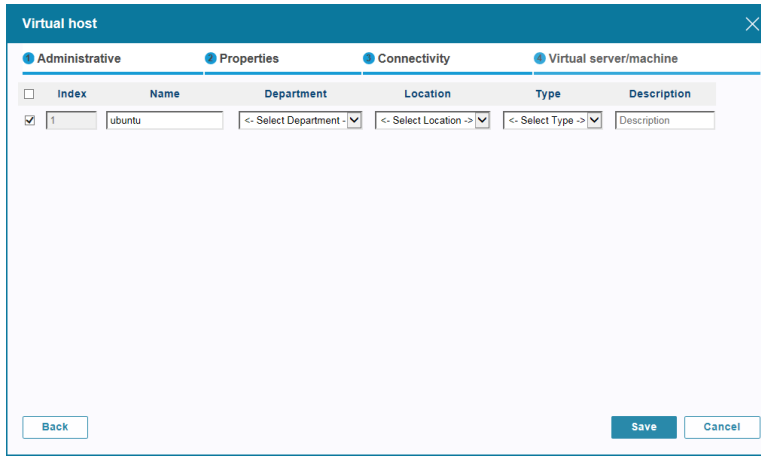
4. When you have finished with this page, click **Next**. The Connectivity page appears.



5. Fill in the fields according to the information in the table below:

Field	Explanation
Network Information	**Select network:** If the server for the virtual host only has one network interface, select **Primary**. If it has more than one network interface, after you finish configuring the Primary one, come back to choose the additional ones and configure each of them in turn. **Name:** For convenience, each of the network interfaces can be named. **IP Address:** Enter the Virtual Host's IP address here. **Access Type:** Use the drop-down menu to select the access type.
Sessions	Check to enable the sessions.

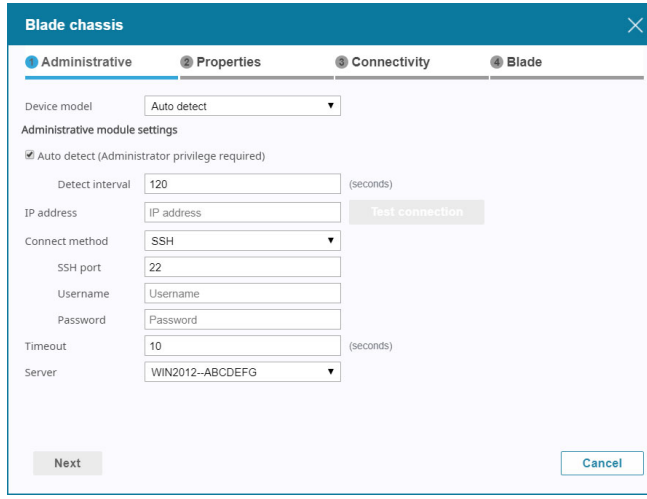
6. When you have finished with this page, click **Next**. The Virtual server/ machine page appears.



7. Check the information and click **Save** to complete.

Adding a Blade Chassis

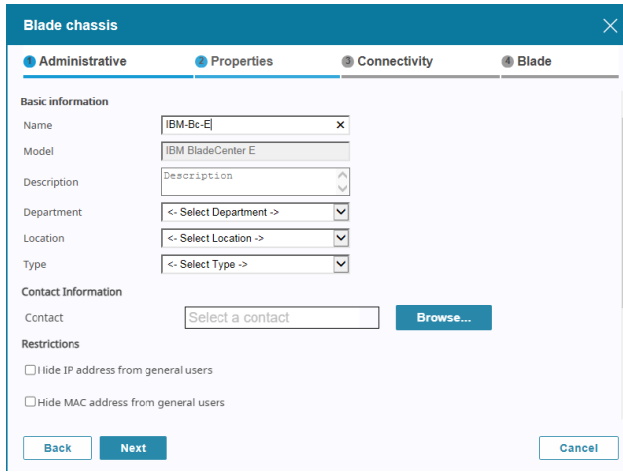
This item refers to adding Blade chassis into the CC2000 management system:



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

Field	Information
Device Model	Use the drop-down menu to select the model type you are adding.
Auto detect	Enable Auto detect for the CC2000 to check if the device is online or not. Only a user with administrator privileges can enable this function.
Detect Interval	Set the detect interval by entering a value in seconds. This is how often the system shall automatically check if the blade server is online or not.
IP Address / Connect method / SSH Port	If Auto detect is not being used, key in the blade server's IP address and the access port used to connect to it (via Telnet or SSH). Select the connection method. The default port is 22 (SSH). Click **Test Connection** to confirm that the IP and port settings have been correctly detected.
Username / Password	Key in a username and password that will be required to access the blade server (via Telnet or SSH). **Note:** Use an account with administrator privileges to get needed information.
Timeout	The amount of time to wait for a connection request to complete before canceling the request.
Server	Select the CC2000 unit that the Blade server is connected under.

2. When you have finished with this page, click **Next**. The Properties page appears.

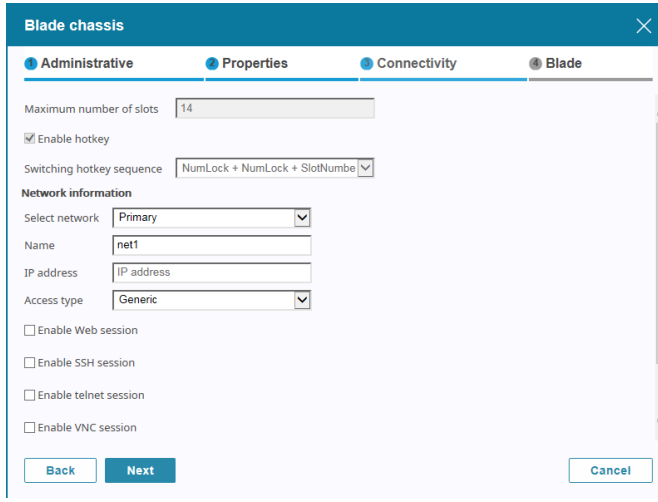


3. Fill in the fields according to the information provided in the table below:

Field	Information
Device Information	**Name:** Provide a name to identify the device. **Model:** The CC2000 recognizes the device model and fills in this field automatically. It cannot be edited. **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 *Category Management* on page 122). If you wish to assign this device to a department, drop down the list of departments (you have previously created), and click on the one you want the device to belong to. **Location:** For organizational purposes, you can establish location categories (West Coast, for example), and assign devices to them (see *Category Management* on page 122). If you wish to assign this device to a location, drop down the list of locations (you have previously created), and click on the one you want the device to belong to. **Type:** Use the drop-down menu to select the type of device it is.
Contact Information	Click **Browse** to add a contact. This field is optional. To create a new contact, go to **System** > **Contacts**.

Field	Information
Restrictions	**Hide IP Address from general users:** As an added security measure, if this feature is enabled, it prevents the device's IP address from appearing in the Device List when users log in via their browser. **Hide MAC Address from general users:** As an added security measure, if this feature is enabled, it prevents the device's MAC address from appearing in the Device List when users log in via their browser.
Power Control Options	Set the Power Control Options as outlined below: ◆ Click the box to enable confirmation for power operation ◆ Click the box to enable delay for power operation, and set the Power on delay/ Power off delay fields in seconds.

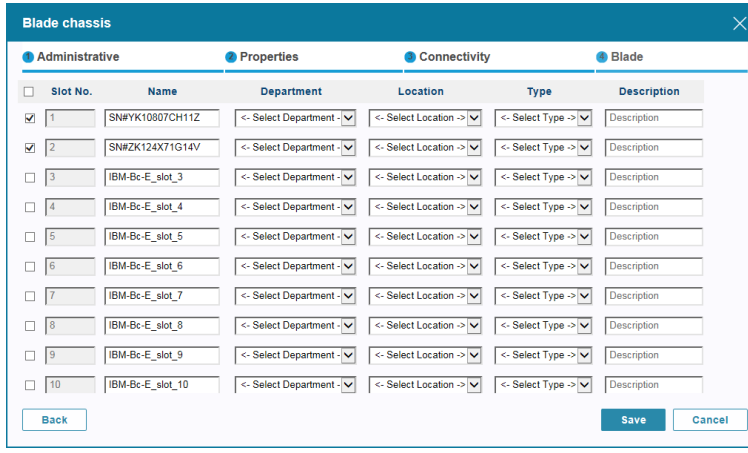
4. When you have finished with this page, click **Next**. The Connectivity page appears.



5. Fill in the fields according to the information in the table below:
   - 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.
   - For the *Blade switching hotkey*, this information is filled in automatically with the details of the assigned model.

Field	Explanation
Network Information	**Select network:** If the server for the blade chassis only has one network interface, select **Primary**. If it has more than one network interface, after you finish configuring the Primary one, come back to choose the additional ones and configure each of them in turn. **Name:** For convenience, each of the network interfaces can be named. **IP Address:** Enter the Virtual Host's IP address here. **Access Type:** Use the drop-down menu to select the access type.
Sessions	Check to enable the sessions.

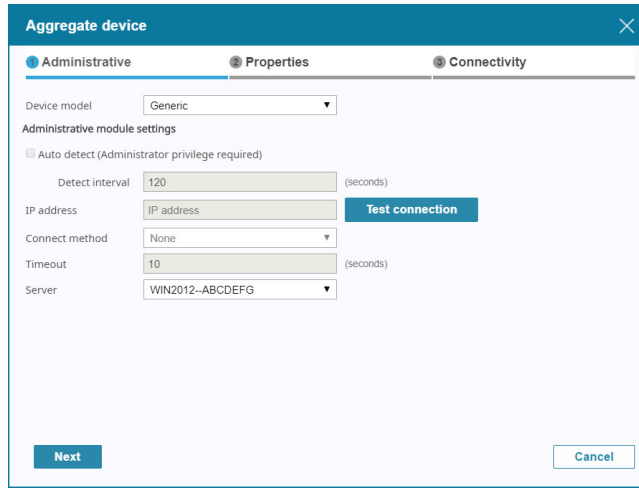
6. When you have finished with this page, click **Next**. The Blade page appears.



7. For each blade, you can specify its Department, Location, and Type, and provide a brief Description.
8. When you have finished, click **Save** to complete the procedure.

Adding an Aggregate Device

This item refers to adding Aggregate device into the CC2000 management system:



Note: See *Aggregate Device* on page 70 for an explanation of aggregate devices.

Follow the steps below to add an Aggregate Device.

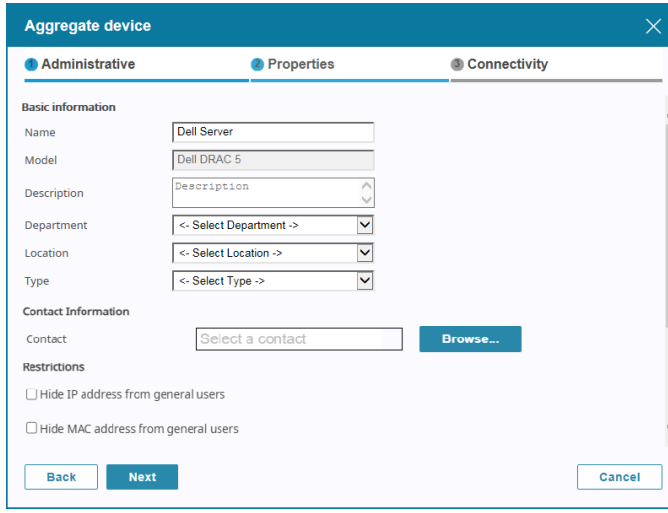
1. On the administrative page, select the Device Model from the drop-down menu and fill in the fields according to the information provided in the table below:

   Note:
   - The available fields depend on the selected Device Model.
   - Redfish-enabled HP iLO 5 and Redfish-enabled Dell iDRAC 8 are supported if you select *Redfish-enabled Device* as the Device Model.

Field	Information
Auto Detect	Enable Auto detect for the CC2000 to check if the device is online or not. Only a user with administrator privileges can enable this function.

Field	Information
Detect Interval	Set the detect interval by entering a value in seconds. This is how often the system shall automatically check if the Aggregate Device is online or not.
IP Address	Enter the Aggregate Device's IP address. Click **Test Connection** to confirm that the IP has been correctly detected.
Connect Method	For IPMI devices, connect method will be IPMI only. For Redfish-enabled Device, connect method will be HTTPS only. For everything else, select either SSH or Telnet from the drop-down menu.
Port	Enter the access port used to connect to it. Default SSH port: 22 Default Telnet port: 23 Default IPMI port: 623 Default HTTPS port: 443
Username / Password	Enter a username and password required to access the Aggregate Device.
Timeout	The amount of time to wait for a connection request to complete before canceling the request.
Server	Select the CC2000 unit that the Aggregate Device server is connected under.

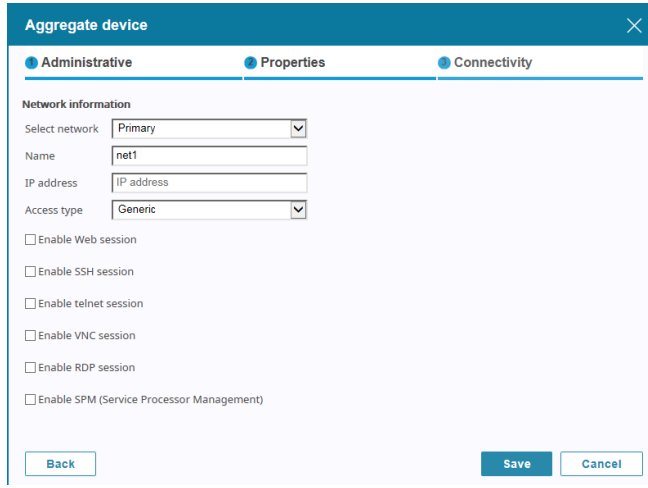
2. When finished, click **Next** for the Properties page.



3. 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. **Model:** The CC2000 recognizes the device model and fills in this field automatically. It cannot be edited. **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 *Category Management* on page 122). If you wish to assign this device to a department, drop down the list of departments (you have previously created), and click on the one you want the device to belong to. **Location:** For organizational purposes, you can establish location categories (West Coast, for example), and assign devices to them (see *Category Management* on page 122). If you wish to assign this device to a location, drop down the list of locations (you have previously created), and click on the one you want the device to belong to. **Type:** Use the drop-down menu to select the type of device it is.
Contact Information	Click **Browse** to add a contact. This field is optional. To create a new contact, go to **System** > **Contacts**.
Restrictions	**Hide IP Address from general users:** As an added security measure, if this feature is enabled, it prevents the device's IP address from appearing in the Device List when users log in via their browser. **Hide MAC Address from general users:** As an added security measure, if this feature is enabled, it prevents the device's MAC address from appearing in the Device List when users log in via their browser.
Power Control Options	Set the Power Control Options as outlined below: ◆ Check the box to enable confirmation for power operation ◆ Check the box to enable delay for power operation, and enter the Power on delay/ Power off delay fields in seconds.

4. When finished, click **Next** for the Connectivity page.



5. Fill in the fields according to the information in the table below:

Field	Explanation
Network Information	**Select network:** If the server for the aggregate device only has one network interface, select **Primary**. If it has more than one network interface, after you finish configuring the Primary one, come back to choose the additional ones and configure each of them in turn. **Name:** For convenience, each of the network interfaces can be named. **IP Address:** Enter the Virtual Host's IP address here. **Access Type:** Use the drop-down menu to select the access type.
Web Session	Check to enable web operation. The drop-down menu of the Operation column in the device list (upper screen) will reflect its availability. **URL:** To access the Aggregate Device server via the Web, enter the URL that will bring up its management page. **Enable SSO**: Check this box to enable single sign on functionality, and then select which credentials to use. ◆ Select *Use login user credentials* to use the same username and password as the CC2000 user account. ◆ Select *Use following credentials* and enter new credentials in the fields below. **Login name, Password:** Fill in these fields according to the Aggregate Device server's authentication and authorization procedures.

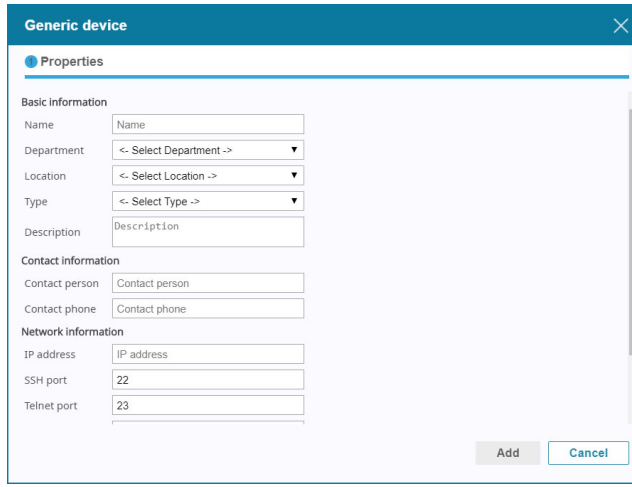
Field	Explanation
SSH/Telnet Session	Check to enable SSH/Telnet operation. The drop-down menu of the Operation column in the device list (upper screen) will reflect its availability. **IP address, Login name, Password, SSH / Telnet port:** To access the Aggregate Device server via an SSH / Telnet session, enter appropriate information into these fields according to the Aggregate Device server's authentication and authorization procedures. **Note:** An SSH session also requires entering login string information
VNC Session	Check to enable VNC operation. The drop-down menu of the Operation column in the device list (upper screen) will reflect its availability. **Port:** Enter the port number for the VNC session **Enable SSO**: Check this box to enable single sign on functionality, and then enter *View only* and *Full control* passwords.
RDP Session	Check to enable RDP operation. The drop-down menu of the Operation column in the device list (upper screen) will reflect its availability. **RDP Port:** Enter the port number for the RDP session. **Enable SSO**: Check this box to enable single sign on functionality, and then select which credentials to use. ◆ Select *Use login user credentials* to use the same account username and password as the CC2000 user account. ◆ Select *Use following credentials* and enter new credentials in the fields below.
SPM (Service Processor Management)	Check to enable SPM operation. The drop-down menu of the Operation column in the device list (upper screen) will reflect its availability. **SPM Method:** Select from the drop-down menu. Options are IPMI, HP iLO 2, HP iLO 3, HP iLO 5, IBM RSA II, IBM IMM, Dell DRAC 5, Dell iDRAC 6 Blade (modular), Dell iDRAC 6 Standard (monolithic), Dell iDRAC 8, Redfish-enabled Dell iDRAC 8 and Redfish-enabled HP iLO 5. **Port:** Enter the port number for the SPM session. **Login name, Password:** Fill in these fields according to the SPM server's authentication and authorization procedures. **Timeout:** Set the amount of time to wait for a connection request to complete before canceling the request.

6. When finished, click **Save** to complete the procedure.

For operations in the drop-down menu of the Operation column, refer to *Operation* on page 125.

Adding a Generic Device

This item refers to adding Generic device into the CC2000 management system:



Note: See *Generic Device*, page 71 for an explanation of generic devices.

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

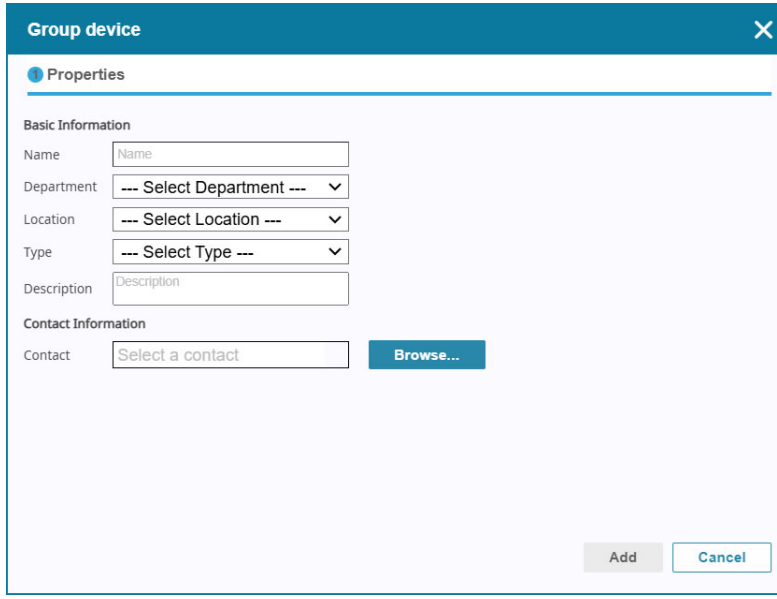
Field	Information
Basic Information	**Name:** Provide a name to identify the device. **Department:** For organizational purposes, you can establish department categories (R&D, for example), and assign devices to them (see *Category Management* on page 122). If you wish to assign this device to a department, drop down the list of departments (you have previously created), and click on the one you want the device to belong to. **Location:** For organizational purposes, you can establish location categories (West Coast, for example), and assign devices to them (see *Category Management* on page 122). If you wish to assign this device to a location, drop down the list of locations (you have previously created), and click on the one you want the device to belong to. **Type:** Use the drop-down menu to select the type of device it is. **Description:** If you wish to provide extra information to describe the device, enter it here. This field is optional.
Contact Information	Click **Browse** to add a contact. This field is optional. To create a new contact, go to **System** > **Contacts**.

Field	Information
Network Information	Fill in the fields according to the following information: ◆ If the Generic Device is to be accessed via a web browser, key its web (or IP) address in the URL field. ◆ If the Generic Device is to be accessed via Telnet or SSH, key in 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	As an added security measure, if *Hide IP Address from general users* is enabled, the device's IP address won't appear in the Device List. This setting is optional.

2. When you have finished, click **Add** to complete the procedure.

Adding a Group Device

This item refers to adding Group device into the CC2000 management system:



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

Field	Information
Basic Information	**Name:** Provide a name to identify the device. **Department:** For organizational purposes, you can establish department categories (R&D, for example), and assign devices to them (see *Category Management* on page 122). If you wish to assign this device to a department, drop down the list of departments (you have previously created), and click on the one you want the device to belong to. **Location:** For organizational purposes, you can establish location categories (West Coast, for example), and assign devices to them (see *Category Management* on page 122). If you wish to assign this device to a location, drop down the list of locations (you have previously created), and click on the one you want the device to belong to. **Type:** Use the drop-down menu to select the type of device it is. **Description:** If you wish to provide extra information to describe the device, enter it here. This field is optional.
Contact Information	Click **Browse** to add a contact. This field is optional. To create a new contact, go to **System** > **Contacts**.

2. When you have finished, click **Add** to complete the procedure.

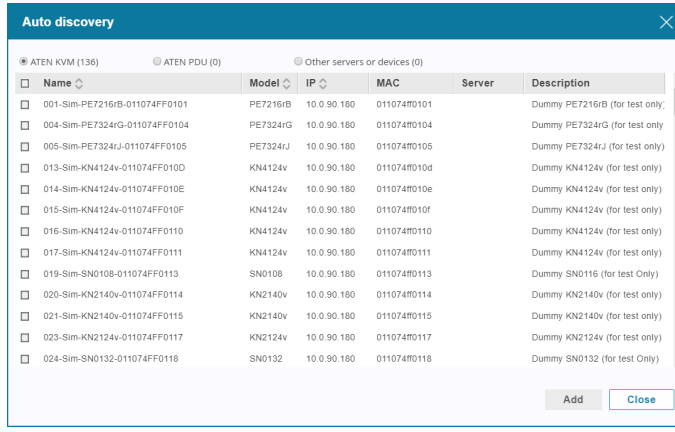
Note: 1. Refer back to *Group Device*, page 71, for an explanation of the differences between Aggregate and Group devices.

2. A port can belong to any number of Group devices. When a port is made part of a Group Device it retains the locked/unlocked status of the original physical port. If you lock or unlock any of these ports, all the ports – including the original physical port – change to the new locked/unlocked status.

Auto Discovery

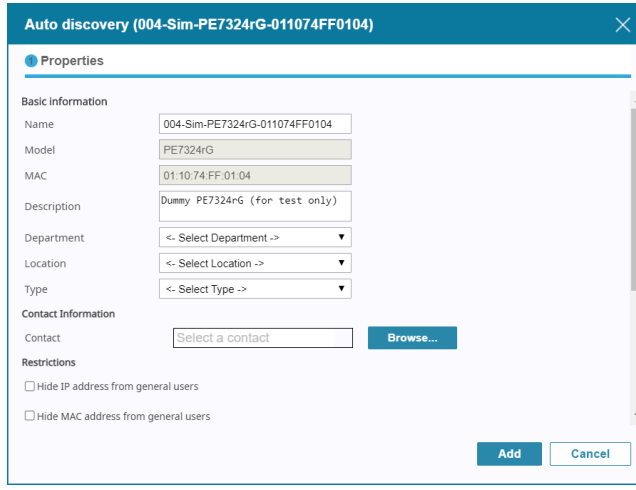
This item refers to adding devices into the CC2000 management system using the Auto discovery option.

The Auto discovery window is shown below:



Use the radio buttons to select what type of devices to display in the table (ATEN devices, ATEN PDUs or Other servers or devices).

Check to select the device you wish to add and click **Add**.



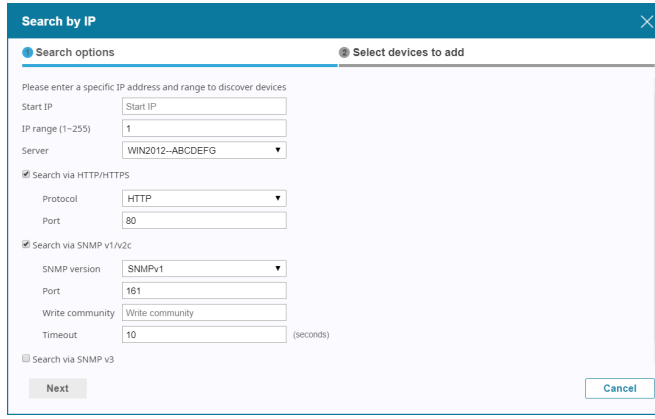
Fill in the Properties fields and click **Add**.

Refer to the sections above if you wish to modify any of the information fields.

Search by IP

This item refers to adding devices into the CC2000 management system using the Search by IP option.

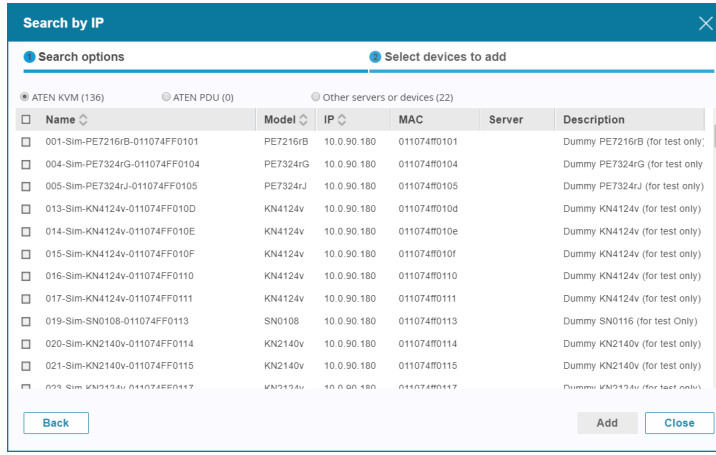
The Search by IP window is shown below:



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

Field	Information
Start IP	Enter the IP address to set the beginning of the search range.
IP Range (1~255)	Enter a number (1~255) to set the end of the search range.
Server	Use the drop-down menu to select the CC2000 server that the device is connected to.
Search via HTTP/HTTPS	If you check this box, use the drop-down menu to select the Protocol and enter the Service port number. This will search for devices that match the HTTP or HTTPS settings.
Search via SNMP v1/v2c	If you check this box, fill in the related SNMP information for the Port, SNMP version, Write community and Timeout. This will search for devices that use the SNMP v1/2c protocol.
Search via SNMP v3	If you check this box it will search for devices that use the SNMP v3 protocol.

2. Click **Next** and a table will appear with the results. Use the radio buttons to select the types of devices to be displayed in the table (ATEN devices, ATEN PDUs or Other servers or devices):



The *Description* column reveals one of three results:

Result	Information
Empty	No such device or server found.
IP Matched	A device or server has been found in CC2000 with the same IP address but of a different type.
Matched	A device or server has been found in CC2000 that matches both the IP address and type.

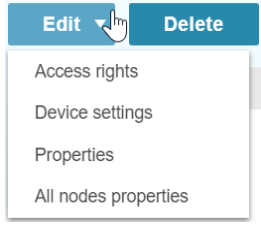
3. Check the check box of the device or server you would like to add and click **Add**.
4. Fill in the Properties fields and click **Add**.

   Refer to the sections above if you wish to modify any of the information fields.
5. When you have finished, click **Add** to complete the procedure.

Editing Devices

Follow the steps below if you wish to edit a device.

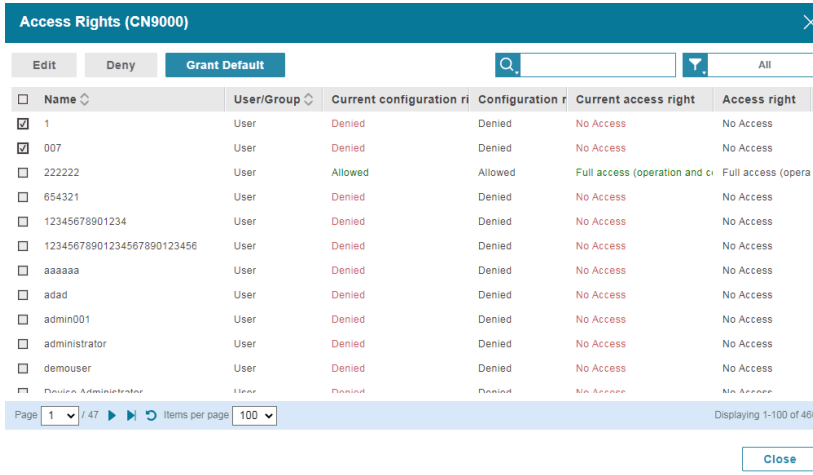
1. Check the device you wish to edit and click *Edit* for a drop-down menu:



2. Click to select what you wish to edit and refer to the following sections.

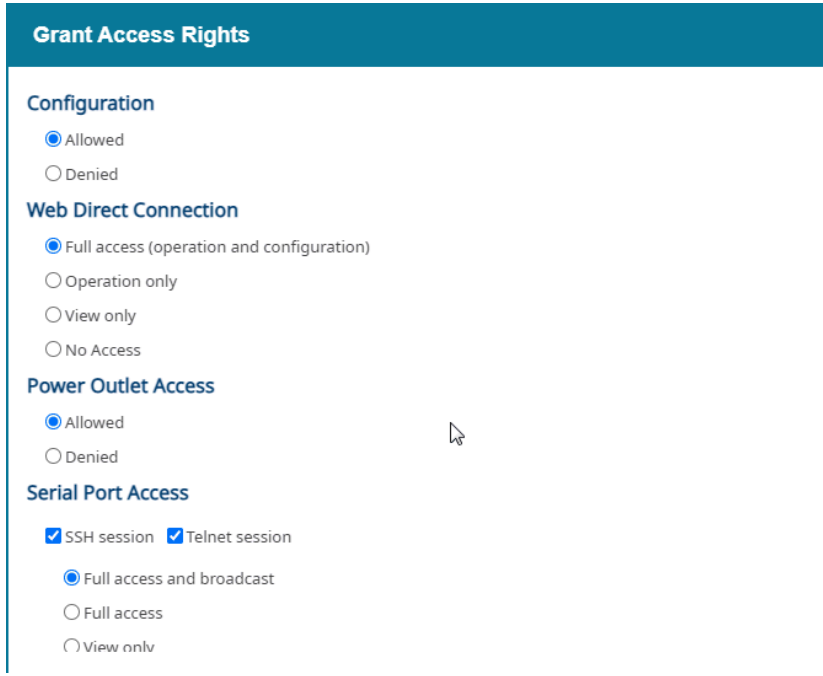
Access rights

Clicking *Access rights* will bring out a window. An example is shown:



To edit access rights of a user, check the user and click *Edit*. Another window will pop up. Access rights options will be different for different device type, refer to the sections below.

Note: You can also use the pencil icon to edit the access rights of a user when you move your cursor over a user row.To grant the same access / configuration rights to multiple users and/or user groups at the same time, click Grant Default. The following dialog box appears.



For details on each of the access / configuration rights that can be granted, please refer to the sections below.

■ ATEN KVM / Serial Console

The options for ATEN KVM devices is shown below:

Set the configuration rights for the user or group:

- **Allowed** – The user or group can configure the device's settings.
- **Denied** – The user or group cannot configure the device's settings.

Set the access rights for the user or group:

- **Full access (operation and configuration)** – The user or group can perform all configurations and operations.
- **Operation only** – The user or group can perform all operations.
- **View Only** – The user or group can only view the device.
- **No Access** – The user or group cannot access the device.

■ ATEN PDU

The options for ATEN PDU is shown below:

Set the configuration rights for the user or group:

- **Allowed** – The user or group can configure the device's settings.
- **Denied** – The user or group cannot configure the device's settings.

Check to set the access rights for the user or group:

- **Web** – The user or group can access the device via a web session.

■ APC PDU

The options for APC PDU is shown below:

Set the configuration rights for the user or group:

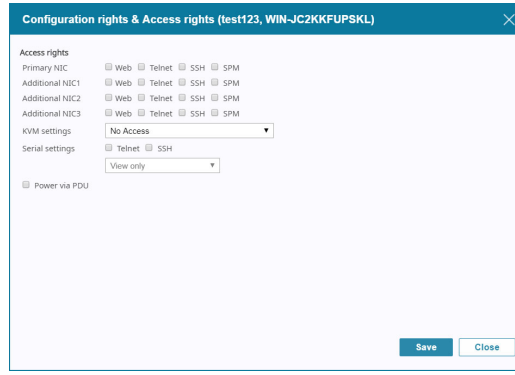
- **Allowed** – The user or group can configure the device's settings.
- **Denied** – The user or group cannot configure the device's settings.

Check to set the access rights for the user or group:

- **Web** – The user or group can access the device via a web session.
- **Telnet** – The user or group can access the device via a Telnet session.
- **SSH** – The user or group can access the device via a SSH session.

■ Virtual Host

The options for Virtual Host is shown below:



Check to set the access rights for the user or group:

- **Primary NIC** – Specify the network protocol(s) for this NIC.
- **Additional NIC1** – Specify the network protocol(s) for this NIC
- **Additional NIC2** – Specify the network protocol(s) for this NIC.
- **Additional NIC3** – Specify the network protocol(s) for this NIC.
- **KVM settings** – Select the access rights. Refer to the table below:

Rights	Explanation
Full access and VM (Read / Write)	The user can access the device (or specified ports on the device), view the screen and can perform I/O operations on it with the keyboard and mouse. The user also has read/write rights to use the virtual media function.
Full access and VM (Read Only)	The user can access the device (or specified ports on the device), view the screen and can perform I/O operations on it with the keyboard and mouse. The user also has read only rights for the virtual media function.
Full access	The user can access the device (or specified ports on the device), view the screen and can perform I/O operations on it with the keyboard and mouse.
View only	The user can access the device (or specified ports on the device), and view the screen, but cannot perform any operations on it.
No access	The user has no access to the device (or specified ports on the device). The device (or the specified ports) will not show up in the *Port Access* Sidebar or List.

- **Serial settings** – Select the network protocol(s) and the access rights (full access and broadcast, full access and view only).
- **Power via PDU** – Check/uncheck to enable/disable.

■ Blade Chassis / Aggregate Device

The options for blade chassis / aggregate device is shown below:

Check to set the access rights for the user or group:

- **Primary NIC** – Specify the network protocol(s) for this NIC.
- **Additional NIC1** – Specify the network protocol(s) for this NIC
- **Additional NIC2** – Specify the network protocol(s) for this NIC.
- **Additional NIC3** – Specify the network protocol(s) for this NIC.
- **KVM settings** – Select the access rights. Refer to the table below:

Rights	Explanation
Full access and VM (Read / Write)	The user can access the device (or specified ports on the device), view the screen and can perform I/O operations on it with the keyboard and mouse. The user also has read/write rights to use the virtual media function.
Full access and VM (Read Only)	The user can access the device (or specified ports on the device), view the screen and can perform I/O operations on it with the keyboard and mouse. The user also has read only rights for the virtual media function.
Full access	The user can access the device (or specified ports on the device), view the screen and can perform I/O operations on it with the keyboard and mouse.

Rights	Explanation
View only	The user can access the device (or specified ports on the device), and view the screen, but cannot perform any operations on it.
No access	The user has no access to the device (or specified ports on the device). The device (or the specified ports) will not show up in the *Port Access* Sidebar or List.

- **Serial settings** – Select the network protocol(s) and the access rights (full access and broadcast, full access and view only).
- **Power via PDU** – Check/uncheck to enable/disable.

Note: The access rights configured for an aggregate device takes priority over the access rights configured for each port of the aggregate device. The access rights for each port only become effective when the port is removed from the aggregate device.

■ Generic Device

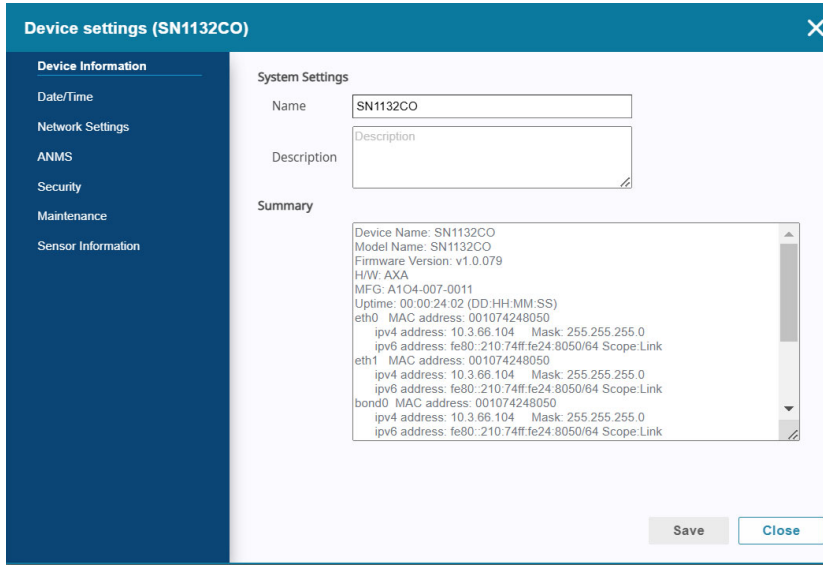
The options for generic device is shown below:

Check to set the access rights for the user or group:

- **Web** – The user or group can access the device via a web session.
- **Telnet** – The user or group can access the device via a Telnet session.
- **SSH** – The user or group can access the device via a SSH session.

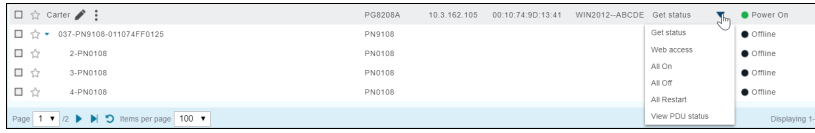
Device Settings

To configure an added device, check the device's checkbox and select **Device settings**. A window pops up, as shown below:



Use the side menu to select the configurable category, configure the appropriate fields and click **Save**. The available options may differ based on model and/or the configuration set to the device. For details of the configurable fields, refer to the device's manual.

If you wish to go to the device's configuration web page, click the drop-down menu under the **Operation** column and select **Web access**. An example is shown:



Properties

You can modify **Properties** of devices here. For information of the options available for different devices, refer to the corresponding device type in *Adding a Device* on page 75.

All Nodes Properties

Clicking this button brings up a page listing all of the items nested underneath the device. This page allows you to configure (or reconfigure) the Department, Location, Type, Description, and Trap Destination of each nested (child) item.

Deleting Devices

To delete a device(s), check to select the device(s) and click **Delete**.

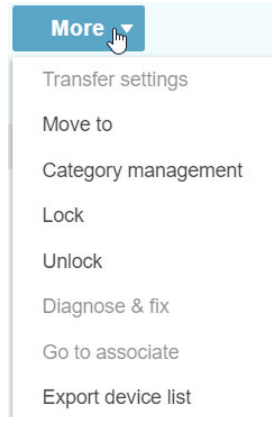
A confirmation message will pop up, click **Yes** to delete the device(s).

Note: 1. 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.

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

More

More configuration options are available here. Click *More* for a drop-down menu as shown:



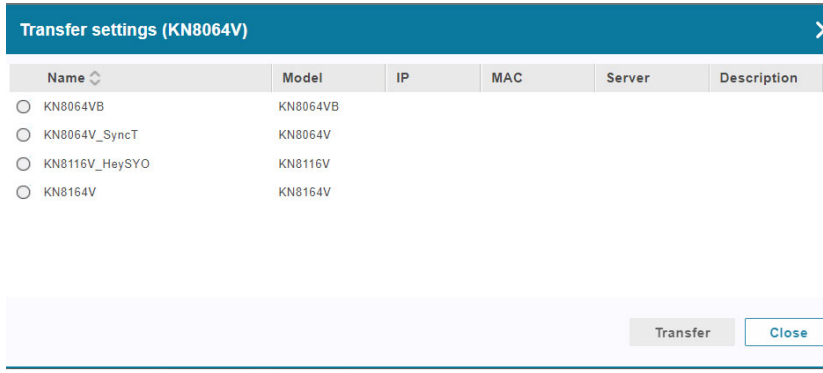
Note: You can also use the More icon ⋮ to access the More configuration options when you move your cursor over a user row.

The configurations are described in the following sections.

Transfer Settings

This function allows you to transfer the device settings and access rights from a source device to the selected device.

Check to select a device (e.g. device A) and click *Transfer* for the pop-up page shown below:



Choose a source device (e.g. device B) and click *Transfer* (bottom right-hand corner). A confirmation message will appear asking you to confirm the transfer. The CC2000 will transfer all device settings (excluding Device ID, model name and port number) and access rights of the source device (device B) to the selected device (device A). The transfer does not affect the settings of the source device.

Moving Folders and Devices

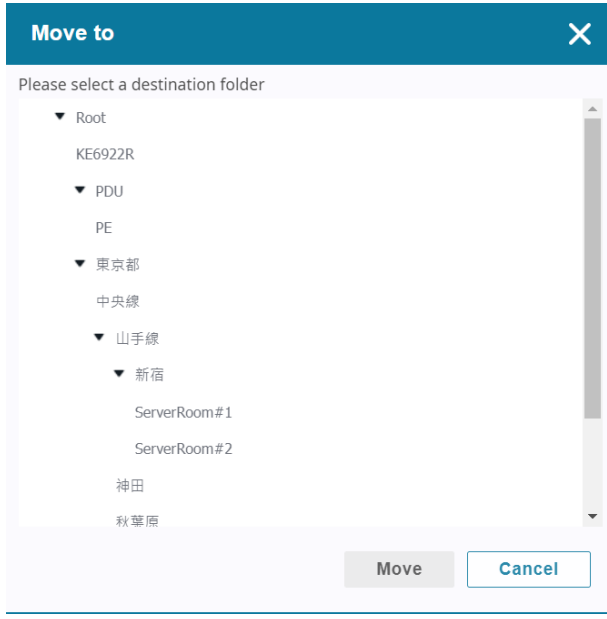
Use the *Move To* function to move and organize added devices.

To move one or more added devices:

1. In the device list, mouse over the target device or folder, and then click the **More** icon ⋮.

   Note: To move two or more devices/folders, click to select (tick) these items from the device list, and then click the More button.

2. From the pop-up menu, click **Move to**. A structure view appears.



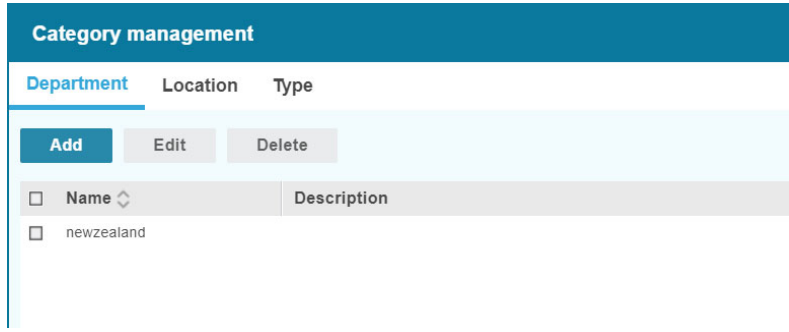
3. Click to select a location and click **Move** to finish the setting.

Category Management

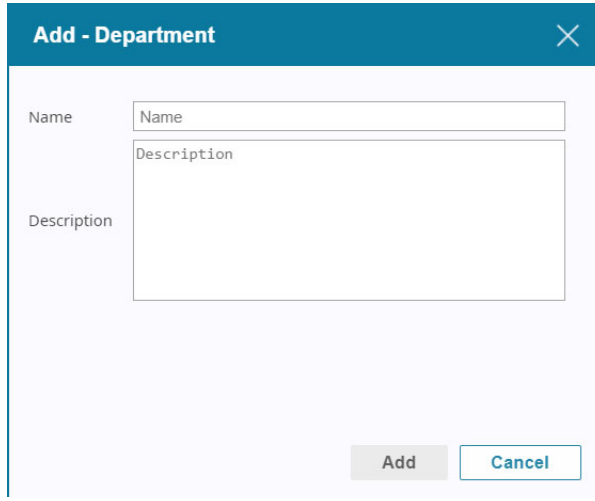
For convenience and ease of management, the devices can be organized into *Departments*, *Locations*, and *Types* categories. To use this organizational scheme, you would first create appropriate categories (such as *R&D* and *Manufacturing* under Departments; *East Coast Operations* under Locations; and *Power* under Types), and then assign devices to them (from the device's Properties page), as described in the sections that follow.

To create a Department, Location, or Type, do the following:

1. Click **More** and click to select **Category management**. A Category management page will pop up:



2. Click **Add**. The Add Department (or Location or Type) page will pop up:



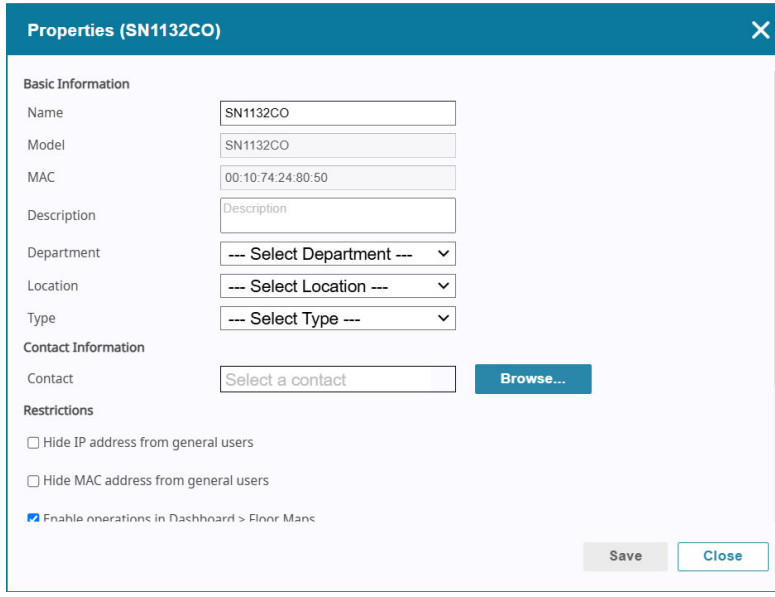
3. Fill in the Name and Description fields, and click **Add**.

To edit a Department, Location, or Type, check the item and click **Edit**. Edit the name and description fields and click **Save**.

To delete a Department, Location, or Type, check the item(s) and click **Delete**. A confirmation message will pop up, click **Yes** to delete the item(s).

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

1. Check to select a device/port on the Device page.
2. Click **Edit** and select **Properties**. A properties window will pop up as shown:



3. Identify where Department, Location and Type is, click their corresponding drop-down menu to select the category you wish to assign the device/port to.
4. Click **Save** to save the configuration.

Locking / Unlocking Devices

To make a port unavailable for monitoring, click **More** and then click **Lock**. A lock icon appears in the last column of the port table. A locked port does not take up a count toward the total number of nodes.

To unlock a device, check to select the device(s) on the upper screen. Click **More** and click **Lock** or **Unlock**.

Note:

- When physical devices are added to the CC2000 management system, their ports are locked by default.
- Ports are automatically unlocked when they are added to an Aggregate Device, but if you only want to use one or two of the device's physical ports, it is not necessary to go through the procedure involved in creating an Aggregate Device to do so. Simply select the target port(s) and click **Unlock**.

Diagnose & Fix

When a device encounters a problem (e.g. changing dongle port), you can click **Diagnose & fix** to fix the problem. The problem will be logged and a warning icon may appear in the last column of the device table (upper screen).

If a device can be diagnosed & fixed, a **Diagnose & fix** icon will appear in the last column of the upper screen (device) table.

Go to Associate

Devices/ports with the ⟨···⟩ icon at the end of their name means they have associated devices/ports.

Selecting this option or clicking the icon will bring you to the associated device/port table.

Associate is used for aggregate devices that can associate different ports on different devices in order to more easily manage ports.

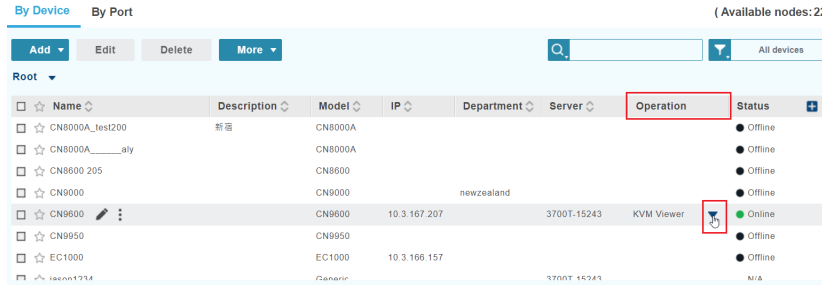
Export Device List

You can generate and export a device list along with information such as its name, description, model, IP address, MAC address, or location in a CSV file. Use one of the following methods to export a device list:

- Click the More button and then click **Export device list**.
- Click the ⋮ icon from an added device, and then click **Export device list**.

Operation

Depending on the selected device, various port operation methods are available for access and control. Click the drop-down menu in the Operation column to select an operation method, as explained below:



Get Status

To update the status of the device/server, click to select **Get Status**.

Shutdown

To shut down the device/server, click to select **Shutdown**.

Force Off

To force the device/server to shut down, click to select **Force Off**.

Restart

To restart the device/server, click to select **Restart**.

Force Restart

To force the device/server to restart, click to select **Force Restart**.

On

To turn on the device/server, click to select **On**.

WebClient Viewer

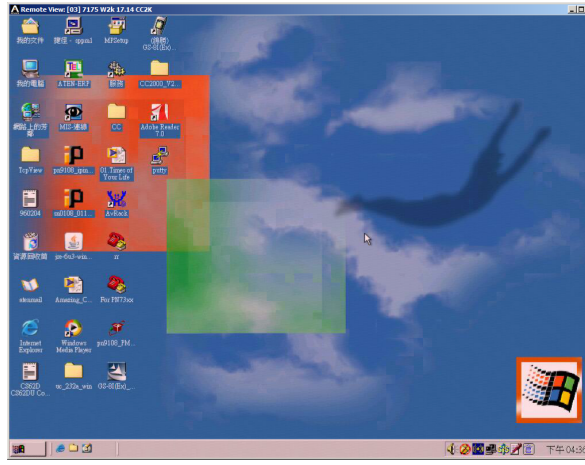
For KVM devices supporting WebClient Viewer, users can choose to launch KVM viewer sessions in a new tab directly on the browser without installing a Windows or Java Client app when clicking KVM Viewer from the drop-down menu. See p. 157.

CC Viewer / KVM Viewer / SN Viewer

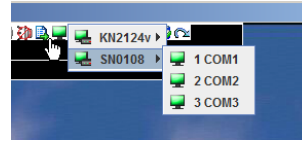
Clicking CC/KVM/SN Viewer from the drop-down menu opens viewer sessions directly to the ports of the selected device. The session opens a window with that device's port(s) on your desktop.

Controlling the viewers is the same as controlling the viewers opened from the KVM/SN devices.

For example, on an aggregate device that contains ports from a KN2124v KVM switch and an SN0108 serial device. When opening the CC Viewer, the first port of the KN2124v's in the aggregate device is displayed:



To switch ports in the viewer, open the hidden Control Panel (by hovering 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.

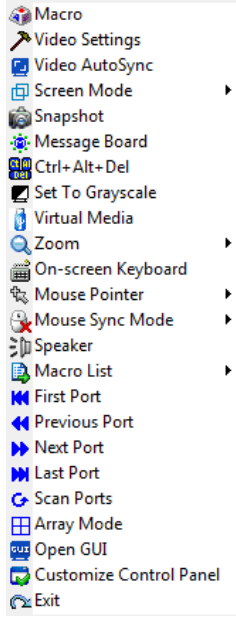


- In the list, select the device the port belongs to and click the port you want to access.
- The device or port name (port ID) displays in the CC Viewer title bar.
- The viewer window of each port has a hidden Control Panel. To switch to a different port on the device, bring up the port list and click the desired port.
- If the target device is associated with a PDU, additional power controls appear in the CC Viewer Control Panel.
- When you have finished with your session, open the Control Panel and select the *Exit* icon.

■ CC/KVM Viewer

The Control Panel of the CC/KVM viewer is hidden in the upper (default) or lower center of the screen, and becomes visible when you mouse over it. The panel consists of three rows: an icon row at the top, and two text rows below it:

- You can right-click your mouse in the text row area to bring up a menu-style version of the toolbar.



Control Panel Functions

The Control Panel functions are described in the table below.

Icon	Function
	This is a toggle. Click to make the Control Panel persistent – i.e., it always displays on top of other screen elements. Click again to have it display normally.
	Click to bring up the Macros dialog box (See the KVM device manual for more information).
	Click to bring up the Video Options dialog box. Right-click to perform a quick Auto Sync (See the KVM device manual for more information).
	Click to perform a video and mouse autosync operation. It is the same as clicking the Auto Sync button in the *Video Options* dialog box (See the KVM device manual for more information).
	Toggles the display between *Full Screen Mode* and *Windowed Mode*.
	Click to take a snapshot (screen capture) of the remote display (See the KVM device manual for more information).
	Click to bring up the Message Board (See the KVM device manual for more information).
	Click to send a Ctrl+Alt+Del signal to the remote system.
	Click to toggle the remote display between color and grayscale views.
	Click to bring up the *Virtual Media* dialog box. The icon changes depending on the status of the virtual media function (See the KVM device manual for more information).
	Click to zoom the remote display window.
	Click to bring up the on-screen keyboard (See the KVM device manual for more information).
	Click to select the mouse pointer type.

Icon	Function
	Click to toggle Automatic or Manual mouse sync. ◆ When the selection is *Automatic*, a green √ appears on the icon. ◆ When the selection is *Manual*, a red X appears on the icon. See the KVM device manual for more information.
	Click to toggle sound from the remote server to be heard on the client computer's speakers on or off. The "prohibited" symbol (a red circle with a diagonal bar) displays on the icon when the speaker is toggled Off.
	Click to control the power outlet of a connected PDU, between On, Off, and Restart. **Note:** This function is only available on aggregate devices with at least 1 KVM port and 1 outlet port.
	Click to display a drop-down list of *User* macros in order to access and run macros more conveniently than using the Macros dialog box (See the KVM device manual for more information).
	The Extended Displays icon allows you to select monitors to view in an extended display setup (See the KVM device manual for more information).
	Under an accessed port, click to skip to the first port accessible to the user on the entire installation without having to recall the Port Access page.
	Under an accessed port, click to skip to the first port accessible to the user that is previous to the current one without having to recall the Port Access page.
	Under an accessed port, click to skip to the first port accessible to the user that is after the current one without having to recall the Port Access page.
	Under an accessed port, click to skip to the last port accessible to the user on the entire installation without having to recall the Port Access page.
	Under an accessed port, click to begin Auto Scan Mode. The KVM over IP switch automatically switches among the ports that were selected for Auto Scanning with the *Filter* function (See the KVM device manual for more information). This allows you to monitor their activity without having to switch among them manually.
	Under an accessed port, click to invoke Panel Array Mode.
	Under an accessed port, click to recall the GUI.
	Click to bring up the Control Panel Configuration dialog box (See the KVM device manual for more information).

Icon	Function
	Click to exit the viewer.
	These icons show the Num Lock, Caps Lock, and Scroll Lock status of the remote computer. ◆ When the lock state is *On*, the LED is bright green and the lock hasp is closed. ◆ When the lock state is *Off*, the LED is dull green and the lock hasp is open. Click on the icon to toggle the status. **Note:** These icons and your local keyboard icons are in sync. Clicking an icon causes the corresponding LED on your keyboard to change accordingly. Likewise, pressing a Lock key on your keyboard causes the icon's color to change accordingly.

■ SNViewer

The SNViewer provides a Control Panel that is hidden at the center top of the screen, and becomes visible when your mouse moves over it. The panel consists of three rows: an icon row at the top, and two text rows below it:

Control Panel Functions

The Control Panel functions are described below and in the following sections:

Icon	Function
	This is a toggle. Click to make the Control Panel appear *Always On Top* – i.e., always displays on top of the SNViewer screen. Click again to have it display in *Auto Hide* mode– allowing it to only appear when the mouse is moved over it.
	Use this to copy the selected text on the screen.
	Use this to copy all text that is displayed on the screen.
	Use this to paste the copied text.
	Use this icon to toggle *Logging on / Logging off*. This starts a log file of characters sent from the serial device to the SNViewer. You must first create and import a text based log file (See the SN device manual for more information).
	Use this to browse for data files to import (See the SN device manual for more information).
	Use this to change the page encoding (See the SN device manual for more information).

Icon	Function
	Use this icon to enable broadcasting. Broadcasting allows you to access and make changes on a single port and the same changes will be made across all Broadcast Ports. Before using the broadcast function, set the *Broadcast Timeout* and *Broadcast Ports* (See the SN device manual for more information). For broadcasting to work, you must first access a port set as a Broadcast Port and then click the Broadcast icon on the control panel.
	Click to send a Break command.
	Use this to reset the terminal to its default settings.
	Click to bring up the Message Board (See the SN device manual for more information).
	Click to open a window and create a list of custom text macros (See the SN device manual for more information).
	Use this to change the font, color and other SNViewer settings (See the SN device manual for more information).
	Use this button to adjust the width of the SNViewer window.
	Click to exit the viewer.

■ WebClient Viewer

The WebClient Viewer provides access to the devices' ports directly on the browser without requiring Windows or Java Client app installation. Its control panel is explained below:

Note: To launch WebClient Viewer when clicking KVM Viewer, see page 157.

Control Panel Functions

Icon	Function
	This is a toggle. Click to pin the Control Panel – i.e., it always displays on top of other screen elements. Click again to have it display normally.
	Click to adjust the video settings (refer to the respective CC / KVM manual for details).
	Click to perform a video autosync operation.
	Click for a Screen Mode drop-down menu. Choose between *Full Screen Mode* and *Fit to Window*.
	Click to toggle the remote display between color and grayscale views.
	Under an access port, click to invoke Panel Array Mode (refer to the respective CC / KVM manual for details).
	Click for a drop-down menu of the available online port(s) and click to select the port you wish to connect to.
	Click to send a Ctrl+Alt+Del signal to the remote system.
	Click to access an on-screen English keyboard (refer to the respective CC / KVM manual for details).

	Click to select the mouse pointer type. **Note:** This icon changes depending on which mouse pointer type is selected (refer to the respective CC / KVM manual for details).
	Click for a menu of mouse sync modes (refer to the respective CC / KVM manual for details).
	Click to bring up the *Virtual Media* dialog box. The icon changes depending on the status of the virtual media function (refer to the respective CC / KVM manual for details).
	Click to toggle sound from remote server to be heard on the client computer's speakers on or off. The "prohibited" symbol displays on the icon when the speaker is toggled off.

Web Access

Clicking Web Access opens a browser session for the device/server on your desktop just as if you had opened your browser and logged into from the URL bar. An example is shown below:

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 show in the table until you leave the page and come back to it.

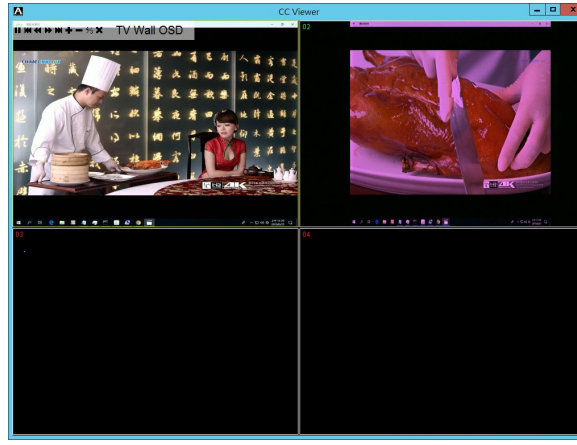
SSH / Telnet Session

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 serial device (SN0108, for example), with your browser and had chosen *Telnet* on the Main Web page.

Panel Array Mode

After you create a group device, you can launch panel array mode of the device by clicking the *CC Viewer* button (Operation column) and click the Start Panel Array icon in the control panel.

An example of the array display is shown below:



Use the icons hovering over the CC Viewer to adjust the panel array view settings.

A quick video reference is available in the link below:

https://www.youtube.com/watch?v=tbaQWK1vh60

SPM Session

Clicking **SPM** in the operations drop-down menu will bring up a window with 3 tabs: **System Information**, **Monitoring Information** and **Event Logs**.

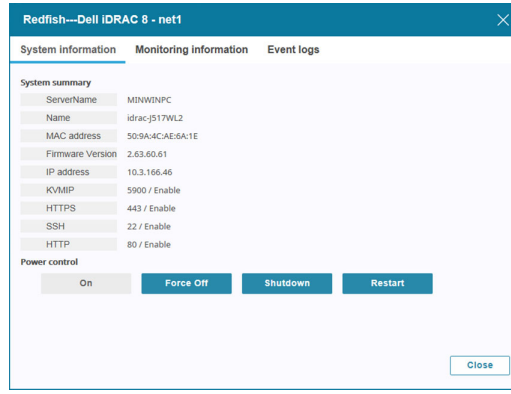
Note: The displayed information and options are different between the two supported Redfish-enabled Devices (HP iLO 5 and Dell iDRAC 8).

■ System Information

This tab displays the system information of the server.

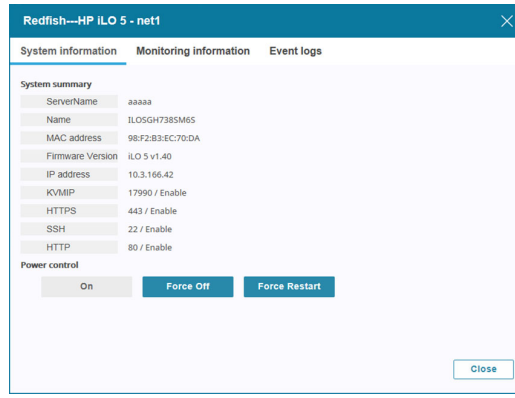
- **Dell iDRAC 8 Example**

  You can also turn the server **On**, **Shutdown**, **Force Off** and **Restart** here.



■ HP iLO 5 Example

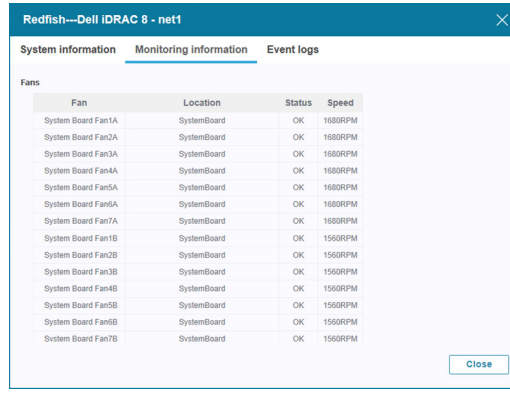
You can also turn the server **On**, **Force Off** and **Force Restart** here.



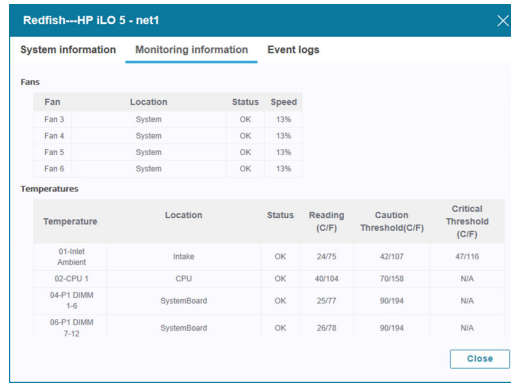
■ Monitoring Information

The information and the details being presented are different for the two supported Redfish-enabled devices.

- **Dell iDRAC 8 Example**

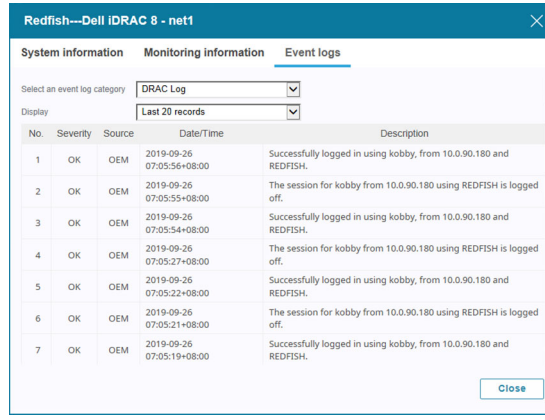


■ HP iLO 5 Example

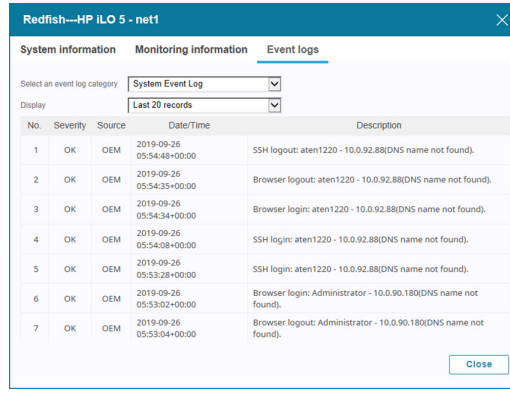


■ Event Logs

◆ Dell iDRAC 8 Example



■ **HP iLO 5 Example**



View PDU Status

Click **View PDU Status** in the operations drop-down menu to look up the following statuses for the selected device:

- general device status (voltage, current, power, power dissipation)
- sensor status
  - current sensor values (temperature, humidity, and/or pressure)
  - number of sensors
  - sensor status (open/close)
- bank status (voltage, current, power, power dissipation)
- outlet status (outlet name, on/off status, voltage, current, power, power dissipation)

Ports

Selecting **By Port** will list all ports in the system.

If you select a device in **By Device**, the lower screen will list all the ports of the added devices.

Port Column Headings

Heading	Explanation
Name	The name given to the port when it was added to the CC2000 installation.
Alias	If you gave the port an alias, the alias name appears here.
Port	The port's port number on the device it belongs to.
Port Type	Indicates the kind of device that the port belongs to.
Status	◆ For KVM ports, indicates whether the port is online or offline. ◆ For Serial ports, indicates whether the port is online or offline. ◆ For Power 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, therefore *N/A* (not applicable) displays in this field for Blade Chassis, and *Unknown* displays for individual blades.
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 port.

All the operations are the same as the device (*By Devices - General Operations* on page 68), except that configurations are at the port level, and it includes a **Launch Viewer** option.

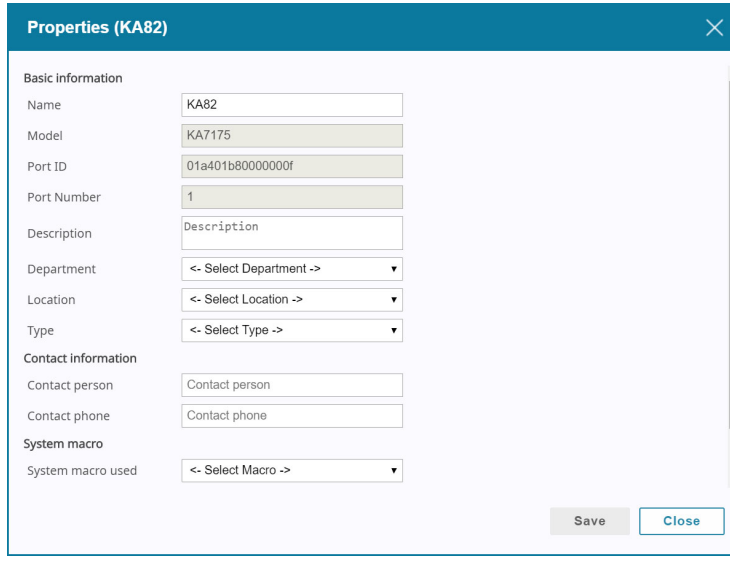
Launch Viewer

If you want to launch viewers to see the screen of the port, check the port and click **Launch Viewer**. The system will open the viewer in a new window (Java or Winclient).

Refer to *Operation* on page 125 for more information.

Properties - System Macro

On the edit properties page (Edit → Properties), everything is the same as the **Properties** page for devices (*Properties* on page 118) except that a System Macro item is present. An example is shown:

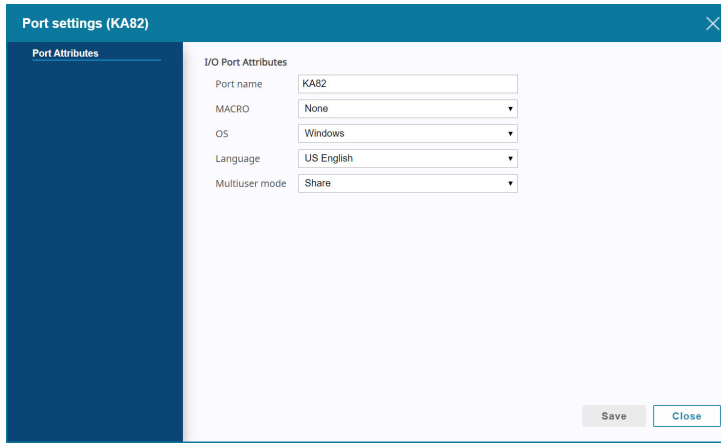


If system macros were created (in the CCViewer), click the drop-down menu to select the one you want.

This item only appears on ports that have servers connected to them.

Port Settings

Click *Edit* → *Port Settings* to edit Port Attributes. An example is shown:



The meanings of the attribute headings are described in the table below:

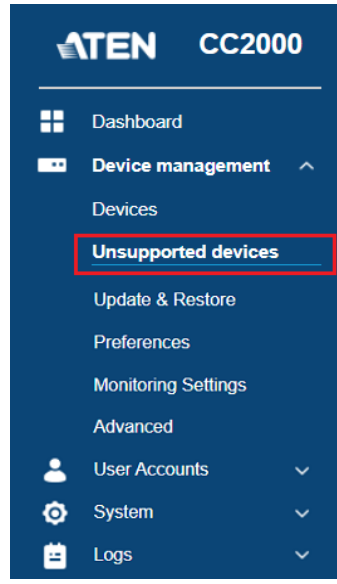
Heading	Meaning
Port Name	This is the name given to the port.
Macro	If system macros were created (in the device's viewer, e.g. WinClient), click the drop-down menu to select the one you want. When you save the changes, the macro will be sent to the server connected to this port and the server will run it.
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.
Multiuser Mode	This corresponds to the Access Mode setting on the original device (Share, Occupy, Exclusive). It defines how the port is to be 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 can be transferred to the user who operates its mouse and/or keyboard next. ◆ **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.

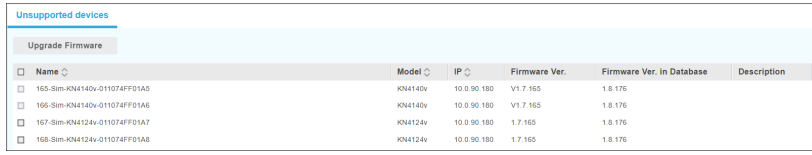
Unsupported Devices

Unsupported devices are ATEN/Altusen devices whose firmware level is not compatible with the current version of CC2000.

When unsupported devices appear in the system, the submenu will appear in the sidebar menu as shown below:



The interactive display panel will list the unsupported devices. An example is as shown:



To make these devices available for management under the CC2000, their firmware must be upgraded to the latest version. To do this, do the following:

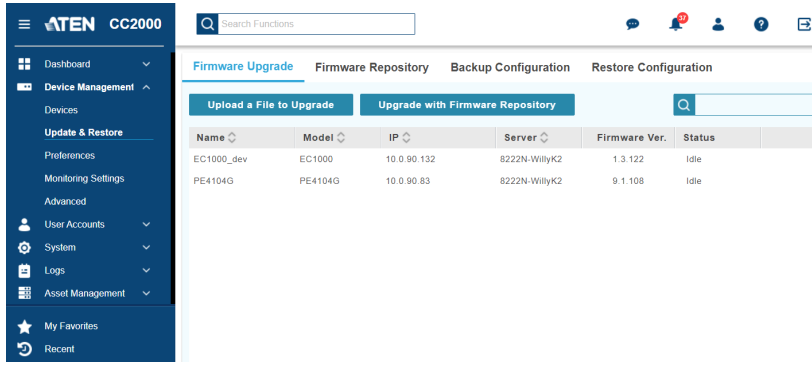
1. Add the device's firmware upgrade file to the CC2000. See *Firmware Repository* on page 149 on how to do this.
2. Once the device's firmware upgrade file is stored on the CC2000, its checkbox on this page becomes active. Check the checkbox.

3. Click **Firmware Upgrade**.
4. A confirmation message will pop up, click **Yes** to upgrade the device's firmware.

Once the firmware upgrade completes, the device is removed and will now appear in the upper screen of the Devices submenu.

Update & Restore

This submenu allows you to manage firmware and back up files.



The table here shows the ATEN and Redfish-enabled devices that have recently firmware upgraded.

The status column shows the firmware upgrade status of the device:

Status	Description
Idle	This status will show if you restart CC2000 when the device does not have any firmware upgrade lined up.
Waiting	The device is waiting for firmware upgrade.
Uploading	Uploading firmware upgrade file to the device.
Upgrading	Upgrading device.
Succeeded	Firmware upgrade/upload has just completed successfully.
Failed	Firmware upgrade/upload has just failed.

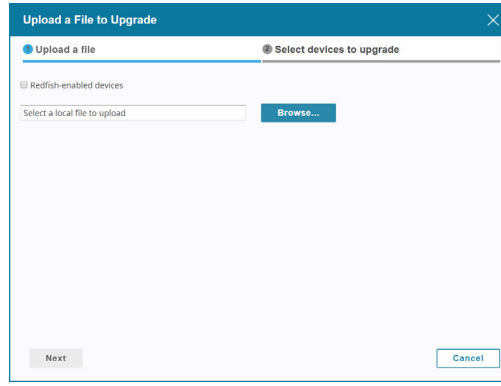
Firmware Upgrade

In this tab, you can choose one of the two ways to upgrade the devices.

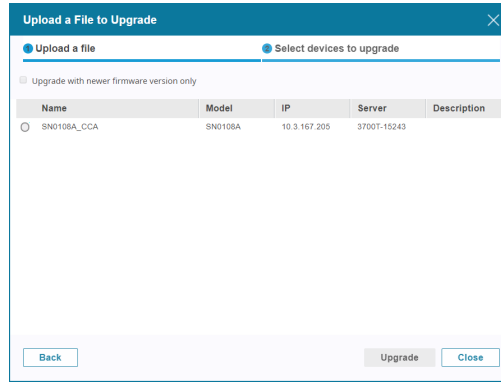
Upload a File to Upgrade

One of the ways to upgrade a device is **Upload a File to Upgrade**. Follow the steps below to upgrade this way:

1. Identify which device you need to upgrade and download its firmware from the ATEN website.
2. Click **Upload a File to Upgrade**, a window will pop up.



3. Click **Browse**, find the firmware file in your system and click **Next**.



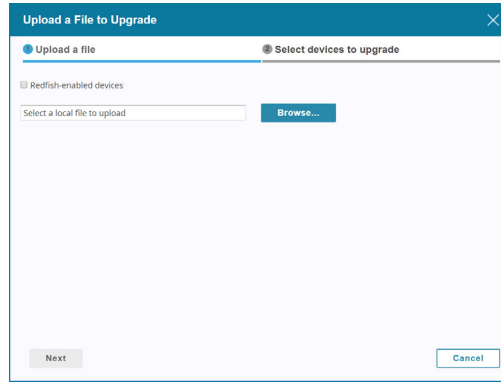
4. Select the device you wish to upgrade and click **Upgrade**.

5. A confirmation message will pop up, click **Yes** to upgrade the device's firmware.

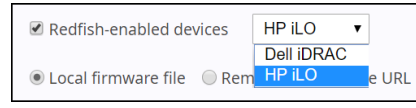
Upgrade Redfish-enabled Device

If you have a Redfish-enabled device, upgrade it using **Upload a File to Upgrade**. Follow the steps below to upgrade this way:

1. Identify which Redfish-enabled device you need to upgrade and download its firmware from the ATEN website.
2. Click **Upload a File to Upgrade**, a window will pop up.

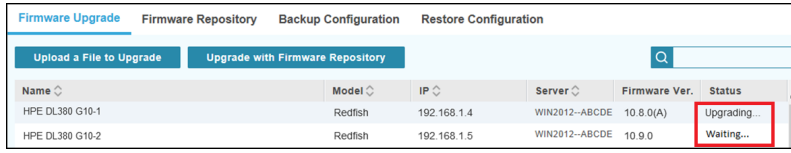


3. Check Redfish-enabled devices. A drop-down menu will appear to allow you to select the type of Redfish-enabled device.



4. Select the Redfish device type, click **Browse** to select the firmware file and click **Next**.
5. The devices belonging to this Redfish device type will appear in the list. Check the device(s) you wish to upgrade and click **Upgrade**.

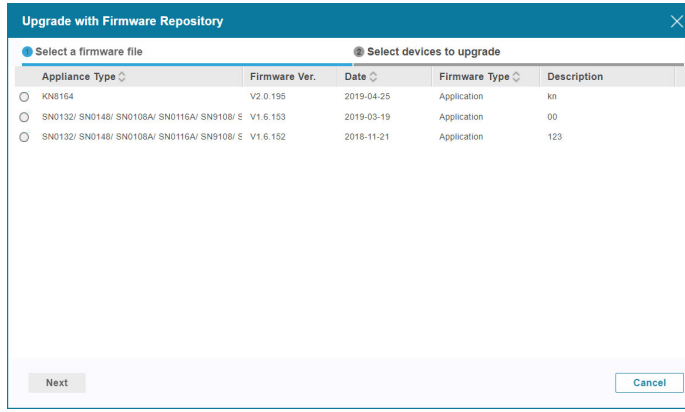
   While upgrading, the status column of the device(s) currently upgrading will show "Upgrading..." and the device(s) waiting will show "Waiting..."



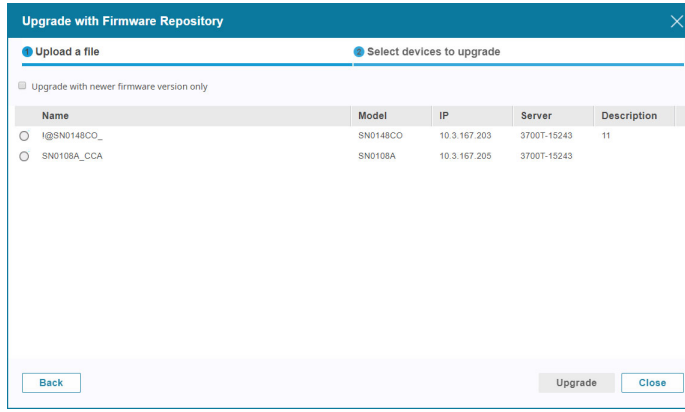
Upgrade with Firmware Repository

One of the ways to upgrade a device is **Upgrade with Firmware Repository**. Follow the steps below to upgrade this way:

1. Identify which device you need to upgrade and make sure the upgrade file is in the firmware repository. Refer to *Firmware Repository* on page 149 on how to upload firmware into firmware repository.
2. Click **Upgrade with Firmware Repository**, a window will pop up.



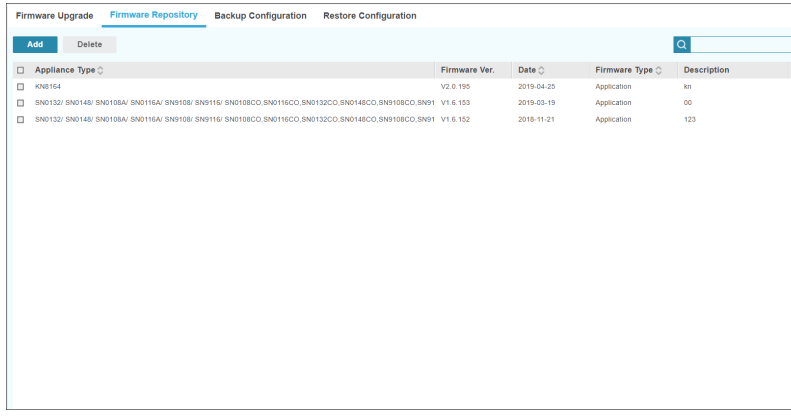
3. Select one of the firmware files and click **Next**.



4. Select the device you wish to upgrade and click **Upgrade**.
5. A confirmation message will pop up, click **Yes** to upgrade the device's firmware.

Firmware Repository

The Firmware Repository tab is shown below:



This page lists all the firmware upgrade files stored on the CC2000 – showing you at a glance the specific information about each of them.

By making the latest firmware upgrade files available for distribution from this single location, you can easily perform upgrades from within the CC2000, and

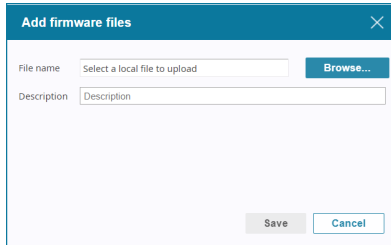
ensure that all the devices on your installation are operating at the same and most up-to-date firmware level.

Note: 1. Firmware upgrades can be also be performed under the Task Manager submenu. See page 250 for details.

2. New firmware upgrade packages are posted on our website as they become available. Check the website regularly to find the latest packages and information relating to them.

Adding Firmware Files

1. To add a firmware file to the list, click **Add**, a window will pop up:



2. Click **Browse** to select the firmware file.
3. Enter a description and click **Save**.

Note: If the firmware file isn't a CC2000 compliant one (even though it is compliant for the device in a stand-alone configuration), the CC2000 will not let you load it.

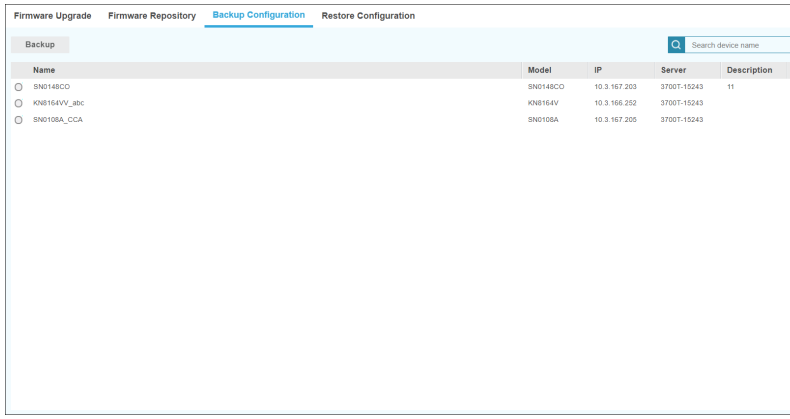
Deleting Firmware Files

To remove a firmware file(s) from the list, check the file(s) and click **Delete**.

A confirmation message will pop up, click **Yes** to delete the firmware file(s).

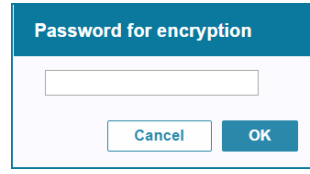
Backup Configuration

This tab will show the devices currently added to CC2000 and their information in the table.



To backup a device's configuration, select the device and click **Backup**.

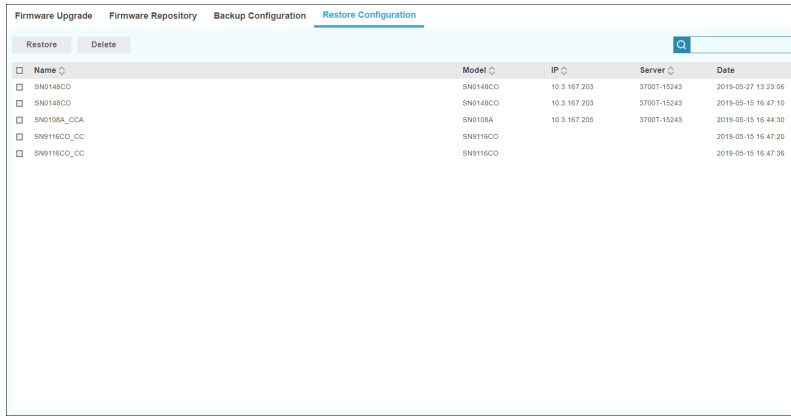
The system will ask if you would like to enter a password for encryption purpose.



Click **OK** to backup the configuration.

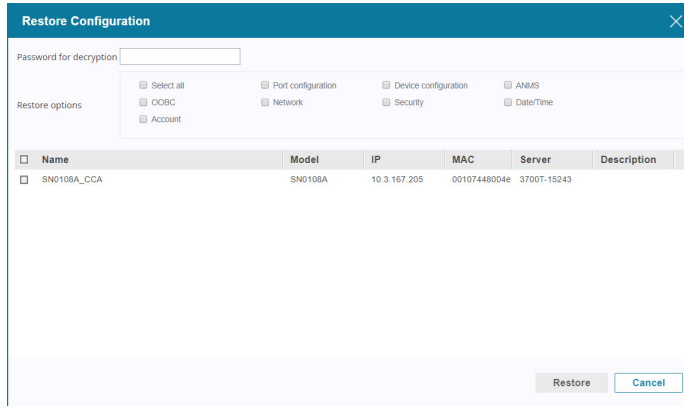
Restore Configuration

This tab will show the device configurations currently in CC2000 and their information in the table.



Restore

1. To restore configuration, check the configuration file from the table and click **Restore**. A window will pop up:



2. If you know the configuration file is password encrypted, enter the password into the password field.
3. Select the restore options by checking the checkbox(es).

4. Select the device you wish to restore by checking the device(s) you wish to restore.
5. Click **Restore**. A confirmation message will pop up, click **Yes** to restore.

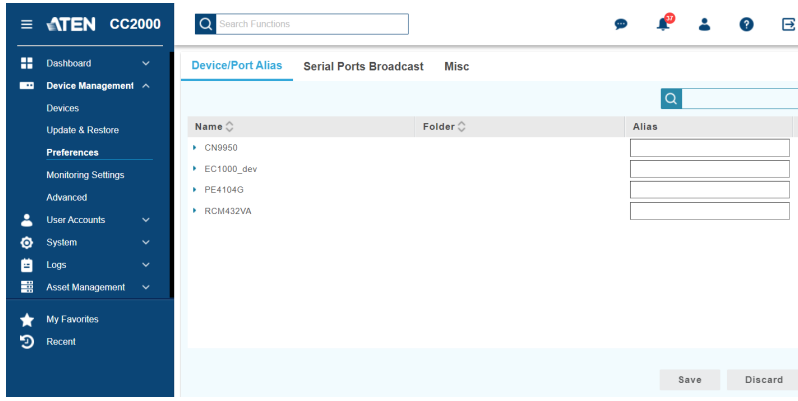
Delete

To remove a configuration file(s) from the list, check the file(s) and click **Delete**.

A confirmation message will pop up, click **Yes** to delete the configuration file(s).

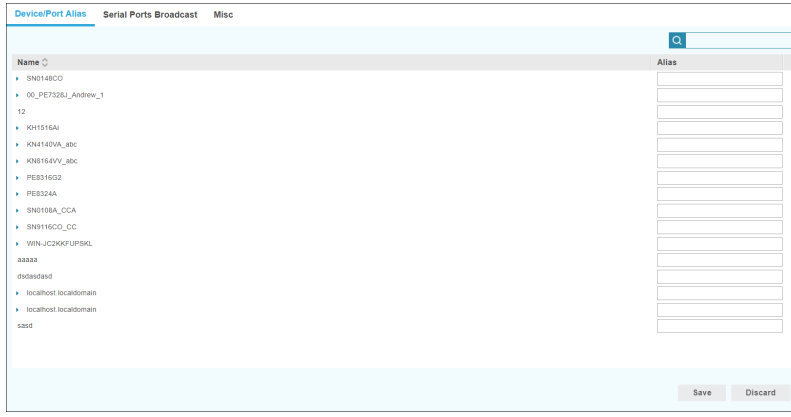
Preferences

This submenu allows you to configure user preferences in different tabs.



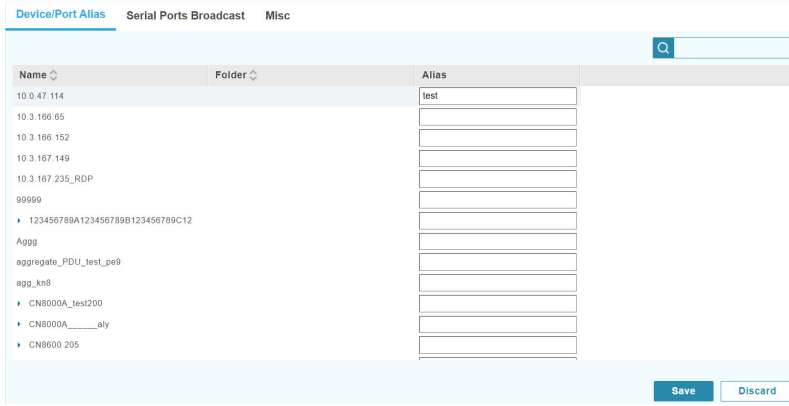
Device/Port Alias

This tab allows you to give your devices, ports, and outlets a nickname (as alias) that may help you identify these items.



- 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.

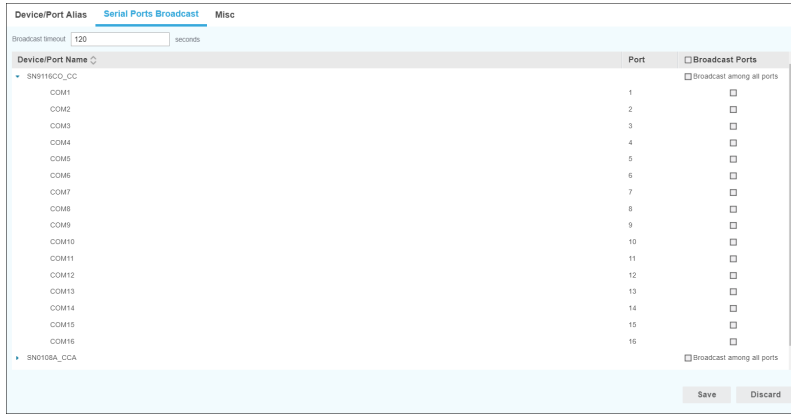
- Key the alias into the *Alias* field that corresponds to the device, port, or outlet and click **Save**.



Note: Aliases only appear for the particular user that creates them. Other users will only see the original name (or any aliases that they have created).

Serial Ports Broadcast

This tab allows you to select ports on a serial device to receive broadcast commands. Selecting multiple Broadcast Ports allows you to access and make changes on a single serial port and the same change will be made across all Broadcast Ports.



For broadcasting to work, you must access a Broadcast Port using the SNViewer and turn Broadcast on from the Control Panel. Refer to the SN user manual (under *Control Panel Functions*) for details.

Broadcast timeout: If there is no user input for the amount of time set here, the Broadcast function (to other ports) is automatically ended. Key in a value from 0–240 seconds. A setting of 0 (zero) has the same effect as disabling the function.

You can check **Broadcast Ports** on the last column of the table to check all serial ports in the table.

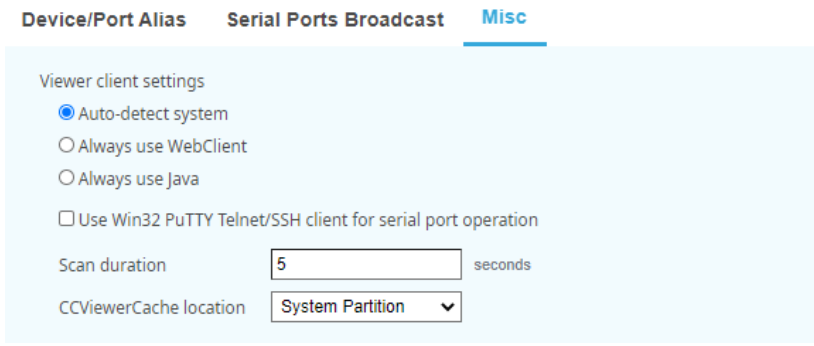
You can check **Broadcast among all ports** for a particular device to check all of its serial ports.

Expand the serial device to see all serial ports by clicking the arrowhead in front of the device. You can check individual port for broadcasting.

Note: The CC2000 will only list serial devices which are connected to a switch that supports broadcast ports.

Misc

This tab allows you to set viewer client settings, and change the path at which the CC Viewer cache is saved.



- If you choose **Auto-detect system**, the CC2000 will check to see if you logged in with IE or other browsers. If you logged in with IE, it will open with Windows Client Viewer when you access a device or port. If you logged in with a browser other than IE, it will open with WebClient Viewer, if supported, or Java Client Viewer.
- If you choose **Always use WebClient**, the CC2000 will always access devices via WebClient Viewer, if supported. When WebClient Viewer is not supported, Java Client Viewer will be used.

Note: For ATEN KVM over IP switches supporting WebClient Viewer, please refer to their product web pages for details.

- If you choose **Always use java**, the CC2000 will open the Java Client Viewer no matter which browser you logged in with.
- Checking the option **Use Win32 PuTTY Telnet/SSH client for serial port operation** will open the PuTTY Telnet/SSH client software when connecting to a serial device via CC2000 with IE.
- **Scan Duration:** sets the interval time for scanning ports when viewing ports in panel array mode.
- **CCViewerCache location** specifies the drive at which the CC Viewer cache is saved. By default, it is set to system partition for saving it at the system drive of the client PC.

Note: If you choose a drive that's non-existent, the CC Viewer cache will be saved at the client PC's system drive.

Event Monitoring

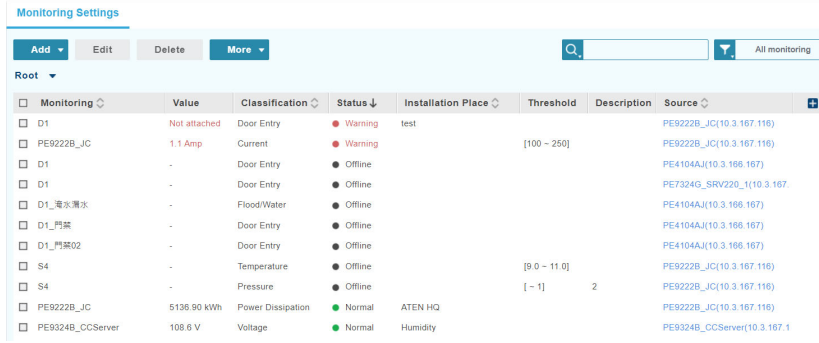
To monitor sensors (e.g. temperature, humidity, air pressure, door entries) or power status (voltage, current, dissipation, consumption), create *monitoring rules*. With monitoring rules, the CC2000 system monitors and records the status of ports and sensors over time, allowing you to:

- be notified of critical events (based on your specified criteria) via e-mail or messages
- view historical data
- export historical data

Note:

- The data size acquired for obtaining the value of a monitored device/port each time is 8 Bytes. Assuming CC2000 updates readings every 15 seconds, it will take around 4.5 MB a day for 100 monitoring rules (100 x 8 x 60/15 x 24 x 60).
- The system does not support backup of monitoring data to secondary/ redundant server. To back up monitoring data, create a backup task to another server. For details, see *Backup Primary Server Database*, page 252.

To access the Monitoring Settings page, go to **Device Management** > **Monitoring Settings**. This page appears.



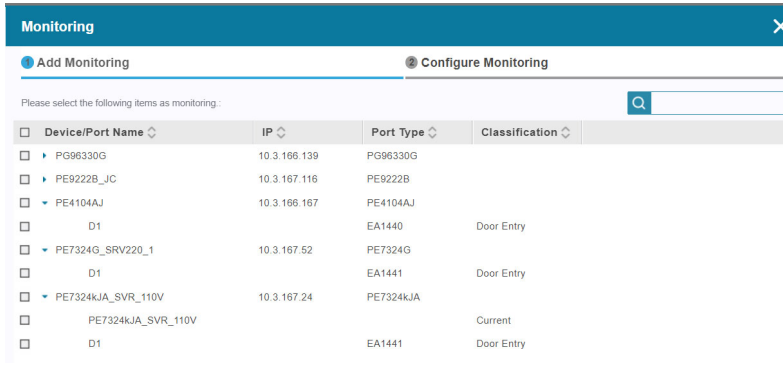
- On the Monitoring Settings page, you can find a list of created monitoring rules, along with the following information (column):
  - **Value:** This is the current value or status for the monitored equipment

- **Classification:** This field indicates the type of the monitored equipment.
- **Status:** This identifies the general status of the monitored equipment to be normal, off-line, locked, or warning.
- **Source:** This field indicates the model and IP address of the source device. Click on the source text (blue) to redirect to the corresponding device list page.

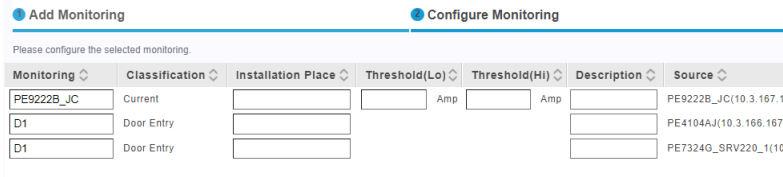
- To re-arrange the entries based on column headers, click the sign next to each column text.
- To hide displayed columns, click and select from the pop-up menu.
- The system supports up to 10,000 monitoring rules.

Creating a Monitoring Rule

1. Make sure have added the devices or equipment you wish to monitor into the device list (Device Management > Devices). For details, see *Adding a Device*, page 75.
2. Go to **Device Management** > **Monitoring Settings**.
3. Click Add and then select **Monitoring**. A list of available devices appears.



4. Click to select one or more devices and/or ports to create monitoring rules and then click **Next**. This screen appears.



5. Enter and edit the settings and descriptions as needed.

Note: To receive notifications when a threshold is exceeded or when a monitored door is open, make sure that related notification settings are configured. For more information about setting up notifications, see *Notifications*, page 222.

6. Click **Add**. The selected device(s)/port(s) appear in the monitoring list.

Note: If you create a monitor for a sensor port, check to make sure it is unlocked.

Editing a Monitoring Rule

- To edit a single monitoring rule, click .
- To edit two or more monitoring rules at a time, select (tick) these items from the Monitoring Settings page, and click Edit .

Adding a Folder

You can create folders and sub-folders to help you organize added monitoring rules by location or product series, depending on your needs. To add a folder, use one of the following method.

■ Using the add button.

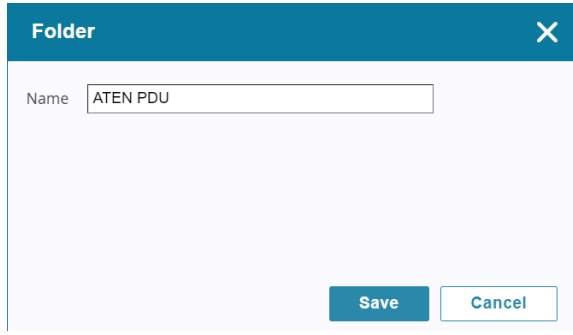
1. In the Monitoring Settings page, mouse over the target folder.
2. Click to open a selection menu and then select **Folder**.

■ Using the navigation menu

1. In the Monitoring Settings page, navigate to a level or folder where you wish to add a folder.

2. Click Add .

3. In the pop-up menu, click **Folder**. This screen appears.



4. Name the folder and then click **Save**.

   To edit a folder name, mouse over the target device, click and then select **Properties**.

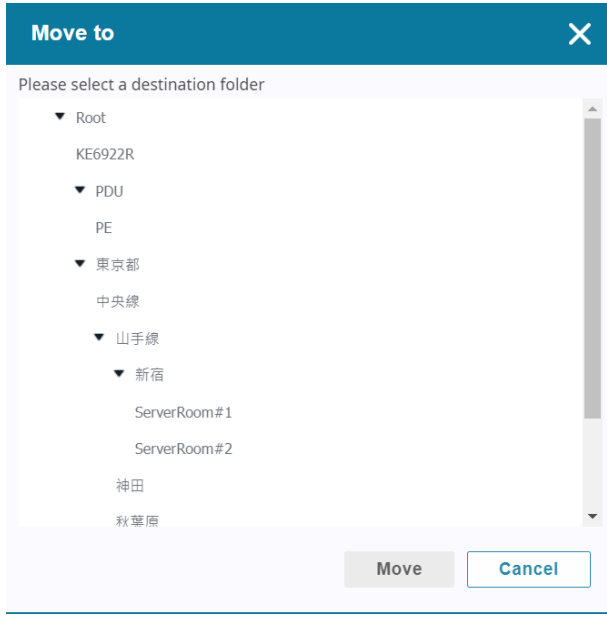
Moving the Added Monitoring Rules

To move added monitoring rules:

1. In the Monitoring Settings page, mouse over the target monitoring rule or folder, and then click the **More** icon ⋮.

   Note: To move two or more monitoring rules or folders, click to select (tick) these items from the Monitoring Settings page, and then click the More button.

2. From the pop-up menu, click **Move to**. A structure view appears.

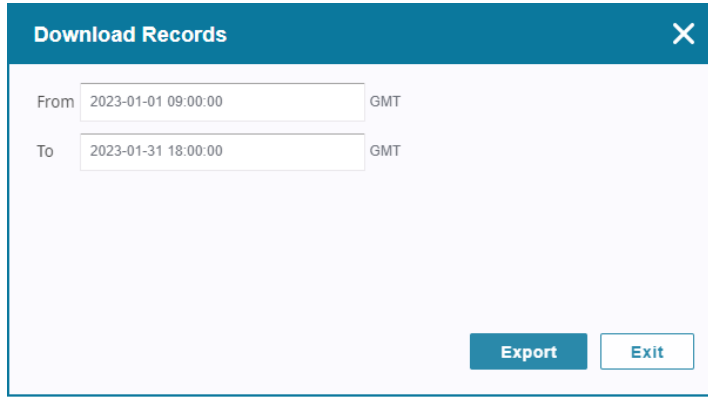


3. Click to select a location and click **Move** to finish the setting.

Exporting Records of Monitored Ports / Devices

To export data of monitored ports and devices in CSV files:

1. In the Monitoring Settings page, click to select one or more monitoring rules.
2. Click More and then select **Download Records**. This screen appears.

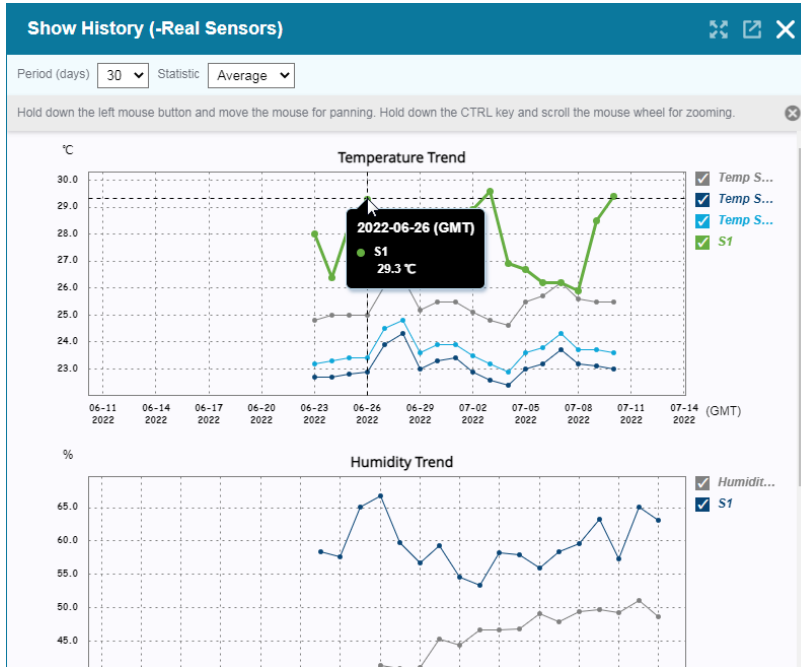


3. Click to specify the time period and click **Export**.

   The record will be exported in CSV format. If multiple monitoring rules are selected, the data for each monitor will be saved into separate CSV file and zipped together.

Viewing Charts of Monitored Equipment

You can generate and view trend charts (as shown below) of monitored ports and equipment to observe the changes using the Show History function.



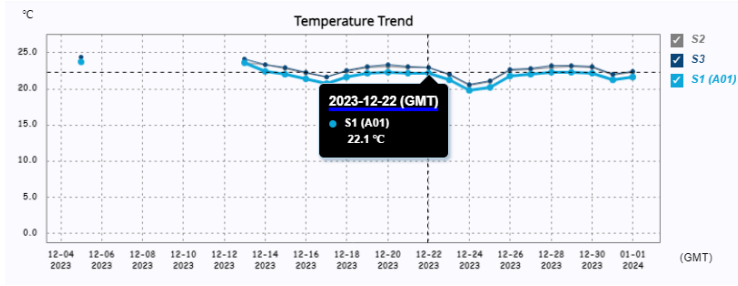
■ Generating Trend Charts

1. Select one or more monitors, and click More and select **Show History**. The Show History screen appears.
2. To change the display duration, click the **Period** drop-down menu and select a duration. The default is **30 days**.
3. To change the analysis, click the **Statistic** drop-down menu, and then select an option. The default is **Average**.

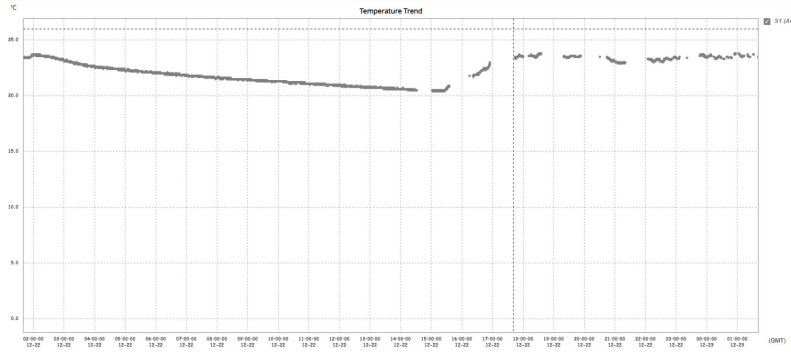
   Trend charts are immediately generated. Ports or equipment of the same type, e.g. temperature sensors on different devices, will be shown in one chart.

■ Reading the Analysis Charts

- To maximize the Show History screen, click  at the top-right corner.
- To display the value for a specific date, mouse over the dot in the chart.

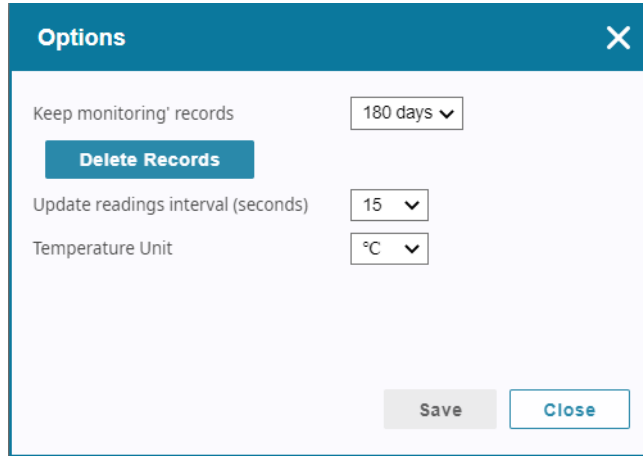


- To see figures on an earlier time, click and hold on the graph to drag the view left and right.
- To see a 24-hour chart, click on the date underlined in blue, for example, **2023-12-22 (GMT)**, a 24-hour chart appears.



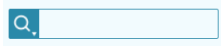
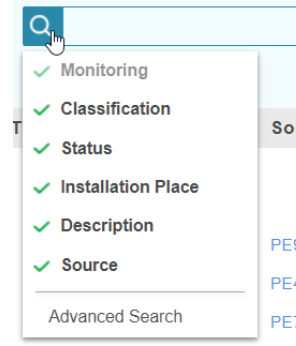
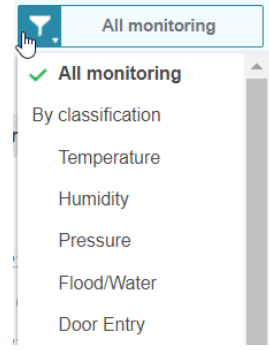
General Settings for Monitors

To change the retention period, temperature unit, detection interval (for obtaining the value of a monitored equipment), or to delete data of monitoring records, click More and select **Options**.



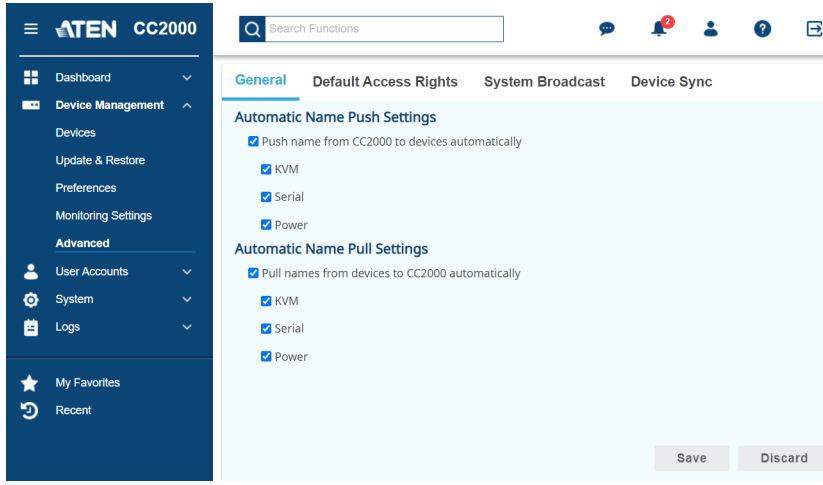
Locating Monitors Using Search and Filters

Use the search box and filters to quickly locate one or more monitors based on your specified criteria. You can access these features from the top-right corner of the Monitoring Settings page. The functions of the search box and filter are described below.

Control Element	Description
	Type in the search box to search monitors based on key words.
	Click on the search icon to change the search range. 
Advanced Search	Use advanced search to search all fields of the added monitors, including monitor name, description, device model, device IP address, department, server, and device status. To access this feature, click on the search icon and then select **Advanced Search**.
	Use the filter box to further filter your search by selected filter. Click on the filter search box and select a filter from the pop-up menu: 

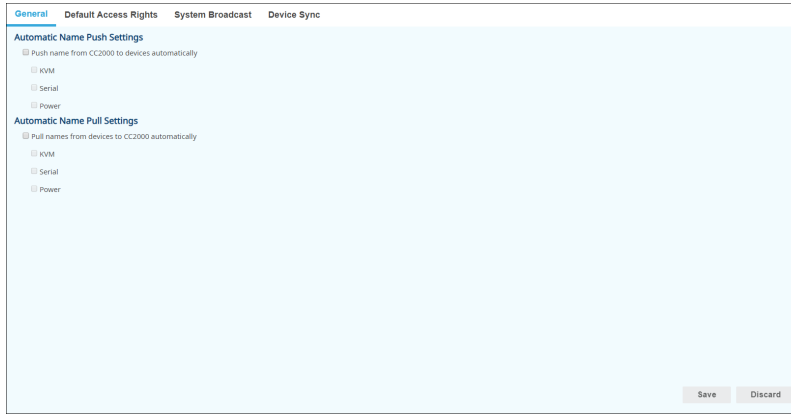
Advanced

The advanced submenu includes many tabs for advanced configurations.



General

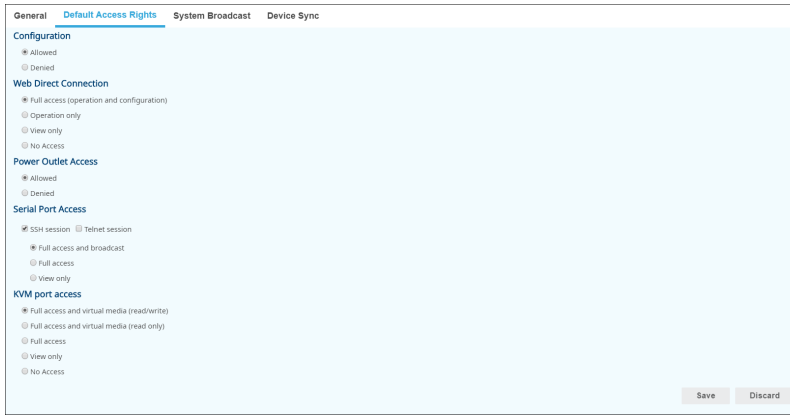
The General tab is as shown below:



This page lets you configure automatic syncing of names between the CC2000 and the installed devices. Check the boxes for the features you want to enable, then click **Save**.

Default Access Rights

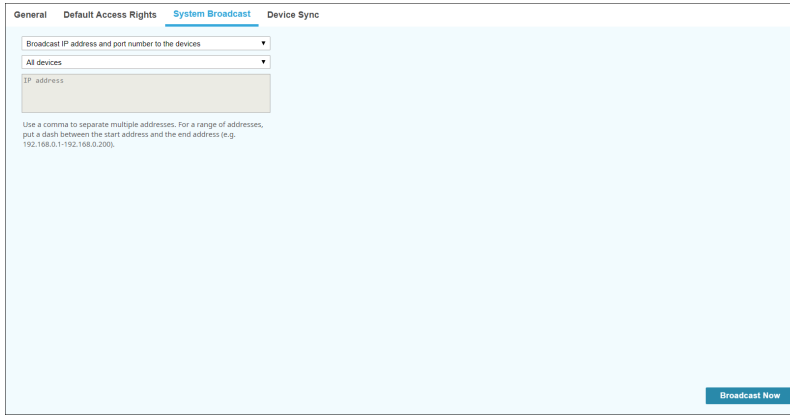
The Default Access Rights tab is as shown below:



This page allows you to set the default access rights for all new devices added to the CC2000 installation.

System Broadcast

The System Broadcast tab is as shown below:



Broadcast IP address and port number to the devices

Before a device can communicate with the CC2000, its ANMS settings have to specify the CC2000's IP address and device management port number.

Selecting this option from the top drop-down menu allows the CC2000 to broadcast its IP address and device management port number to the devices connected to it on its network, which automatically sets them on the devices (instead of having to set them manually on the device itself). This is done the first time that you connect a device to the CC2000 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 a network segment that can be reached by CC2000 (VPN will not work). UDP uses port 18768 – make sure that the network settings for computers that the CC2000 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 CC2000.

3. If you change CC2000s, you must use the ANMS settings page to specify the IP Address and port number.

On the next drop-down menu, select **All Devices** or **Specific IP Address**. If you choose **Specific IP Address**, enter the IP address in the next field.

Click **Broadcast Now** to start broadcasting.

Broadcasting IP Address or Port Number Changes to Devices

This feature is used when the CC2000's IP address and/or device management port number changes.

Selecting this option from the top drop-down menu allows the CC2000 to broadcast its 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 a network segment that can be reached by CC2000 (VPN will not work).

2. For heightened security, the receiving devices will only accept UDP broadcasts from the CC2000 that originally initialized them.

On the next drop-down menu, select **All Devices** or **Specific IP Address**. If you choose **Specific IP Address**, enter the IP address in the next field.

Click **Broadcast Now** to start broadcasting.

Device Sync

Use this function to sync device names between the selected device(s) and the stored names on CC2000.

1. Go to **Device Management** > **Advanced**. The General page appears.
2. Click the **Device Sync** tab. This page appears.

3. Click the drop-down menu to select an option.

- **Sync names from CC2000 to devices:** Push the names from CC2000 to the selected devices.
- **Sync names from devices to CC2000:** Pull the names from the selected devices to CC2000

4. Click to select one or more devices.
5. Click **Sync Now**.

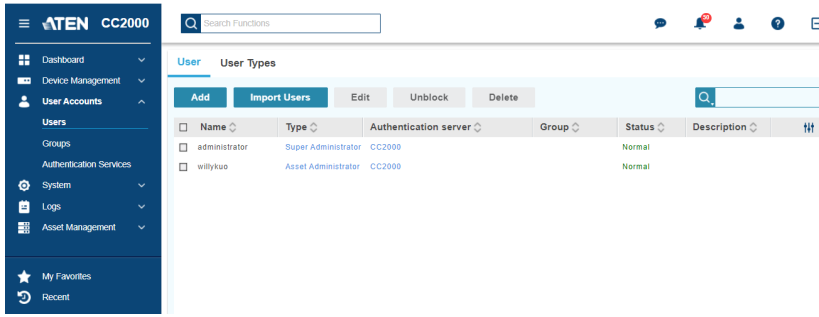
Chapter 6
User Management

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 CC2000 (internal) or via an external authentication server

Below is the displayed page when User Accounts is selected:

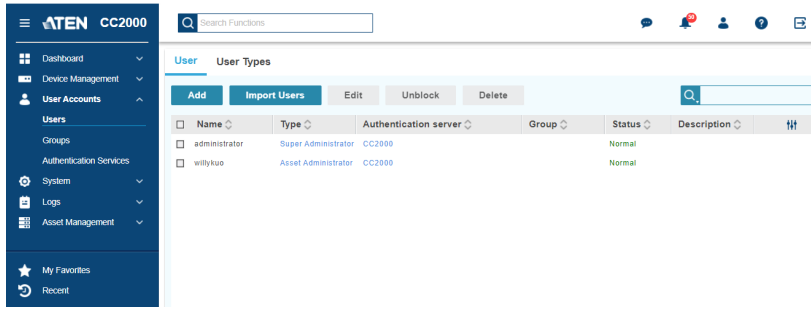


The submenus include Users, Groups, and Authentication Services.

Note: The User Accounts page access is for Super Administrators, System Administrators, User Administrators and Auditors. Auditors can only view the items in this menu.The maximum numbers of users and user groups that can be created are 4096 and 512, respectively.

User Accounts

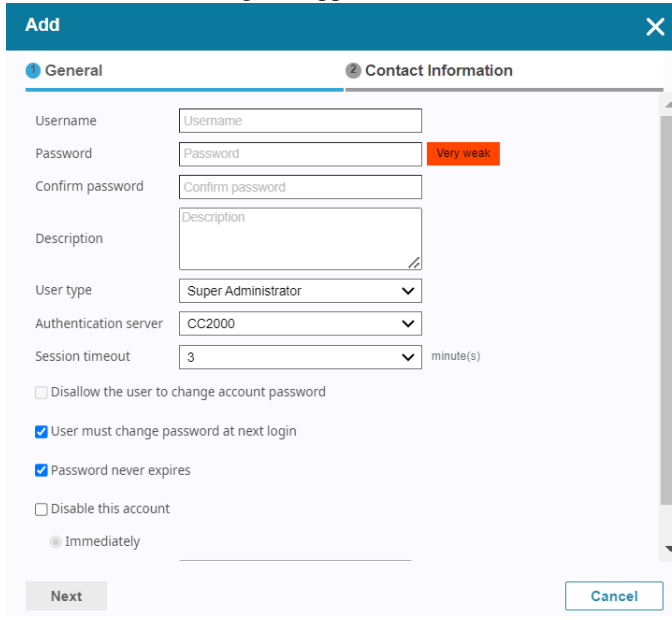
The Users submenu looks similar to the one below:



User

Adding a User Account

1. Go to **User Accounts** > **Users**.
2. Click **Add**. This dialog box appears.

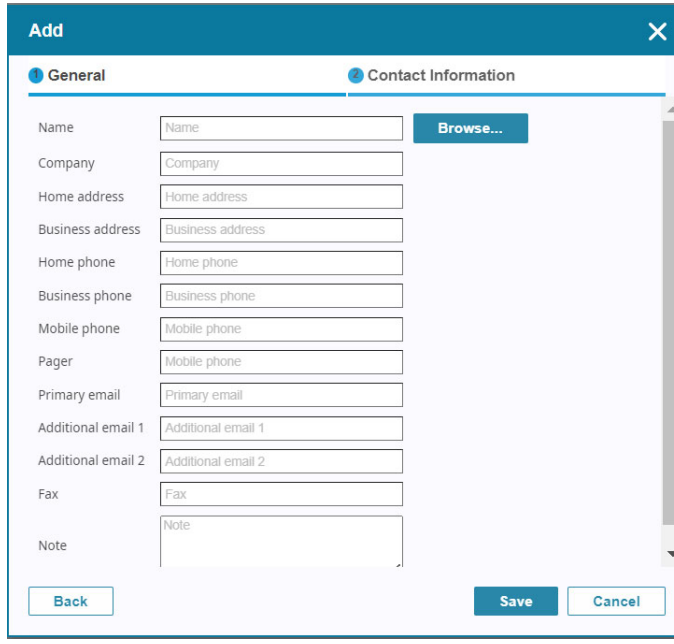


3. Enter the required information in the appropriate fields. A description of each of the fields is given in the table below:

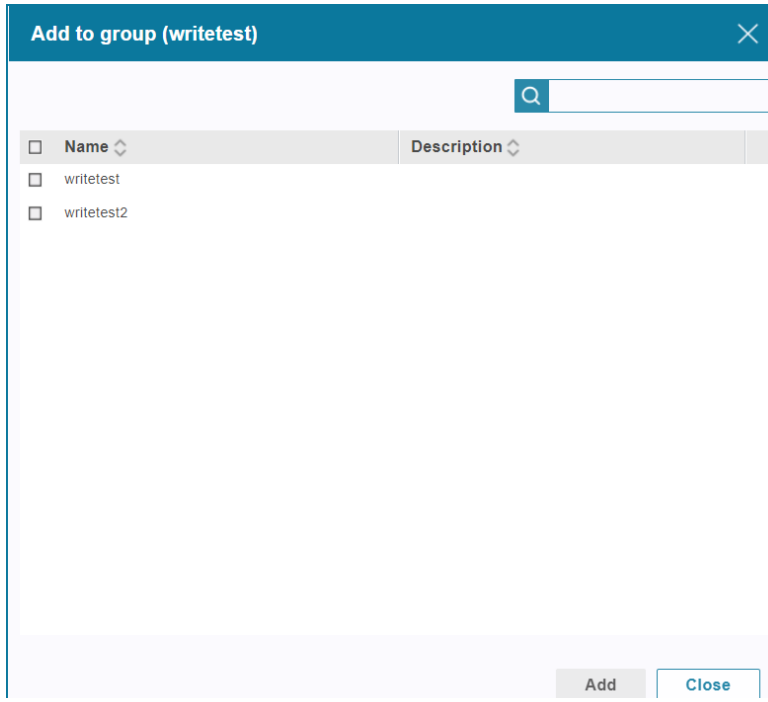
Field	Description
Username	**Internal (CC2000) Accounts:** A maximum of 32 English alphanumeric characters is allowed. The minimum number of characters is based on the CC2000's account policy settings (see *CC2000's Built-in Authentication Service*, page 204). **External Authentication:** The Login name 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 CC2000 management system, therefore the access rights need to be set in the CC2000.
Password / Confirm password	Enter a password of up to 32 alphanumeric characters and confirm the password.
Description	Additional information about the user that you may wish to include. A maximum of 256 Bytes is allowed.
User type	Click the drop-down menu to select the User Type you want to assign the new user to. See p. 181 for information about User Types.
Authentication server	For authentication by the CC2000, leave the selection as is. For authentication by an external authentication service, drop down the list to select the one you wish to use. **Note:** Before you can make this selection, an external authentication server must first be added. See *Adding a Third-party Authentication Server*, page 192, for details.
User base RDN	If the authentication server is an LDAP server, the user's base RDN setting must be in this field.
Session Timeout	If you want to have a login session time out after the user has been idle for a specified amount of time, select a time in the drop-down menu. The default is 3 mins. If you don't want to have a login session time out after the user has been idle for a specified amount of time, select *Never* in the drop-down menu. **Note:** This setting takes effect upon the user's next login. **Apply the session timeout to all users:** Select this option to apply the timeout setting to all users. The setting is applied immediately once you save the changes in the Properties window. If you open the Properties window again, the option will appear unchecked. **Note:** This option is only available when editing the properties of an existing user.

Field	Description
Other Information	Check the checkbox(es) for the extra policies governing this account.

4. Click **Next** for the personal information page. The information entered here is to help identify the user only. You may browse for contacts that you have created.



5. Click **Save** to save the information. The system will bring you to the Add to Group page where you can add the user to group(s).



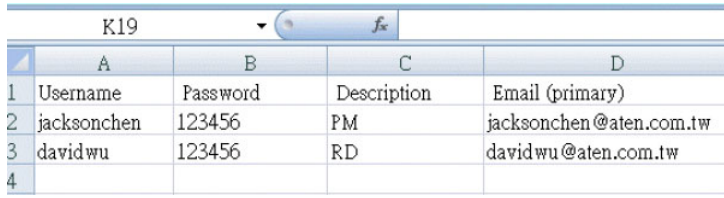
6. Check the group you wish the user to be added to and click **Add**.
7. Click **Close** to complete the process.

Importing User Accounts

If you have many user accounts to add you can simplify this process by using the **Import Users**. Clicking this button lets you import a previously saved users list saved using **.csv* format.

To create the list, do the following:

1. Create a spreadsheet with a list of users using the following format to define the data for each user's account:



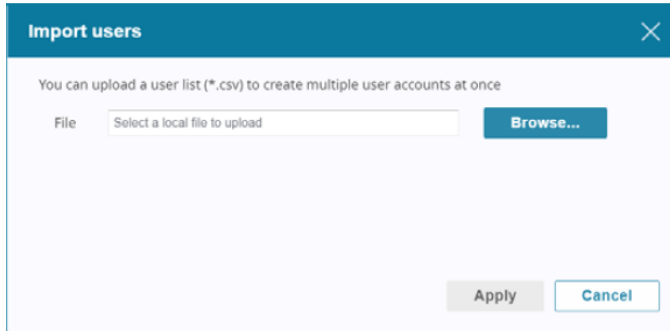
	A	B	C	D
1	Username	Password	Description	Email (primary)
2	jacksonchen	123456	PM	jacksonchen@aten.com.tw
3	davidwu	123456	RD	davidwu@aten.com.tw
4				

Note: Make sure there's a space between *Email* and *(primary)*.

2. Save the spreadsheet as a **.csv* file.

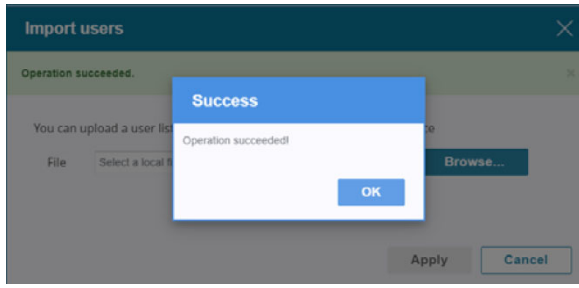
To import the list, do the following:

1. Go to **User Accounts** > **Users**.
2. Click **Import Users** for the following dialog window:



3. Click **Browse** to choose file to upload.
4. Locate the list in the choose file window and open it (double-click or select and click **Open**).
5. Click **Apply**.

6. When completed, a success message will be shown.



If import isn't successful, check the format of your *.csv file.

Editing User Accounts

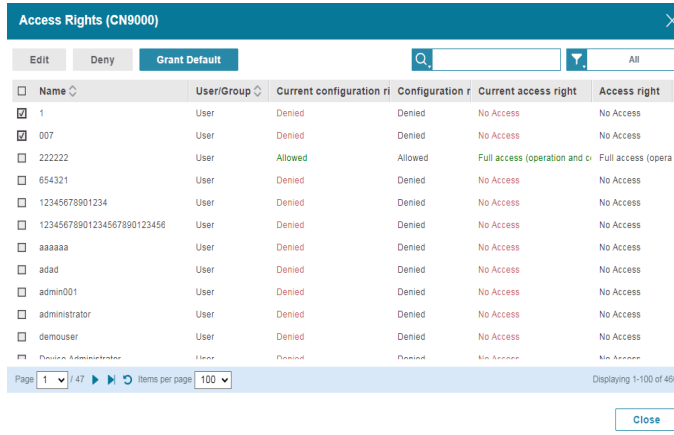
You can edit the Access Rights and the Properties of a user.

■ Editing Access Rights

1. Check the user and click **Edit**.

   Alternatively, you can move your cursor over the user and click the pencil icon.

2. Click **Access rights** and a window will pop up. An example is shown:



3. Check a device or port and click **Edit**.

   Alternatively, you can move your cursor over the device or port and click the pencil icon.A window will pop up. An example is shown:

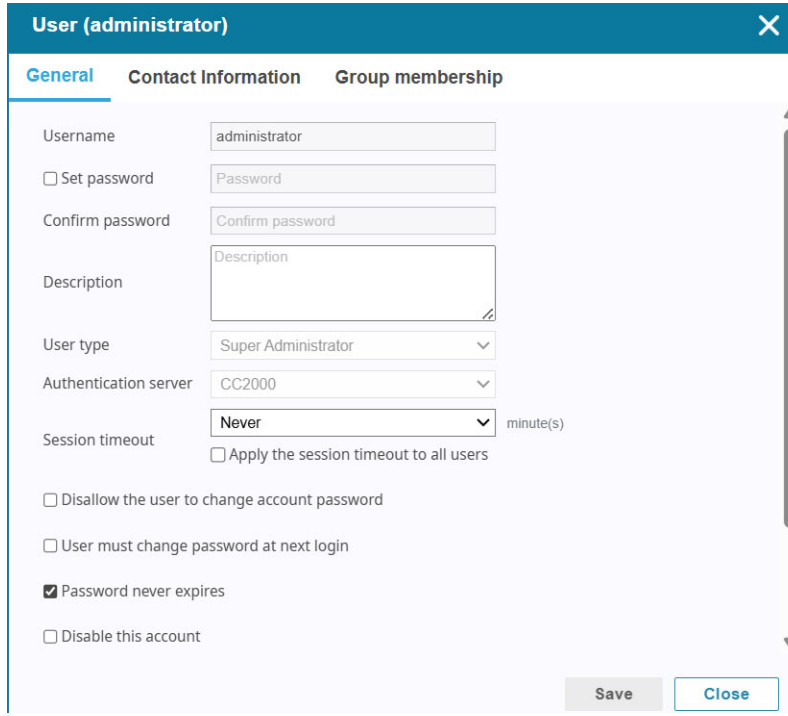
4. Refer to the information in *Access rights* on page 111 to help you edit the rights.

■ Editing Properties

1. Check the user and click **Edit**.

   Alternatively, you can move your cursor over the user and click the pencil icon.

2. Click **Properties** and a window will pop up. An example is shown:



3. Edit the options in this tab. You can change to a different tab by clicking it.

   Refer to *User* on page 173 for information about the three tabs shown here.

■ Unblocking User Accounts

A user may be blocked out due to exceeding the number of login attempts.

To unblock user(s), check to select the blocked user(s) and click **Unblock**.

A confirmation message will pop up, click **Yes** to unblock the user(s).

Note:

- You can unblock more than one user by checking as many names as you require. You can check all accounts by checking the box at the top of the column.
- If all users – including the System Administrator – gets blocked, the System Administrator can use the CC2000Pro Utility to restore his account and then unblock the locked out users. See *Restore*, page 373.

■ Deleting User Accounts

To delete user(s), check to select the user(s) and click **Delete**.

A confirmation message will pop up, click **Yes** to delete the user(s).

- **Reactivate Disabled Users**

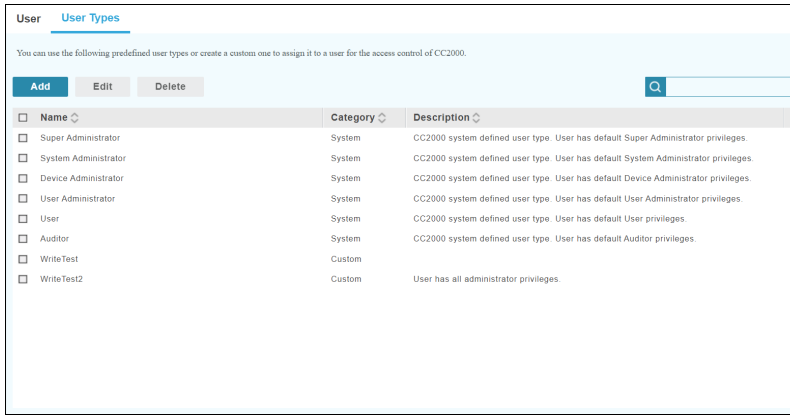
  When you wish to reactivate a disabled user, go to bottom of the properties page. An example is shown:

  Uncheck the “Disable this account” option and click **Save**.

  An *Operation succeeded* message will be shown on top of the page.

User Types

Click the User Type tab to show a list of user types. An example is shown:



There are System and Customer user types where the Category column helps you identify which is which.

The CC2000 supports six system user types and are predefined in the system. The roles assigned to members of these user types are fixed and cannot be changed.

The *Custom* user type category provides you with the convenience and flexibility of assigning various combinations of roles that best suit your installation's requirements.

System User Types

The supported functions and features for each user type are fixed, and they are summarized in the table below:

Functions & Features	Super Admin	System Admin	User Admin	Device Admin	Asset Admin	User	Auditor	Dashboard Viewer
System Management	√	√					◊	
System tasks	√	√					◊	
Authentication services	√	√	√				◊	
User / Group management	√	√	√				◊	
User / Group device access rights	√	√	√				◊	
Device management	√	√		√			◊	
Asset Management	√	√			√		◊	
Log configuration and settings	√	√	√	√	√		◊	
View logs / reports	√	√	√	√	√		◊	
Users can change their own passwords	√	√	√	√	√	√	√	√

Symbols:

√: Full Access

◊: View Only

Note:

1. The differences between Super Administrators and System Administrators are as follows:
   - Super Administrators are authorized for all roles automatically, and includes access to all devices, ports, and outlets. The roles are fixed and cannot be changed.
2. **Auditor:**
   - Auditors can access all tabs and pages, but is restricted to *View Only* rights.
   - For **Logs**, Auditors can export and print logs in addition to viewing them, but cannot change any settings.
   - For **Preferences**, Auditors can change his/her *Web Options* and *Password*.
3. **Dashboard Viewer:** Dashboard Viewers have view-only rights to dashboards and the rights to change their own login credentials.

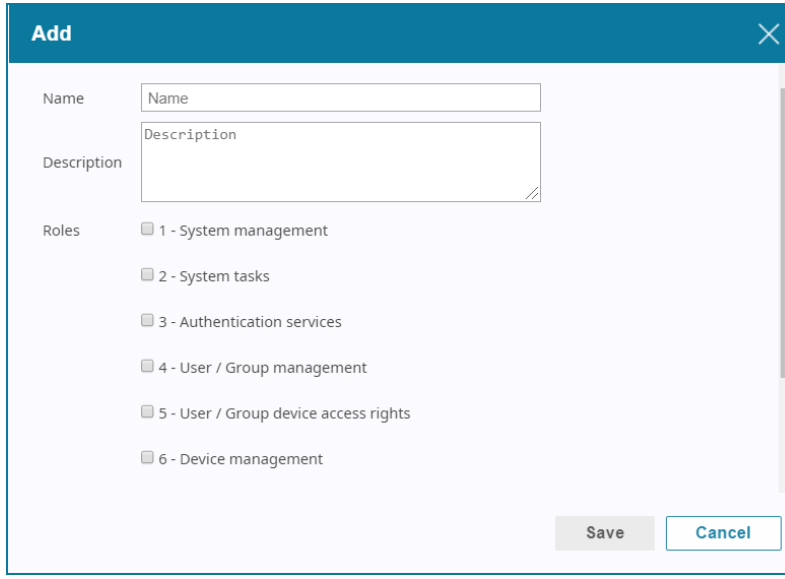
Custom User Types

You can create custom user types with any combination of roles assigned to them to suit your requirements.

■ Add User Type

Follow the steps below to create a custom user type:

1. Click **Add** for a pop-up window as shown:



2. Enter a name, description and check the roles you want the new user type to have.

Note:

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

3. Click **Save** to complete.

■ Editing User Type

1. Check the user type you wish to edit and click **Edit**.

   Alternatively, you can move your cursor over the user type and click the pencil icon.

2. Edit the name, description and check/uncheck the roles you want this user type to have.
3. Click **Save** to complete.

Deleting a User Type

Check the user type and click **Delete**.

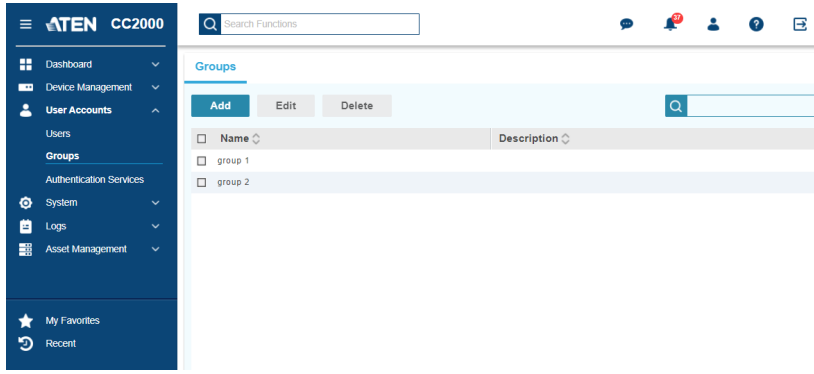
A confirmation message will pop up, click **Yes** to delete the user type(s).

Note: You can only delete non-system user types.

Group Accounts

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

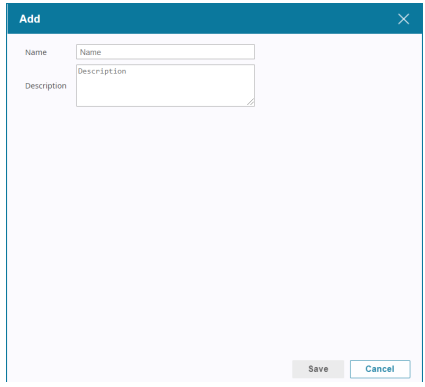
The Groups submenu looks similar to the one below:



Groups Tab

Adding a Group

1. Click **Add** and a window will pop up:

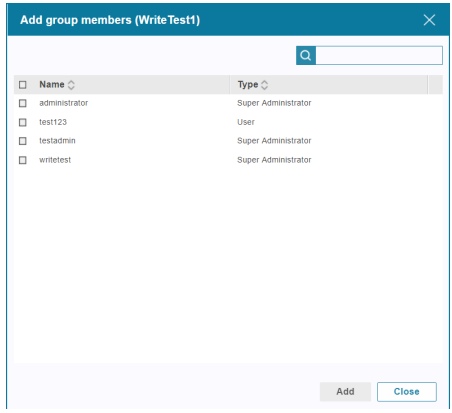


2. Enter a name and description.

Note:

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

3. Click **Save**.
4. The system will ask you to add members to this group. An example is shown:



5. Check the users you wish to include into the group and click **Add**.
6. When you have finished adding the users, click **Close**.

Editing a Group

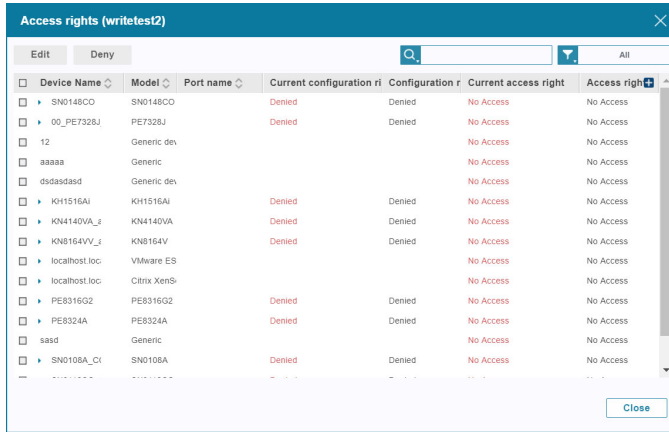
■ Editing Group Access Rights

Follow the steps below to edit the access rights of a group:

1. Check the group and click **Edit**.

   Alternatively, you can move your cursor over the group and click the pencil icon.

2. Click **Access rights** and a window will pop up. An example is shown:



3. Check a device or port and click **Edit**.

   Alternatively, you can move your cursor over the device or port and click the pencil icon.

   A window will pop up. An example is shown:

4. Refer to the information in *Access rights* on page 111 to help you edit the rights.

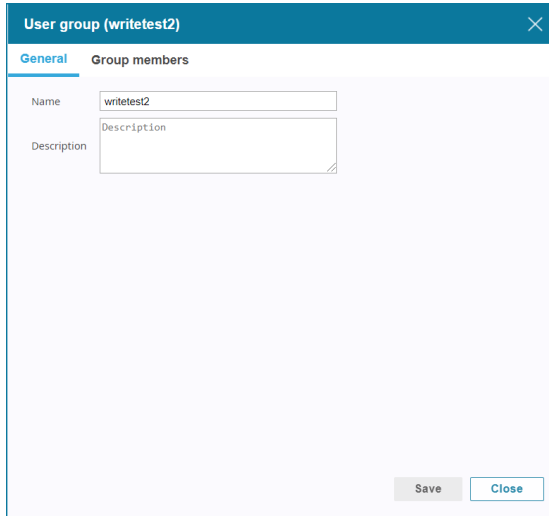
Note: When a user is assigned to two or more groups, and the access rights of those groups conflict, the CC2000 applies to the most permissive access level.

■ Editing Properties

1. Check the group and click **Edit**.

   Alternatively, you can move your cursor over the group and click the pencil icon.

2. Click **Properties** and a window will pop up. An example is shown:



3. Edit the options in this tab. You can change to a different tab by clicking it.

   Refer to *Adding a Group* on page 185 for information about the two tabs shown here.

Deleting a Group

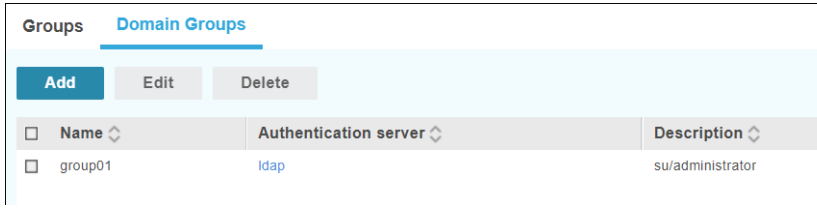
Check the group(s) and click **Delete**.

A confirmation message will pop up, click **Yes** to delete the group(s).

Domain Groups tab

Create one or more domain groups if you are using a third-party authentication server or Active Directory System to manage users.

The Domain Groups tab is shown below:



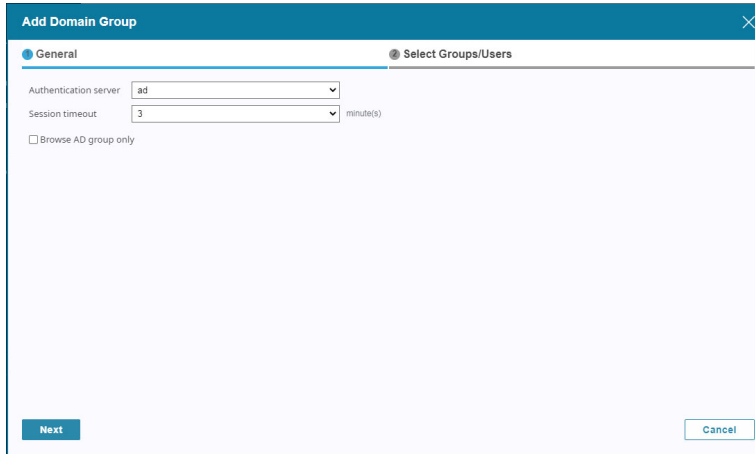
Note: When a user is assigned to two or more domain groups, and the access rights of those groups conflict, the CC2000 applies to the most permissive access level.

Adding a Domain Group

1. Make sure you already have an external authentication service set up.

   For more information about how to add an authentication service to CC2000, see *Adding a Third-party Authentication Server* on page 192.

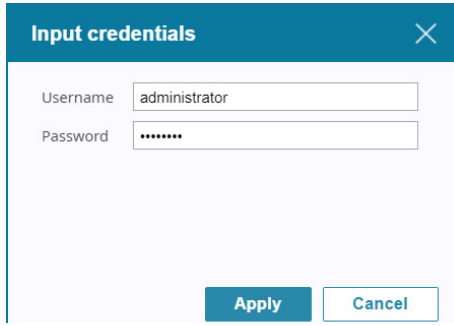
2. Click **Add** for the Add domain group pop-up window:



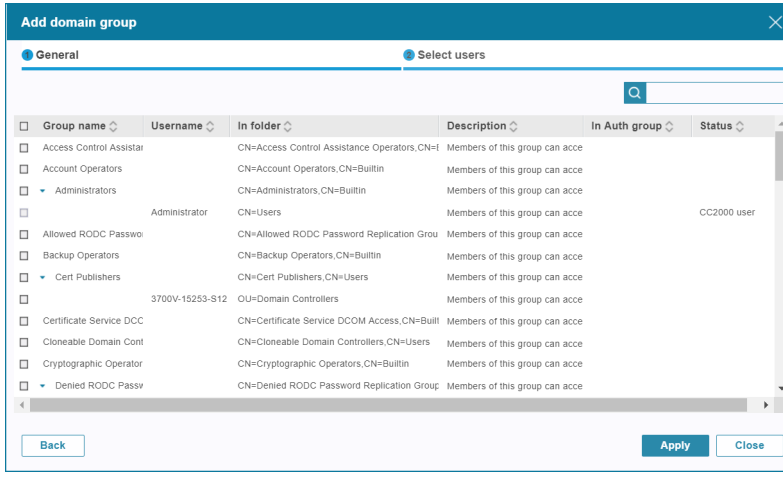
3. Select the Authentication server and Session timeout by clicking and selecting from their corresponding drop-down menu.

Note: When AD Server is selected as your authentication server, you can optionally check *Browse AD group only* to only browse for AD groups and omit individual AD users.

4. Click **Next**. Where necessary, the server may prompt you for credential input. An example is shown:



5. After entering the credentials, click **Apply**. You will be taken to the Select users page.



6. Check the group(s) and click **Apply**.

Authentication Services

CC2000 supports login authentication via its built-in server, as well as a variety of third-party, external authentication servers. These external servers can be added to the system and made available as options when configuring user accounts. The supported external authentication servers include:

- Active Directory
- Kerberos server
- LDAP server
- MOTP server
- RADIUS server
- TACACS+ server
- Windows NT Domain
- Dual Authentication
- Microsoft Entra ID
- Two-factor authentication

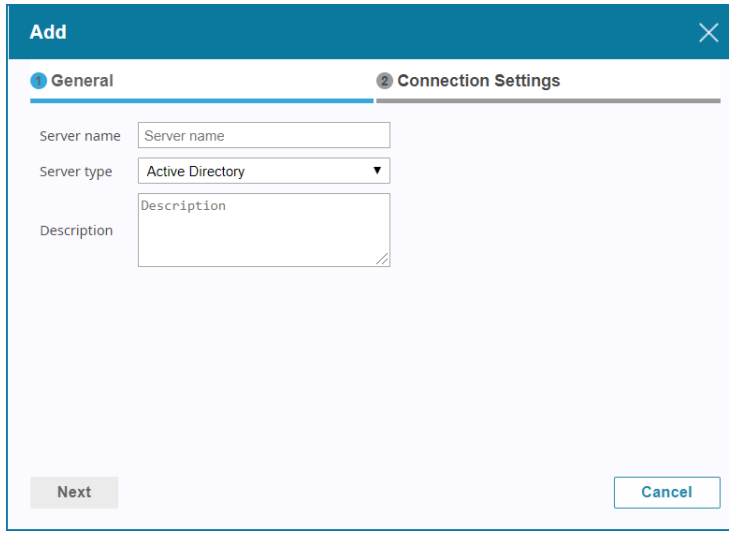
Note:

- *Authentication* refers to determining the authenticity of the person logging in; *authorization* refers to assigning permission to use the device's various functions.
- These external servers provide authentication services only – they do not provide authorization services. Authorization is provided through the CC2000 management system.
- The CC2000 supports Mobile One-Time Password (MOTP) servers that can be used as 3rd-party authentication servers to improve security. For more information, see *MOTP Settings*, page 410, or visit our web site at *www.aten.com/CC2000-OTP*
- For LDAP and Active Directory there is an additional authentication method in which the user attempting to log in does not have an account on the CC2000. In this case, the CC2000 checks the external server to see if it contains an account with the username and password of the user attempting to log in. If it does, the CC2000 checks to see if the user belongs to a group that corresponds to a CC2000 domain group. If it does, the CC2000 lets the user log in and assigns him the access rights of the group. See *Domain Groups tab*, page 189, for details.

Adding a Third-party Authentication Server

Follow the steps below to add authentication services:

1. Go to **User Accounts** > **Authentication Services**.
2. Click **Add**. This window appears.

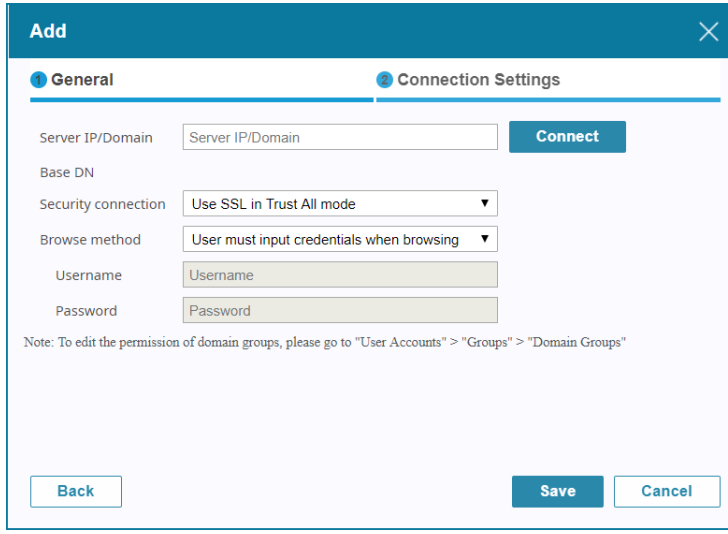


3. Enter the Server name, choose the Server type using the drop-down menu, and optionally enter a description for the server.

Note:

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

4. Click **Next** for the Connection Settings page. This page will be different for different Server type.



5. Enter information on the page. Refer to the corresponding section below for the information fields.
   - *Active Directory* (page 194)
   - *Kerberos* (page 195)
   - *LDAP* (page 195)
   - *Microsoft Entra ID (SAML)* (page 196)
   - *MOTP (Mobile One-Time Password)** (page 197)
   - *RADIUS and TACACS+* (page 199)
   - *Windows NT Domain* (page 200)
   - *Dual Authentication* (page 200)
6. Enter the server IP/domain and click **Connect** to test the connection.

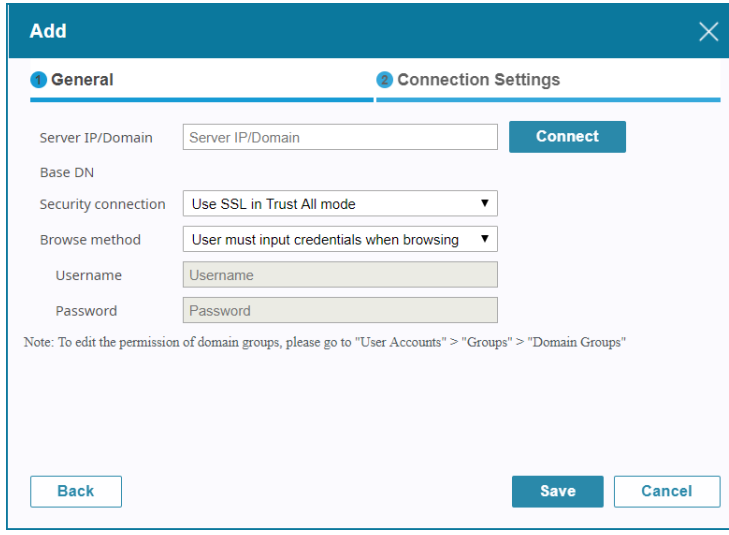
7. Select the Security connection and Browse method using the corresponding drop-down menu.
8. Click **Save**.

Server Information

An explanation of the information required for each of the servers is provided, below.

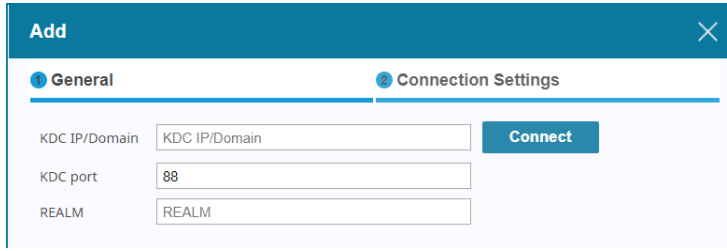
- **Active Directory**

Heading	Information
Server IP/Domain	Get the information for these fields from the Active Directory administrator. For example settings see *Active Directory Settings Example*, page 397.
Security connection	Use the drop-down menu to choose whether or not to use SSL in Trust All mode.
Browse Method	◆ Select *Browse with user credentials* to allow the user to browse the Active Directory using credentials configured on the server. If this is selected the user doesn't 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.



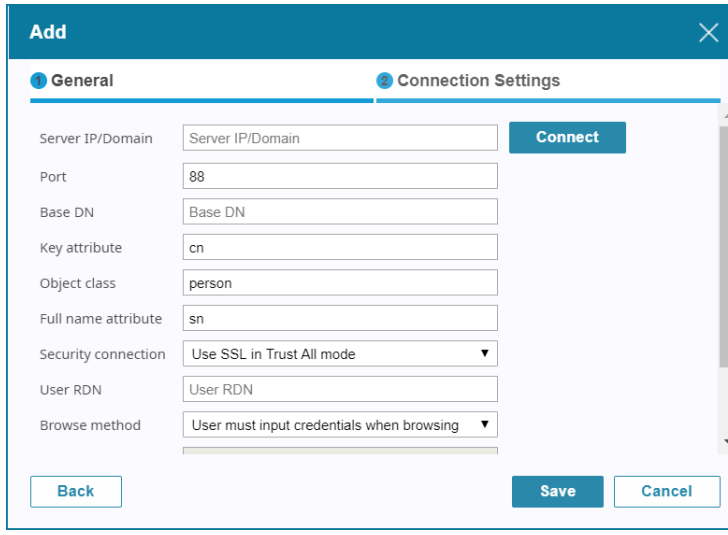
- **Kerberos**

Heading	Information
KDC IP/Domain	Get the IP/Domain from the Kerberos administrator.
KDC port	Get the port information from the Kerberos administrator.
REALM	This is the domain over which Kerberos authentication server has the authority to authenticate a user, host or service. Get the realm information from the Kerberos administrator.

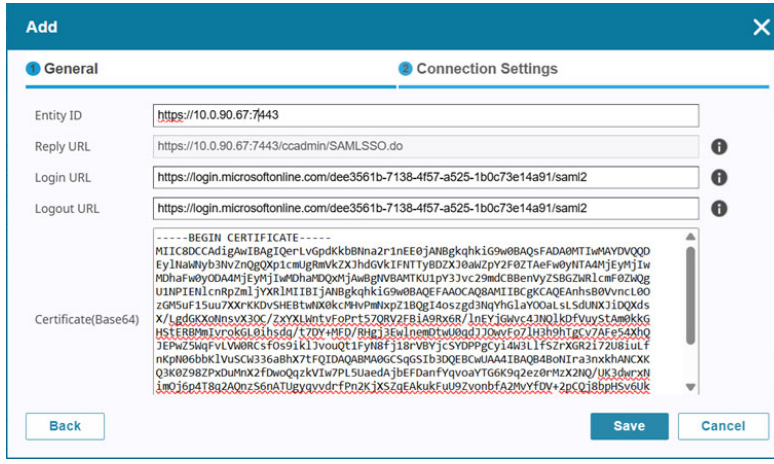


- **LDAP**

Heading	Information
Connection Settings	Get the information for these fields from the LDAP administrator. The port default is 636, but check with the LDAP/LDAPS administrator to see if it may be something else. For example settings see *LDAP/LDAPS – OpenLDAP Setting Example*, page 395.
Security connection	Use the drop-down menu to choose whether or not to use SSL in Trust All mode.
User RDN	Get the information for these fields from the LDAP administrator. For example settings see *LDAP/LDAPS – OpenLDAP Setting Example*, page 395.
Browsing Method	◆ Select *Browse with user credentials* to allow the user to browse LDAP/LDAPS using credentials configured on the server. If this is selected the user doesn't 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/LDAPS.



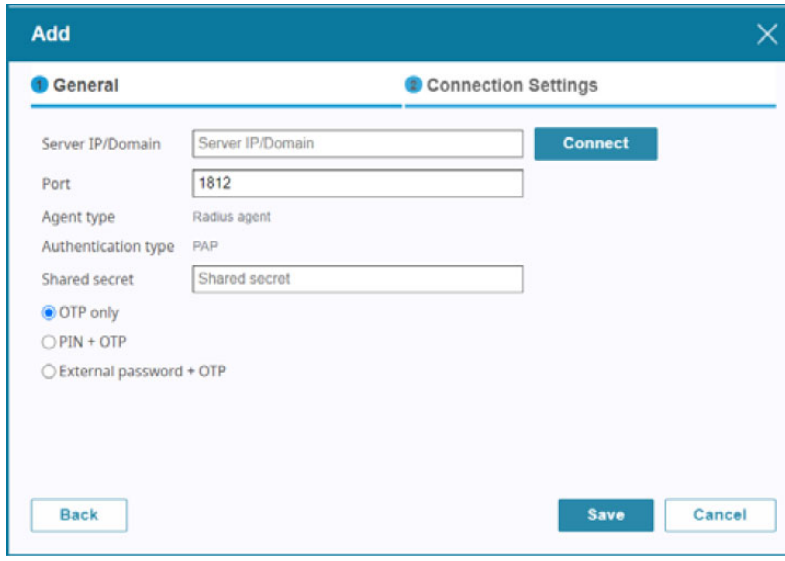
- **Microsoft Entra ID (SAML)**



Heading	Information
Entity ID	Enter the entity ID. Make sure this ID matches the setup on the Entra ID platform.
Reply URL	Enter the Assertion Consumer Service (ACS) URL— the place where Entra ID sends the SAML response after a user successfully signs in. Obtain this information from the Entra ID platform.

Heading	Information
Login URL	Enter the login URL. Obtain this information from the Entra ID platform.
Logout URL	Enter the logout URL. Obtain this information from the Entra ID platform.
Certificate (Base 64)	Enter the SAML signing certificate. Obtain the certificate by downloading the certificate file labeled with “Certificate (Base64)” from the Entra ID paltform.

- **MOTP (Mobile One-Time Password)***



Note:

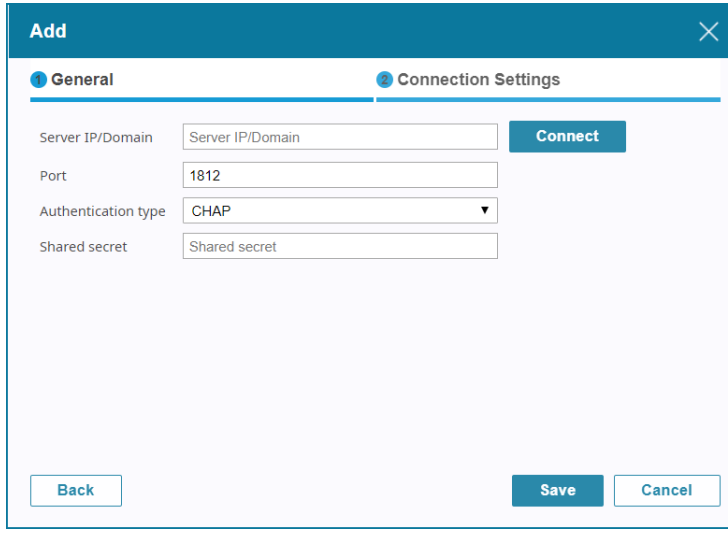
- The MOTP server is for One-Time Password (OTP) token authentication only. If you want to adopt the OTP function, you need to install a MOTP server first.
- If you want to purchase a MOTP server, contact CHANGING Information Technology Inc. (https://www.changingtec.com/EN/).

Heading	Information
Server IP/Domain	Get the information for the IP from the service administrator and enter it here. Click **Connect** to test the connection.

Heading	Information
Port	Get the information for the Port from the service administrator and enter it here. The default MOTP port is 1812.
Agent type	Radius is automatically selected for you.
Authentication Type	PAP is automatically selected for you.
Shared secret	Enter the character string that you use for authentication with the MOTP server. If unsure, get the most up to date information for shared secret from the service administrator.
Two Factor	This section allows you to select the MOTP authentication method used for logging in to the CC2000. 1. If you select *OTP only*, the CC2000 will require you to enter the Username to log in and the system will prompt you to enter the OTP (from your token device). The Password field can be ignored. 2. If you select *PIN + OTP*, the CC2000 will require you to enter the Username to log in and the system will prompt you to enter the OTP (from your token device) and PIN (set in MOTP server). Password field can be ignored. 3. If you select *External password + OTP*, the CC2000 will require you to enter the Username to log in and the system will prompt you to enter the OTP (from your token device) and the external password from a 3rd-party authentication server (configured in the MOTP server). Password field can be ignored.

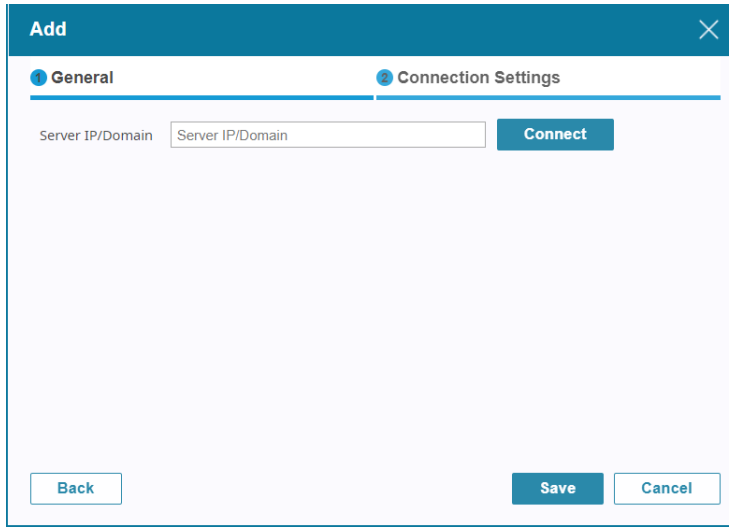
- **RADIUS and TACACS+**

Heading	Information
Connection Settings	Get the information for these fields from the service administrator. The default port for RADIUS is 1812 and TACACS+ is 49, but check with the service administrator to see if it may be something else. For example settings see *RADIUS Settings Example*, page 398 and *TACACS+ Settings Example*, page 400.
Authentication Settings	Get the information for these fields from the service administrator. For example settings see *RADIUS Settings Example*, page 398 and *TACACS+ Settings Example*, page 400. 1. Use the drop-down menu to select the *Authentication type* your RADIUS/TACACS+ server is configured for. 2. In the Shared Secret field, key in the character string that you use for authentication with the RADIUS server. 3. Key the shared secret in again in the Confirm Shared Secret field.

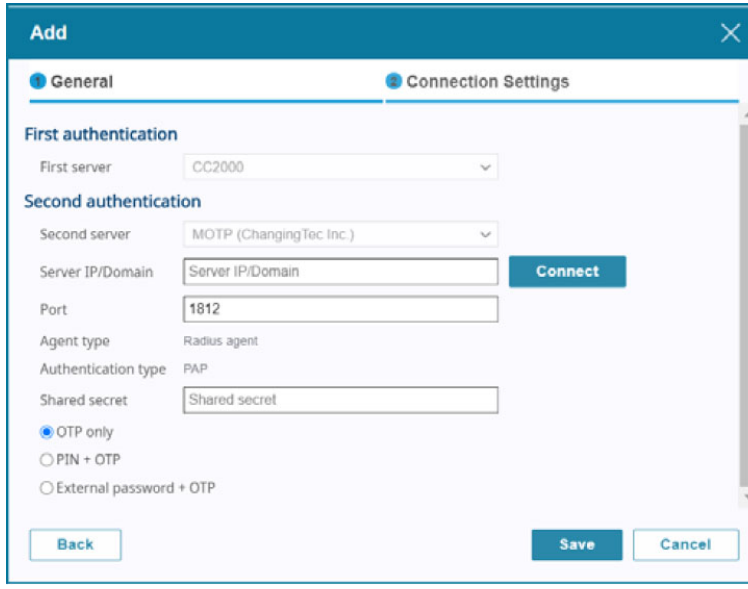


- **Windows NT Domain**

  Get the information for the Domain Name from the service administrator. For example settings see *NT Domain Settings Example*, page 402.



- **Dual Authentication**



Dual authentication requires you to log in by entering the username and password of a user in the CC2000 server, followed by the MOTP authentication.

Heading	Information
First authentication	The first authentication method would be CC2000's authentication.
Second authentication	The second authentication method would be MOTP authentication.
Server IP/Domain	Get the information for the IP from the service administrator and enter it here. Click **Connect** to test the connection.
Port	Get the information for the Port from the service administrator and enter it here. The default MOTP port is 1812.
Agent type	Radius is automatically selected for you.
Authentication Type	PAP is automatically selected for you.
Shared secret	Enter the character string that you use for authentication with the MOTP server. If unsure, get the most up to date information for shared secret from the service administrator.
Two Factor	This section allows you to select the MOTP authentication method used for logging in to the CC2000. 1. If you select *OTP only*, after entering the username and password to log into the CC2000, the system will prompt you to enter the OTP (from your token device). 2. If you select *PIN + OTP*, after entering the username and password to log into the CC2000, the system will prompt you to enter the OTP (from your token device) and PIN (set in MOTP server). 3. If you select *External password + OTP*, after entering the username and password to log into the CC2000, the system will prompt you to enter the OTP (from your token device) and the external password from a 3rd-party authentication server (configured in the MOTP server).

Note:

- The MOTP server is for One-Time Password (OTP) token authentication only. If you want to adopt the OTP function, you need to install a MOTP server first.
- If you want to purchase a MOTP server, contact CHANGING Information Technology Inc. (https://www.changingtec.com/EN/).

Single Sign-On Using Microsoft Entra ID

CC2000 supports identity authentication and single sign-on (SSO) using Microsoft Entra ID. This section provides suggested procedures on configuring Entra ID and CC2000.

SSO Setup Overview

A. Configure Entra ID

Note: The user interface of Microsoft Entra admin center may be updated at any time. Please consult the Microsoft Entra online help for detailed or current practice.

1. Register CC2000 and other applications to be authenticated by Entra ID.
   For details, see *Registering Applications in Microsoft Entra ID*, page 431.
2. Create users and/or groups on Entra ID based on your needs.
   - *Creating Users on Microsoft Entra ID*, page 436
   - *Creating Groups on Microsoft Entra ID*, page 439
3. Add group claims to the SSO tokens.
   For details, see *Adding Group Claims to Tokens*, page 440
4. Grant access privileges to the added users and/or groups.
   For details, see *Granting Access Privilege to Users and Groups*, page 441.

B. Add Entra ID as a new authentication service to CC2000

For details, see *Adding a Third-party Authentication Server*, page 192

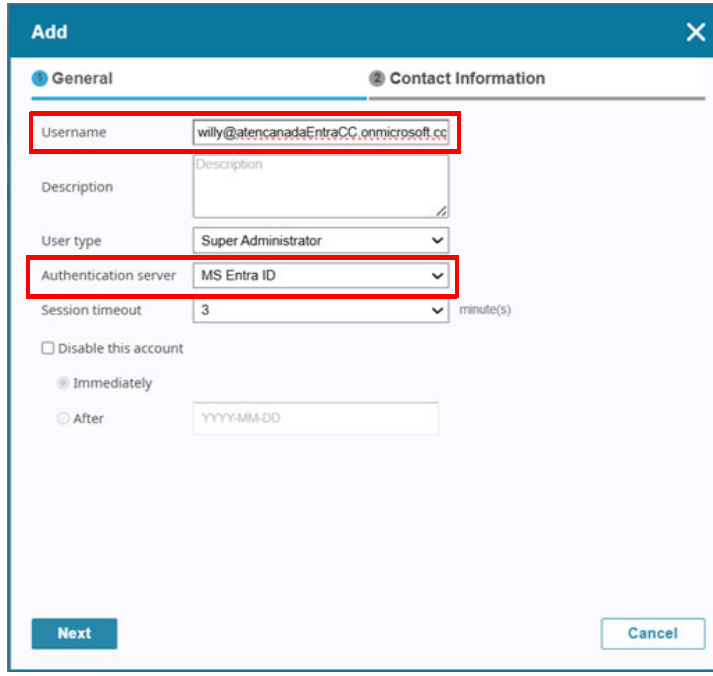
C. Add users and/or groups in CC2000

Make sure that the created Entra ID users and/or groups have been added to CC2000 so that CC2000 can manage their access privileges, while Entra ID handles login authentication.

1. To add user accounts, follow the steps below.
   a) In the CC2000 web console, click **Users**. The user list appears.
   b) Click **Add**.
   c) In the pop-up window, configure the following.

- Enter the account details. Make sure the **Username** matches its corresponding Entra ID account name.
- For **Authentication server**, select the Entra ID added in step B.

  For example:



d) Configure other settings if needed. For full details on creating user account, see *User Accounts*, page 173.

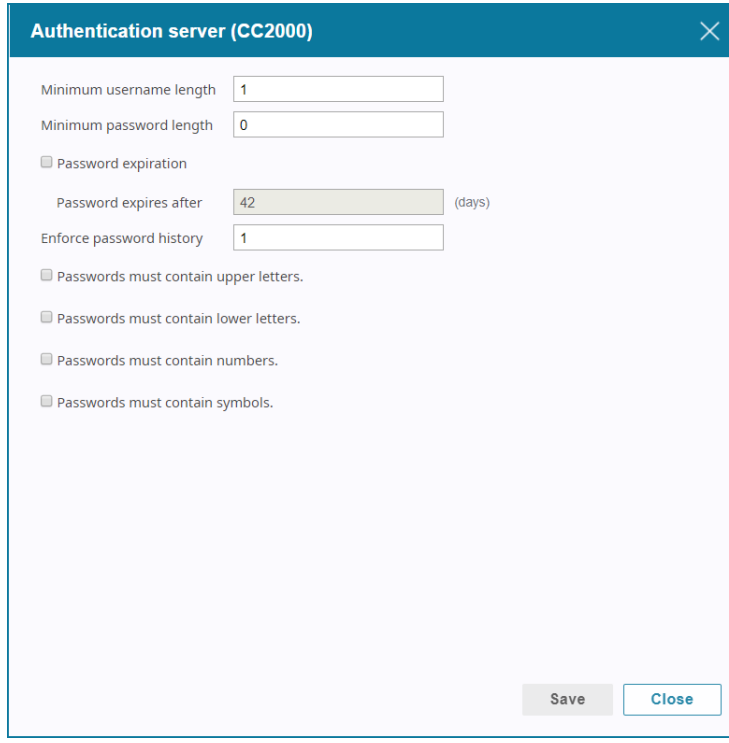
2. (Optional) Add group accounts if you have created group accounts on Entra ID. For full details on creating group accounts, see *Group Accounts*, page 185.

CC2000's Built-in Authentication Service

With regard to the CC2000's internal authentication services, 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 the CC2000's password policy, do the following:

1. Check the server and click **Edit**.

   Alternatively, you can move your cursor over the server and click the pencil icon.



2. Make the configuration choices you desire. Refer to the table below for an explanation of the fields.

Heading	Information
Minimum username length	The username length can be from 1–32 English alphanumeric characters. The default is 6 characters.

Heading	Information
Minimum password length	The password length can be from 0–32 English alphanumeric characters. The default is 6 characters. A setting of 0 means that no password is required. Since this leaves your installation in a highly insecure state, we strongly recommend against a setting of 0.
Password expiration	For security purposes, you can force users to renew their passwords at specific time intervals. To do so, enable *Password expiration*, then specify the number of days that the password will expire after. 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.
Enforce password history	For security purposes, enable this setting and enter the number of unique passwords that must be created before a user can use a password that was previously used.
Passwords must contain upper case letters	For security purposes, enable this setting to force the user to include upper case letters in the password.
Passwords must contain upper case letters	For security purposes, enable this setting to force the user to include lower case letters in the password.
Passwords must contain numbers	For security purposes, enable this setting to force the user to include numbers in the password.
Passwords must contain symbols	For security purposes, enable this setting to force the user to include symbols in the password.

3. When you have finished, click **Save**.

Deleting an Authentication Server

To delete an authentication server, check the server(s) and click **Delete**.

A confirmation message will pop up, click **Yes** to delete the user(s).

Note:

- You can delete all deleteable servers by checking the box at the top of the column.
- If a user account has been created on the CC2000 that uses an external authentication server, the server cannot be deleted.

Two-factor Authentication

To prevent unauthorized access or credential leaks, enable two-factor authentication (2FA) on the CC2000 accounts. This requires the user to enter a time-sensitive passcode generated by an authenticator app. This function is disabled by default.

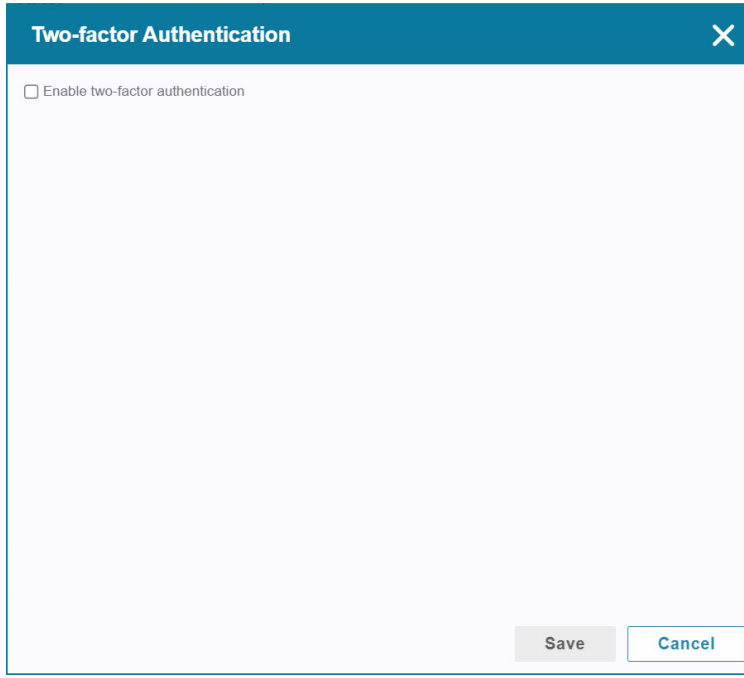
Note:

- Domain groups do not support two-factor authentication.
- Two-factor authentication is not supported for user accounts using MOTP servers.

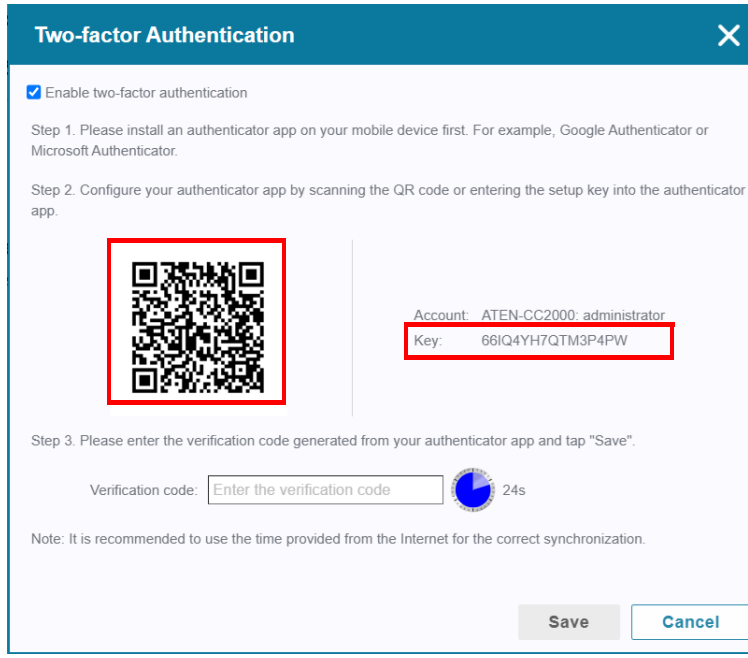
Enabling Two-factor Authentication on One Account

1. On a mobile device to be used for generating the verification code, install an authenticator app, such as Google Authenticator or Microsoft Authenticator.
2. On CC2000's web console, log in to the target account.

3. Click from the task bar, and then click **Enable two-factor authentication**. This screen appears.



4. Click **Enable two-factor authentication**.
5. Register the CC2000 account on the authenticator that you installed.
   a) Launch the authenticator app, scan the QR code on the Two-factor Authentication window, or enter the key. A 6-digit verification code is then generated by the authenticator.



   b) In the Two-factor Authentication window (CC2000), type in the verification code. Make sure to do this within the indicated countdown.
6. Click **Save**. The two-factor authentication takes effect from the next login.

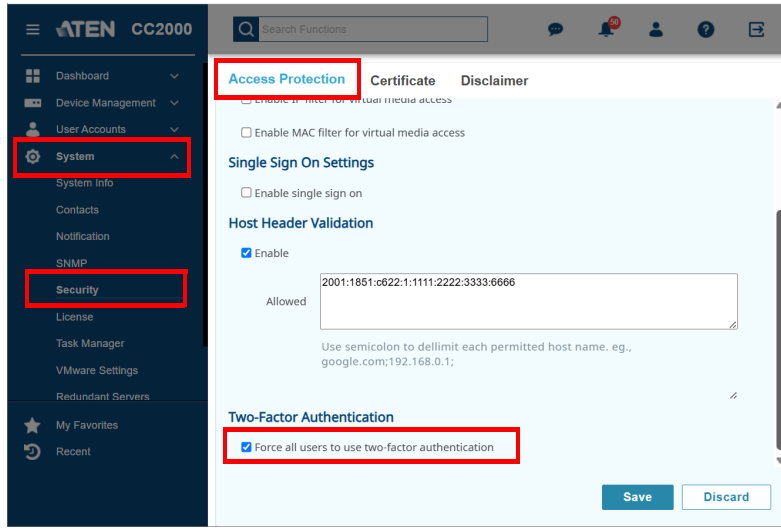
Note: To avoid login failure due to time discrepancy between your mobile device and the CC2200, make sure that both systems are set to sync with the NTP server.

Enabling Two-factor Authentication on All Accounts

You can apply two-factor authentication to all accounts by enabling a global setting on the system security page with a system administrator, super administrator. or user administrator account. Once two-factor authentication is enabled this way, it can only be turned off by clearing the setting on the system security page.

To enable two-factor authentication to all accounts:

1. Log in the CC2000 management console as a system administrator, super administrator, or user administrator.
2. From the left panel, go to **System** > **Security** > **Access Protection**, and enable **Force all users to use two-factor authentication**.



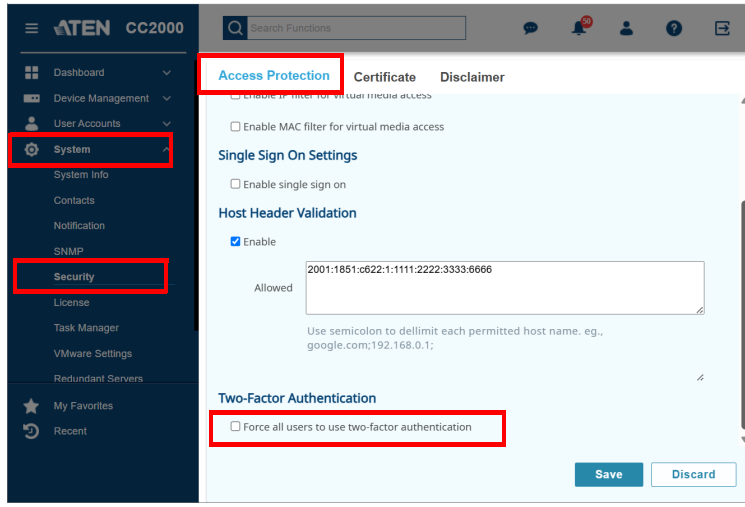
3. Click **Save** to apply the setting. The setting takes effect upon the next login.

Disabling Two-factor Authentication

- To disable two-factor authentication **for all accounts**:

  1. Log in CC2000 using as a system administrator, super administrator, or user administrator.

  2. From the left panel, go to **System** > **Security** > **Access Protection**, and disable **Force all users to use two-factor authentication**.



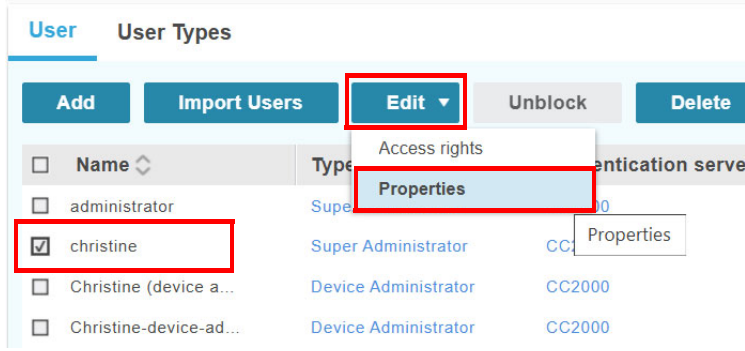
Note: If the setting is not enabled, it is likely that two-factor authentication was previously enabled individually through this account. In this case, follow the steps in the next section to disable the setting.

- To disable two-factor authentication **on a few accounts**:

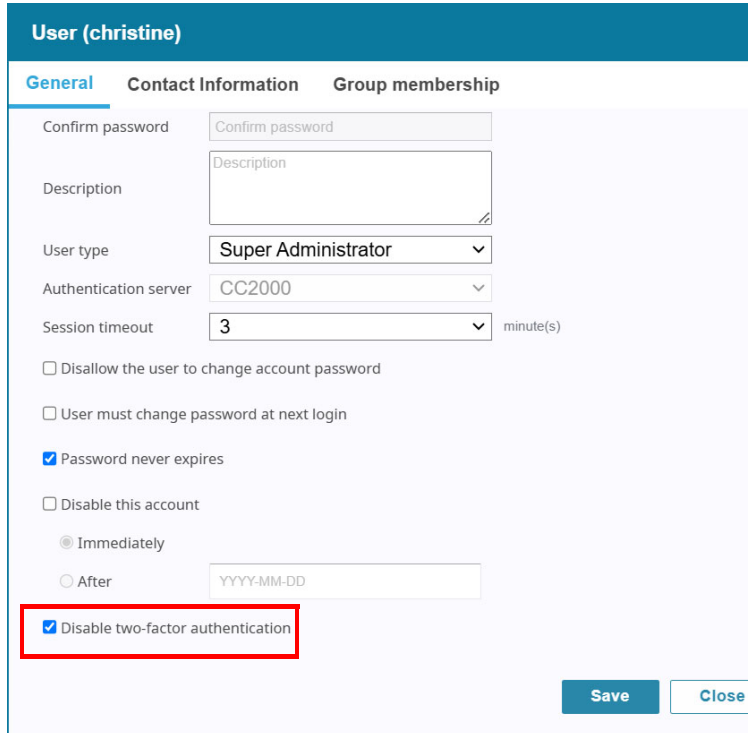
  1. Log into CC2000 using a super administrator, system administrator, or user administrator account.

  2. Go to **User Accounts** > **Users**. The user list appears.

3. Click to select a user, click **Edit**, and then select **Properties**.



4. In the pop-up user properties window, scroll down and select **Disable 2-factor authentication**.



5. Click to enable the setting.

- To disable two-factor authentication on one account:

  1. Log into the target account on CC2000. Enter the verification code as prompted.
  2. Click from the task bar, select **Two-factor authentication**.
  3. In a pop-up window, uncheck **Enable two-factor authentication**.

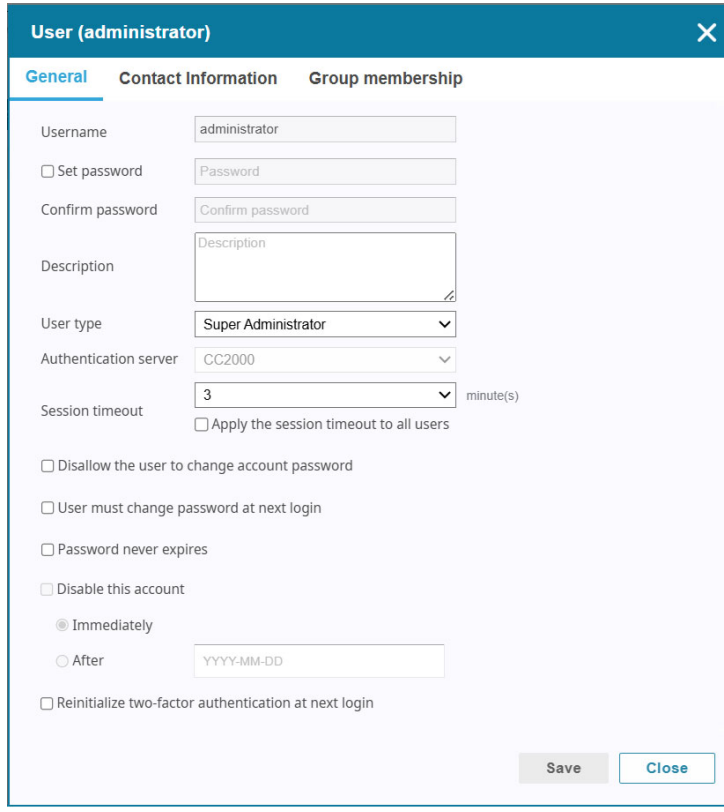
  Note: If the setting cannot be unchecked, it is likely that two-factor authentication was previously enabled globally through the System Security page by your system administrator.

  4. Click **Save** to apply the setting.

Re-initializing Two-factor Authentication

If a user changes the phone or re-install the authenticator app, follow the steps below to re-initialize the authentication.

1. Log in to the CC2000 web console as a system administrator, super administrator, or user administrator.
2. Go to **Users**.
3. Locate the target user from the user list
4. Click , and then select **Properties**. This screen appears.



5. Click to enable **Reinitialize two-factor authentication at next login**.

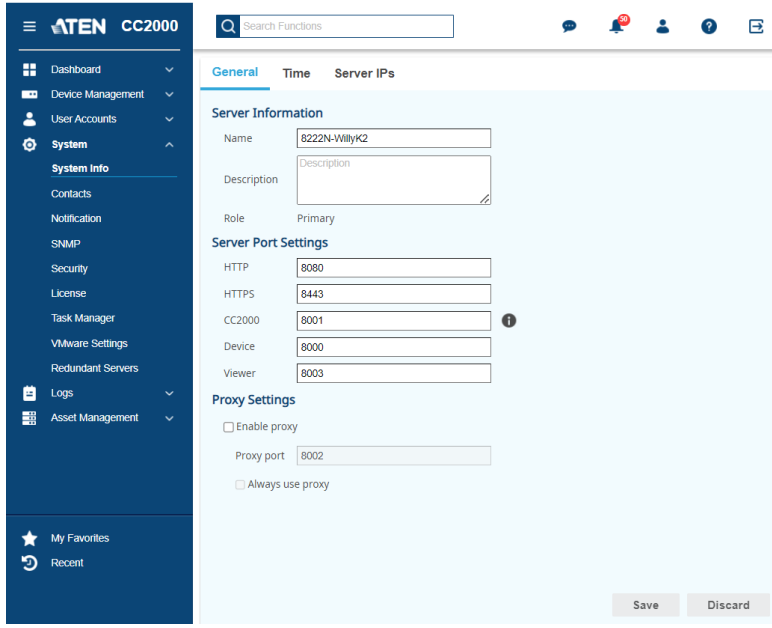
   The user will be prompted to re-initialize two-factor authentication at the next login.

Chapter 7
System

Overview

A CC2000 installation is comprised of CC2000-compatible devices that are connected – over-IP – to a CC2000 server, and these devices reside on a network segment that can be reached by CC2000. By connecting individual CC2000 server segments through their IP addresses into an integrated worldwide network, the CC2000 provides secure, centralized, single IP address login access, to all your data center equipment from anywhere there is an Internet connection, at any time.

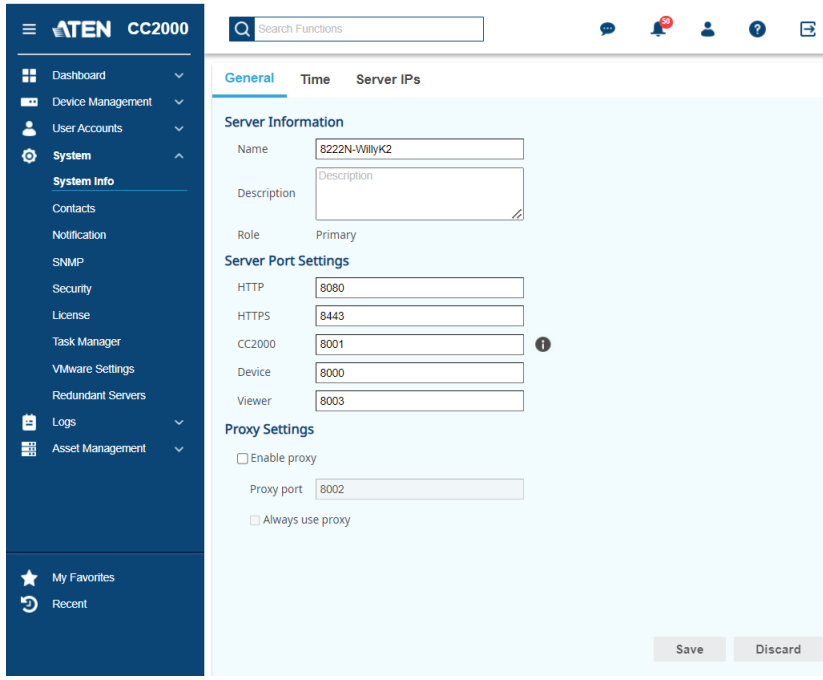
For administrative and deployment purposes, one of the CC2000 servers is considered the primary server while all others are considered Secondaries. When you click the System, the CC2000 opens to the default System page, which looks similar to the screen below:



Note: The System page access is for Super Administrators, System Administrators and Auditors. Auditors can only view the items in this menu.

System Info

The System Info submenu offers three tab menu choices: General, Time and Server IPs. The default System Info page is General, as shown below:



General

The default page is General and looks similar to the one above:

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

This page allows you to configure the CC2000 server's settings.

The meanings of each fields are described in the table below:

Field	Description
Name*	You can change the CC2000 server's name by editing this field.
Description	You can change the CC2000 server's description by editing this field. The description can be from 2–32 Bytes in any supported language.

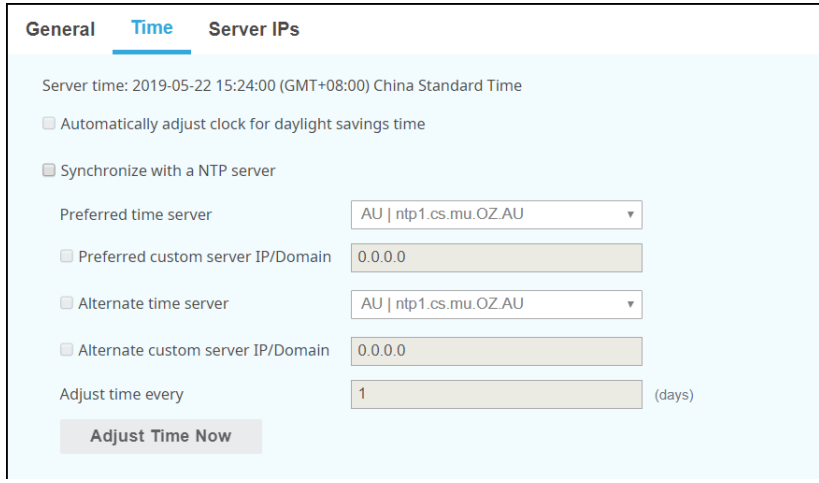
Field	Description
Role	Indicates whether this server is a Primary or Secondary.
HTTP*	The port that the CC2000 uses to communicate with Internet browsers.
HTTPS*	The secure port that the CC2000 uses to communicate with a browser over the Internet.
CC2000*	The port that the CC2000 uses to communicate with other CC2000 servers on the installation.
Device*	The port that the CC2000 uses to communicate with devices on the installation.
Viewer	The port that the CC2000 uses for the viewers to communicate with when Multiviewer is in effect. See *Launch Viewer*, page 140.
Enable proxy	If you need to use the proxy function, check this box, then specify the proxy port in the indicated field. See *CC2000 Proxy Function*, page 355.
Always use proxy	If you wish to always use proxy function, check this box.

Note: See the table on page 15 for more details.

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

Time

The Time page allows you to automatically synchronize the time of the server in which the CC2000 is installed to a network time server.



Note: If you are in a timezone that doesn't have daylight savings time, the **Automatically adjust clock for daylight savings time checkbox** is disabled.

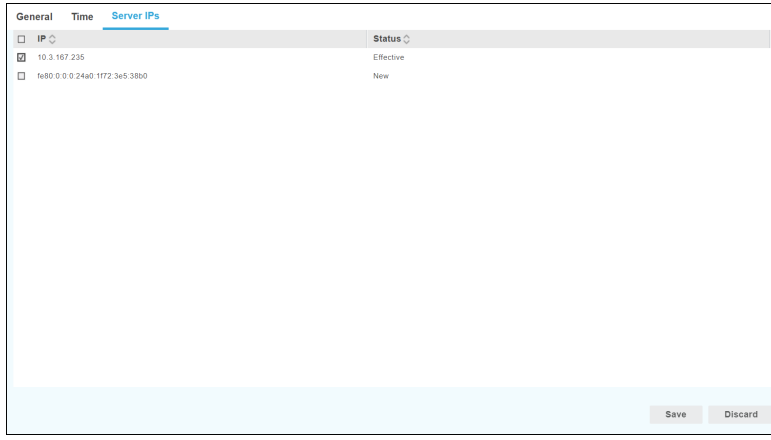
To synchronize to a network time server, do the following:

1. Check the **Synchronize with a NTP server** checkbox.
2. Use the drop-down menu **Preferred time server** to select your preferred time server, or

   Check the **Preferred custom server IP/Domain** checkbox, and key in the IP address of the time server of your choice.
3. If you want to configure an alternate time server, check the **Alternate time server** and **Alternate custom server IP/Domain** checkbox, and repeat step 2 for the Alternate customer time server IP/Domain entries.
4. Key in your choice for the number of days between synchronization procedures in **Adjust time every** field.
5. If you want to synchronize time immediately, click **Adjust Time Now**.
6. When all your settings have been made, click **Save**.

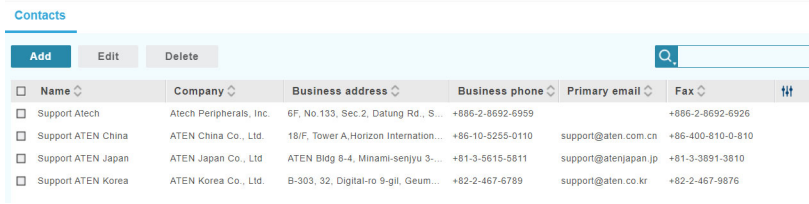
Server IPs

The Server IPs page shows available IP for the server that CC2000 is installed on. Check the checkbox of the IP(s) you wish to use and click **Save** to enable the server and make it Effective.



Contacts

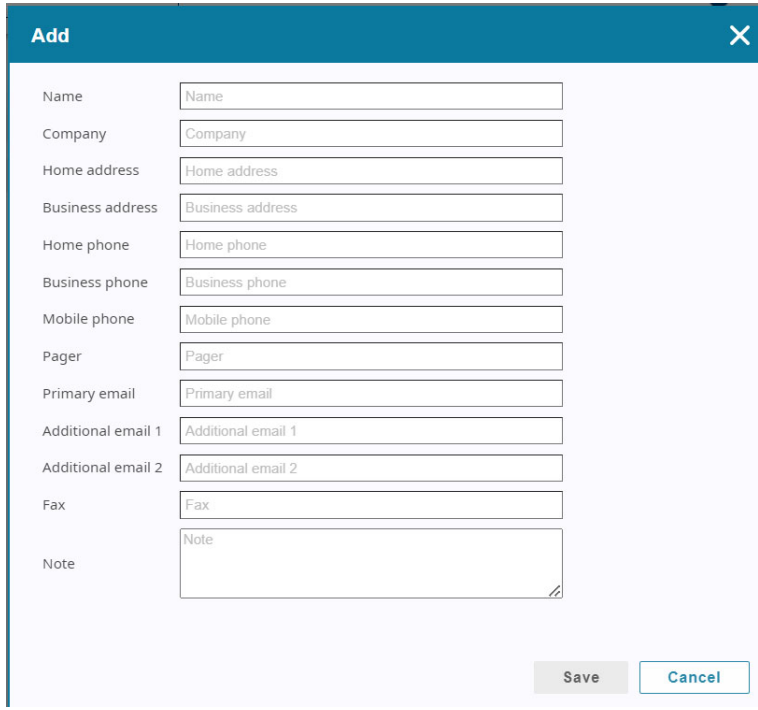
The contacts page stores a list of contacts from which you can browse and quick add within the CC2000 GUI, such as when creating users.



To access the contacts page, log in the CC2000 browser GUI, and then go to **System** > **Contacts**.

Adding a Contact

1. In CC2000 browser GUI, go to **System** > **Contacts**. The contacts page appears.
2. Click **Add**. This dialog box appears.



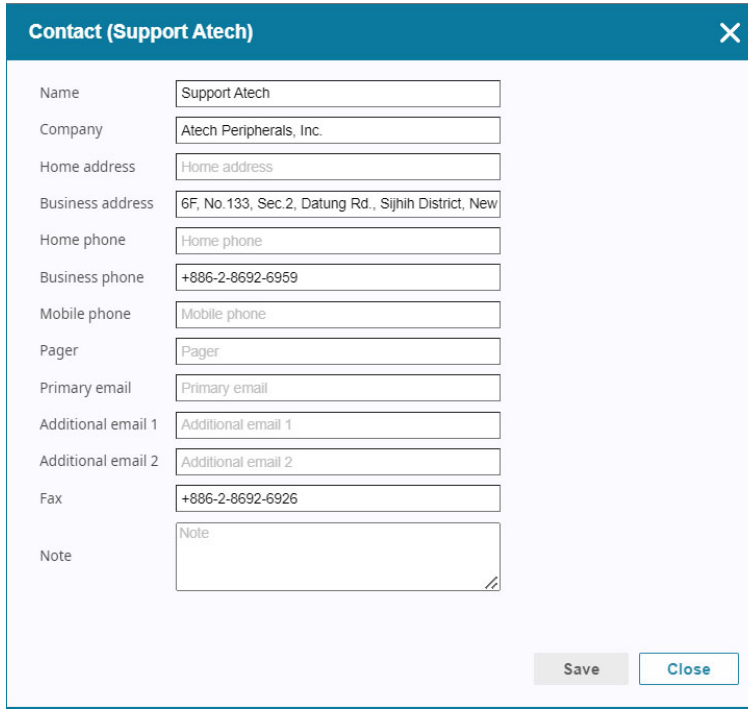
3. Fill in the name and other contact information as needed.

Note: You may save up to two contacts of the same name.

4. Click **Save**. The contact is immediately listed on the contacts page.

Editing a Contact

1. In CC2000 browser GUI, go to **System** > **Contacts**. The contacts page appears.
2. Mouse over the contact you want to edit and click . The contact dialog box appears. For example:

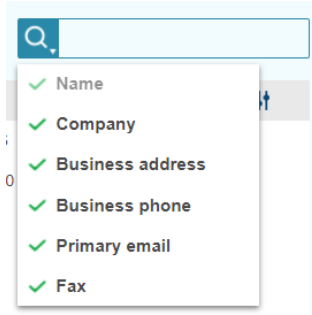


3. Edit the contact information as needed and click **Save** to apply the changes.

Browsing for Contacts

To search for contacts

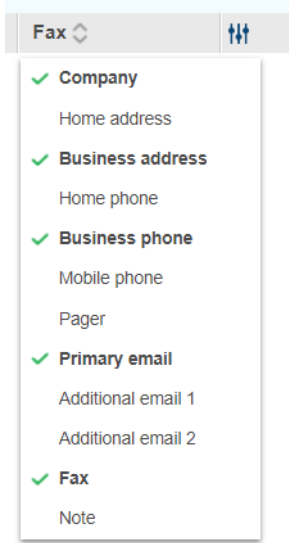
1. Click  to select/unselect the columns that the browsing is done.



2. Type one or more keywords into the search box  and press the Enter key (on your keyboard). The system will do a fuzzy search within the name and company fields.

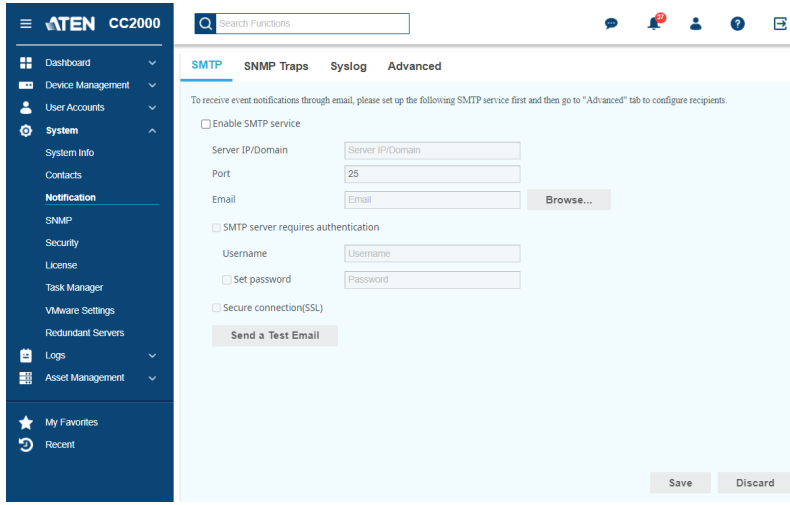
Adding / Removing Columns

You can add or remove the displayed columns on the contacts page by clicking  , and the click to select or unselect from the pop-up menu, as illustrated below.



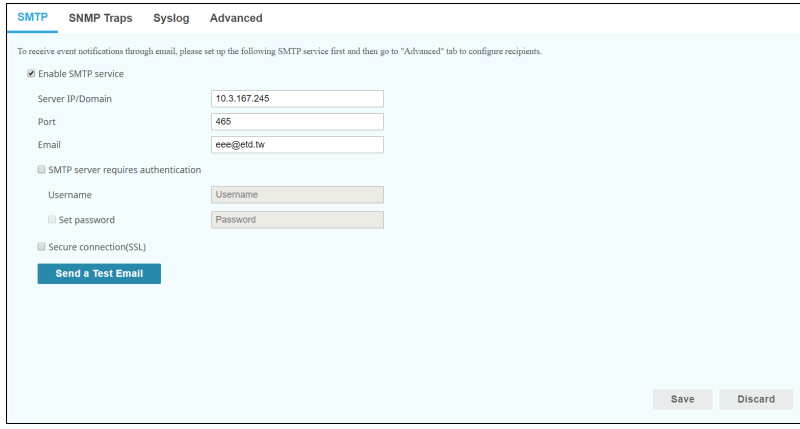
Notifications

The Notification menu offers four tab menu choices: SMTP, SNMP Traps, Syslog and Advanced. The default Notification page is SMTP, and it looks similar to the one below:



SMTP

The CC2000 can send email notification of events traps on the installation to specified users.



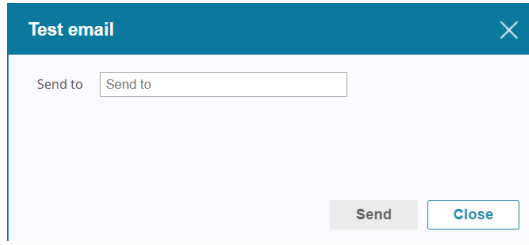
Note: Please set up the SMTP first and then go to *Advanced* tab to configure recipients, see page 226.

To enable SMTP server setting, do the following:

1. Check the **Enable SMTP service** checkbox.
2. Specify the IP address or domain name of the computer running your SMTP server in the **Server IP/Doamin** field.
3. Specify the port number in the **Port** field.
4. Specify the CC2000 administrator's email address in the **Email** 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 username and check the **Set password** checkbox to set password in the appropriate fields.
6. If you wish to secure the SMTP through SLL, check the **Secure connection(SSL)** checkbox.
7. Click **Send a Test Email** to check that the SMTP server setting is configured properly. A screen similar to the one below appears:



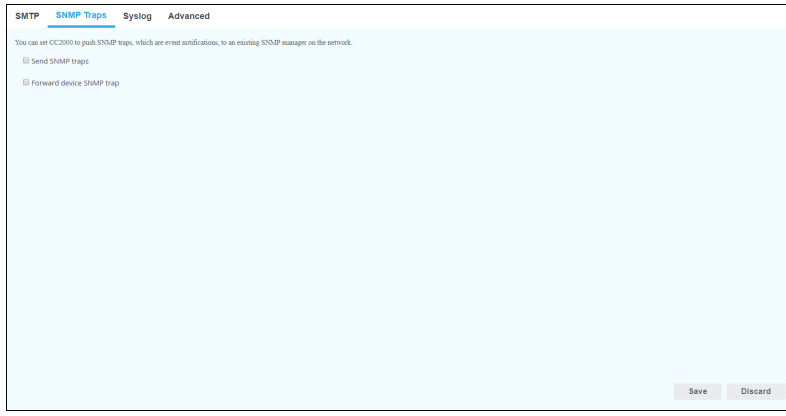
8. Key in an email address for the recipient of the test email then click **Send**. If the settings have been configured correctly, the recipient will receive the test email.

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

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

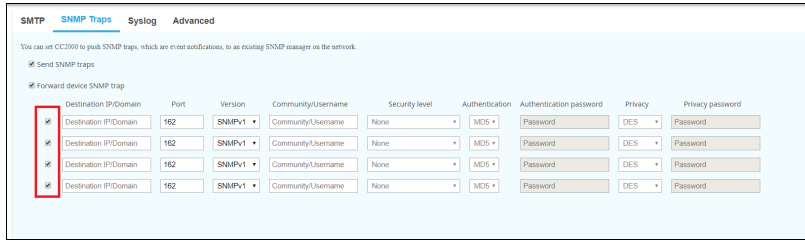
SNMP Traps

The SNMP Traps page lets you set your main SNMP trap settings, including information for up to four SNMP managers, as detailed below:



If you want to use SNMP trap notifications, do the following:

1. Check the **Send SNMP traps** checkbox to bring out the SNMP managers.
2. Check the **Forward device SNMP trap** checkbox if you want the trap information forwarded to a device.
3. Check the checkbox to configure the manager settings.



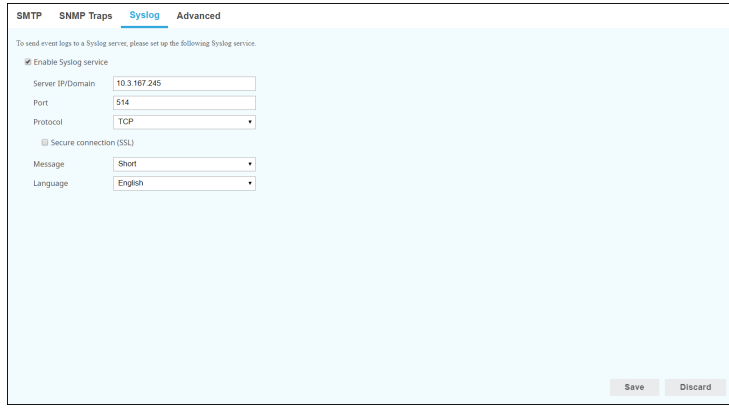
4. Key in the IP address(es) in the **Destination IP/Domain** field and the service port number(s) in the **Port** field of the manager computer(s) to be notified of SNMP trap events. The valid port range is 1–65535. The default port number is 162.

> **Note:** Make sure that the port number you specify here matches the port number used by the SNMP receiver computer.

5. Use the drop-down menu **Version** to select from one of the three options available, SNMPv21, SNMPv2c, and SNMPv3.
6. Key in the **Community/Username** value(s) for the SNMP version and select **Security level**.
7. Use the drop-down menu **Authentication** to select your authentication type, and key in the authentication password(s) in **Authentication password** field that correspond to each of the stations.
8. Use the drop-down menu **Privacy** to select your Privacy type and key in the privacy password(s) in **Privacy password** field that correspond to each of the stations.
9. Repeat steps 4–8 for up to three further SNMP managers.
10. When all your settings have been made, click **Save**.

Note: Make sure all the fields are filled in correctly so the system can successfully save your settings.

Syslog



To record all the events that take place on the CC2000 and write them to a Syslog server, do the following:

1. Check the **Enable Syslog service** checkbox.
2. Key in the IP address in the **Server IP/Domain** field and the port number of the Syslog server in **Port** field. The valid port range is 1-65535.

3. Use the drop-down menu **Protocol** to select the protocol type from two options: UDP and TCP.

   If TCP is selected, you can check the **Secure connection (SSL)** checkbox to enable secure connection (SSL).

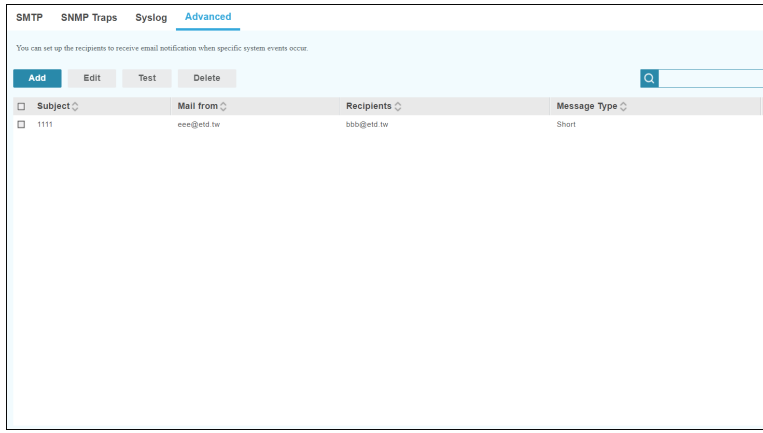
4. Use the drop-down menu **Message** to select whether to log a short message or a full message.

5. Use the drop-down menu **Language** to select the language you want the message to be sent in.

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

Advanced

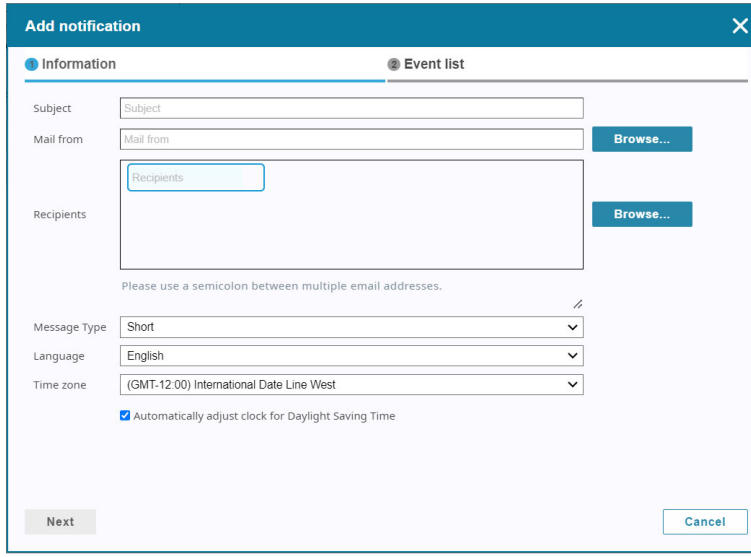
The Advanced page is used to inform select users of specified events that occurred on the CC2000. When you select Advanced, a page similar to the one below appears:



Adding Notification Settings

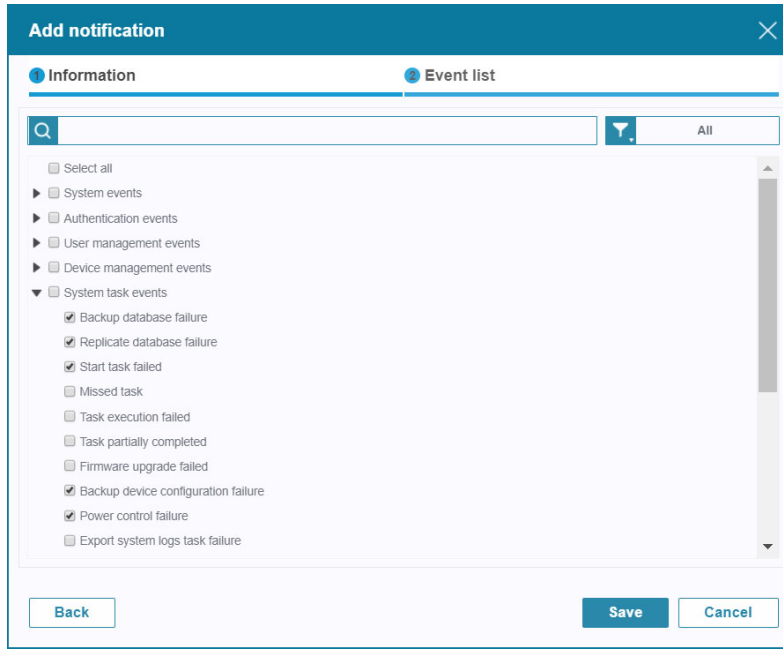
There are four buttons in the Advanced page: Add, Edit, Test, and Delete. Follow the instructions below to add users and specify the events they will receive notification of.

1. Click **Add** for the Add notification page:



2. Key an appropriate title for the notification message in the **Subject** field
3. Key in the email address of one of the administrators in the **Mail from** field.
4. Key in the email address of the person who will receive the email notification in the **Recipients** field. If you want the notification to go to more than one person, use a semicolon to separate the email addresses. There should not be a space before or after the semicolon.
5. Use the drop-down menu **Message Type** to select your message type, Full or Short.
6. Use the drop-down menu **Language** and **Time zone** to select the language and time you want the message to be sent in. Check the **Automatically adjust clock for Daylight Saving Time** checkbox if you are in a timezone that has Daylight Saving Time.

7. Click **Next** to select event(s) that you want to receive email notification of. You can use the filter on the top-right corner to help you see what you have selected. Select **Selected** to check the event(s) you have selected, or select **All** to display all the events.



8. When you have finished selecting the event(s) on this page, click **Save** to save your configuration and return to the Advanced page.

Note: In order for users to receive email notification of events, SMTP settings information must be configured on the CC2000's SMTP Settings page (see page 222 for details).

Edit Notification Settings

To modify a notification's settings, do the following:

1. Check the checkbox of the notification's name and click **Edit**.
2. Make your desired changes on the Information and Event list from **Edit notification** page.

3. When all your settings have been made, click **Save** at the bottom-right of the panel.

Testing Event Notifications

To test event notifications, do the following:

1. Check the checkbox of the notification's name and click **Test**.
2. If the system is working properly, the event notification recipient will receive an email with the event notification. If it fails, a fail message will appear.

Deleting Notification Settings

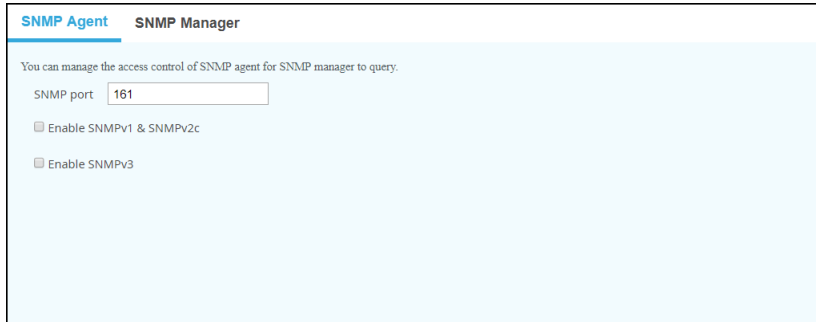
To delete a notification setting, check the checkbox of the notification's name and click **Delete**. A confirmation message will be shown, click **Yes** to proceed.

SNMP

The **SNMP** menu offers two tab menu choices: **SNMP Agent** and **SNMP Manager**. You can manage the access control of SNMP agent for SNMP manager to query. The default SNMP page is **SNMP Agent** and it looks similar to the one below:

SNMP Agent

The SNMP Agent page lets you set the CC2000's agents and control access for SNMP trap events, as detailed below:

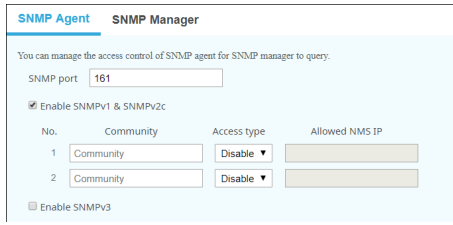


To set the SNMP agents, do the following:

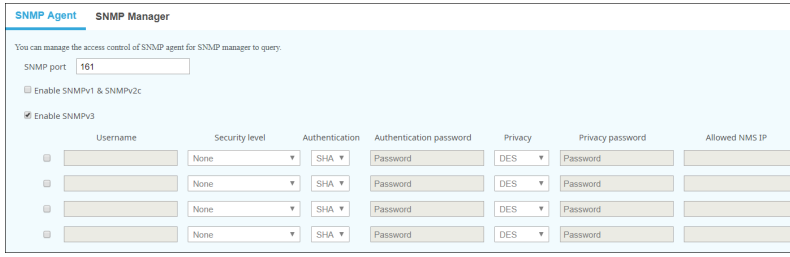
1. In the SNMP Port field, key in the port number(s) of the agent computer(s) that will collect trap event information. The valid port range is 1–65535. The default port is 161.

   Note: Make sure that the port number you specify here matches the port number used by the SNMP manager.

2. For SNMPv1 & SNMPv2c, check the **Enable SNMPv1 & SNMPv2c** checkbox and its configuration will be shown.



3. Key in the community name in the Community field and select the **Access Type** from the drop-down menu (Disable / Read / Write). If Read or Write is selected, Allowed NMS IP field will light up, fill in a NMS IP address.
4. For SNMPv3, check the **Enable SNMPv3** checkbox and its configuration will be shown.



5. Check the checkbox of the SNMP Agent, enter a Username in the username field and select a **Security Level** from the drop-down menu (None / Auth Protocol / Authentication & Privacy).
6. Select the **Authentication** protocols from the drop-down menu (MD5 / SHA) and key in the authentication password(s) in the Authentication password field.
7. Select the **Privacy** protocols and key in the privacy password in the Privacy password field.
8. Key in the allowed NMS IP address that correspond to each of the profiles in the Allowed NMS IP field.
9. Click **Save** to save your settings.

Note: Make sure all the fields are filled in correctly so the system can successfully save your configurations.

SNMP Manager

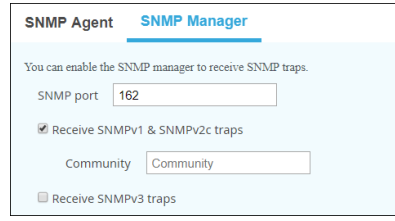
The SNMP Manager page lets you set the CC2000's management stations to receive notifications of SNMP trap events, as detailed below:

To set the SMNP managers, do the following:

1. In the SNMP port field, key in the service port number(s) of the computer(s) that will receive notifications. The valid port range is 1–65535. The default port is 162.

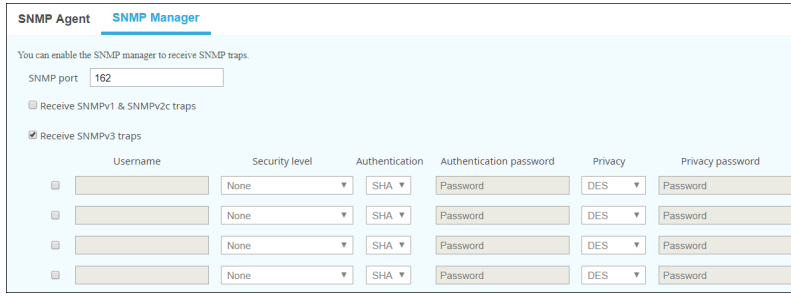
Note: Make sure that the port number you specify here matches the port number used by the SNMP agent computer.

2. For SNMPv1 & SNMPv2c, check the **Receive SNMPv1 & SNMPv2c traps** checkbox and a community field will appear.



3. Key in the community value(s) for the SNMP version.

4. For SNMPv3, check the **Receive SNMPv3 traps** checkbox and its configuration will be shown.



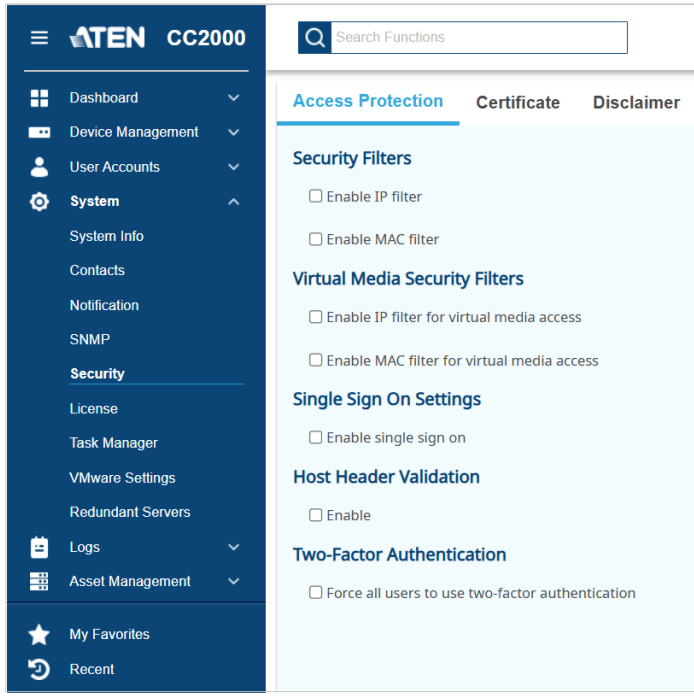
5. Check the checkbox of the SNMP Manager, enter a Username in the username field and select a **Security Level** from the drop-down menu (None / Auth Protocol / Authentication & Privacy).
6. Select the **Authentication** protocols from the drop-down menu (MD5 / SHA) and key in the authentication password(s) in the Authentication password field.
7. Select the **Privacy** protocols and key in the privacy password(s) in the Privacy password field.
8. Click **Save** to save your settings.

Note: 1. Make sure all the fields are filled in correctly so the system can successfully save your configurations.

2. To receive SNMP v3 traps from ATEN PDUs, you must select **MD5** and **AES-128** from the *Authentication* and *Privacy* drop-down lists, respectively.

Security

The **Security** menu offers three tab menu choices: **Access Protection**, **Certificate** and **Disclaimer**. This page provides a level of security by controlling access to the CC2000. The default Security page is **Access Protection**, and it looks similar to the one below:

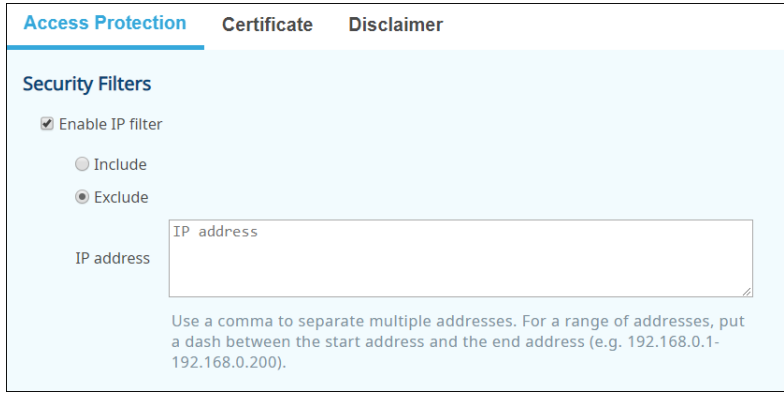


Access Protection

Security Fileters

- **IP Filtering**

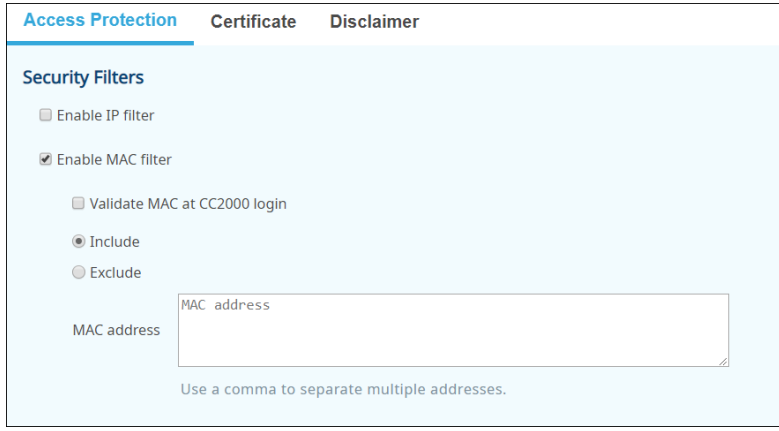
  IP filtering controls access to the CC2000 based on the IP addresses of the computers attempting to connect to it.



  - 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 while all others are denied access.
    - If the **Exclude** button is selected, all the addresses specified in the Address List are denied access while all others 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. Key the addresses directly into the **IP address** text input box as follows:
    - 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, key in the starting IP address, followed by a dash, then the ending IP address.
  - Click **Save** to save your settings.
  - To modify or delete a filter, make your changes directly in the **IP address** text input box.

- **MAC Filtering**

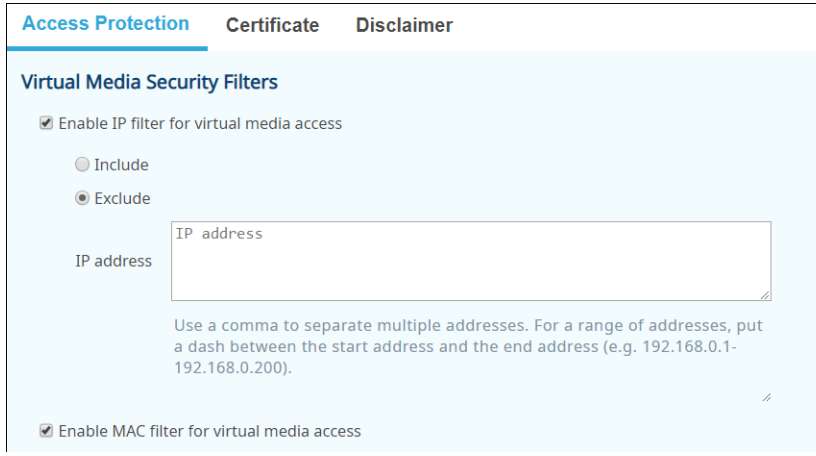
MAC filtering controls access to the CC2000 based on the MAC addresses of the computers attempting to connect to it.



- To enable MAC filtering, check the **Enable MAC filter** checkbox.
  - If **Validate MAC at CC2000 login** is enabled, the CC2000 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 while all others are denied access.
  - If the **Exclude** button is selected, all the addresses specified in the address list are denied access while all others 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. Key the addresses directly into the MAC address field. Use a comma between the addresses with no space before or after the comma(s).
- Click **Save** to save your settings.

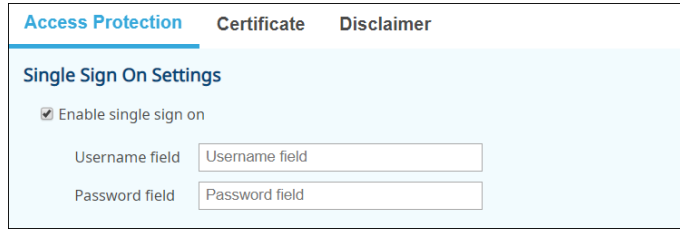
Virtual Media Security Filters

IP and MAC filtering can also be used to control Virtual Media access, based on the IP and MAC addresses of the computers attempting to use virtual media access.



- To enable Virtual Media Security Filters, check the **Enable IP filter for virtual media access** or **Enable MAC filter for virtual media access** checkbox and follow the instructions given in *IP Filtering*, page 235 or *MAC Filtering*, page 235.
- Click **Save** to save your settings.

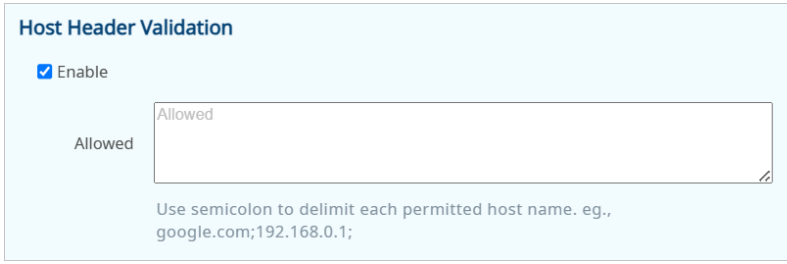
Single Sign On Settings



If **Single Sign On** is enabled, it will allow users to log in CC2000 automatically from another web application through a form-based authentication. To integrate, please refer to *SSO HTML Sample Codes* on page 443.

Host Header Validation

Enable **Host Header Validation** on the CC2000 to allow HTTP connections only when the requests come from a matching IP address or domain name, as specified in the **Allowed** list. This prevents host header attacks in which the host headers are tampered with.

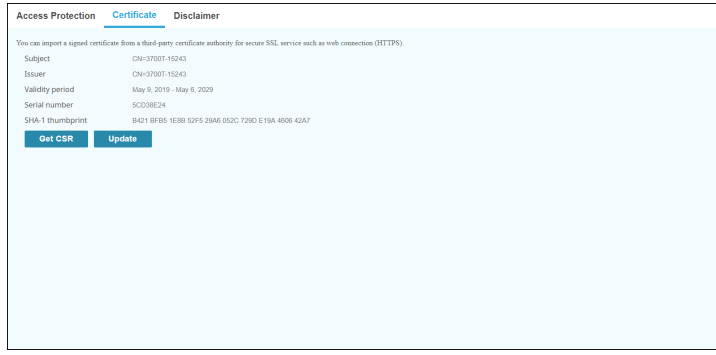


Certificate

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.

You can import a signed certificate from a third-party certificate authority for secure SSL service such as web connection (HTTPS).

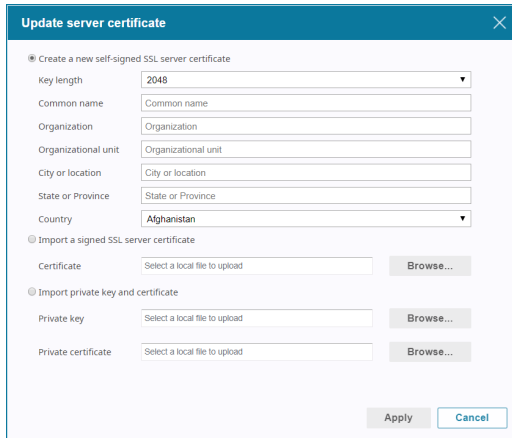
During installation, each CC2000 creates its own, independent, self-signed certificate based on the installation information similar to the one below:



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, do the following:

1. At the bottom-left of the page, click **Update** for the following page:



2. Check the **Create a new self-signed SSL server certificate** checkbox and fill in the fields according to the information in the table below:

Field	Description
Key length	Use the drop-down menu to select the key length (number of bits) for the certificate. Options are 1024, 2048, and 4096.
Common Name	This is the Fully Qualified Domain Name (FQDN) for which you are requesting the SSL certificate. For example: www.yourdomainname.com
Organization	This is 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. For example: accounting, marketing, etc.
City or Location	Key in the full name of the city or location. For example: Taipei
State or Province	Key in the full name of the state or province.

Field	Description
Country	This is the two letter country code for the country where the organization that the certificate is being registered to is located. **Note:** These don't always correspond to common abbreviations. If you are not sure of the code, you can do an online search for **ssl+country codes**.

3. When you have finished filling in the fields, click **Apply**.

   A message appears asking you to wait while the database gets updated with the new information. After a moment the web page closes.

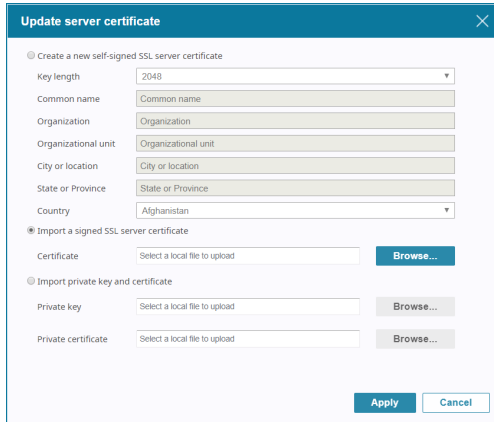
   At this point you are brought back to the beginning of the login sequence where you must go through the procedure of accepting the security certificate and logging in.

Importing a Signed SSL Server Certificate

In order to avoid users having to 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, do the following:

1. After generating the self-signed certificate, click **Get CSR** (Certificate Signing Request).
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 Certificate page, click **Update** at the bottom-left of the panel.

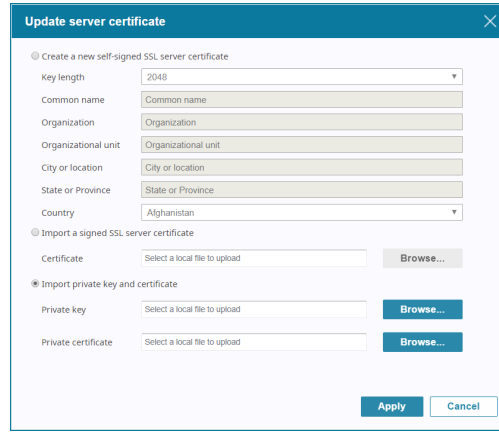


4. Check **Import a signed SSL server certificate** checkbox, then browse to where the certificate file is located and select it.
5. Click **Apply** at the bottom-right of the panel.

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.

Import Private Key and Certificate

When logging in over a secure (SSL) connection, a signed certificate is used to verify that the user is logging in to the intended site. For enhanced security, the Private Certificate section allows you to use your own private encryption key and signed certificate, rather than the default ATEN certificate.



There are two methods for establishing your private certificate: generating a self-signed certificate; and importing a third-party certificate authority (CA) signed certificate.

- Generating a Self-Signed Certificate

  If you wish to create your own self-signed certificate, a free utility – openssl.exe – is available for download over the web. See *Self-Signed Private Certificates*, page 370 for details about using OpenSSL to generate your own private key and SSL certificate.

- Obtaining a CA Signed SSL Server Certificate

  For the greatest security, we recommend using a third party certificate authority (CA) signed certificate. To obtain a third party signed certificate, go to a CA (Certificate Authority) website to apply for an SSL certificate. After the CA sends you the certificate and private encryption key, save them to a convenient location on your computer.

- Importing the Private Certificate

  To import the private certificate, do the following:

  1. Click **Update.**
  2. Click **Browse** on the right of **Private key**, locate your private encryption key file and select it.

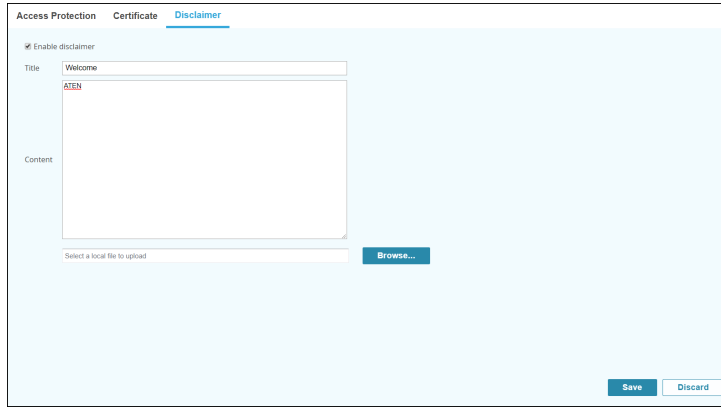
3. Click **Browse** on the right of **Private certificate**, locate your certificate file and select it.
4. Click **Apply** at the bottom-right of the panel.

Note: Both the private encryption key and the signed certificate must be imported at the same time.

Disclaimer

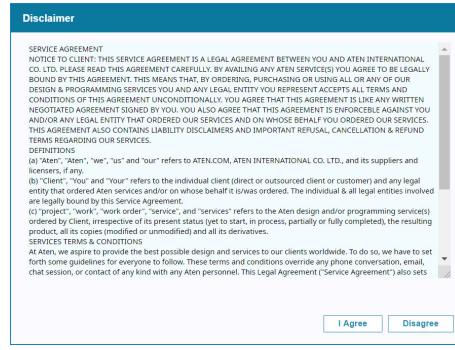
A disclaimer notice can be set up on the CC2000 server for users to accept when he/she logs into CC2000.

To set up a disclaimer, check the Enable disclaimer checkbox, enter the title and content of the disclaimer and click **Save**.



You can also click **Browse** to upload a previously saved disclaimer file.

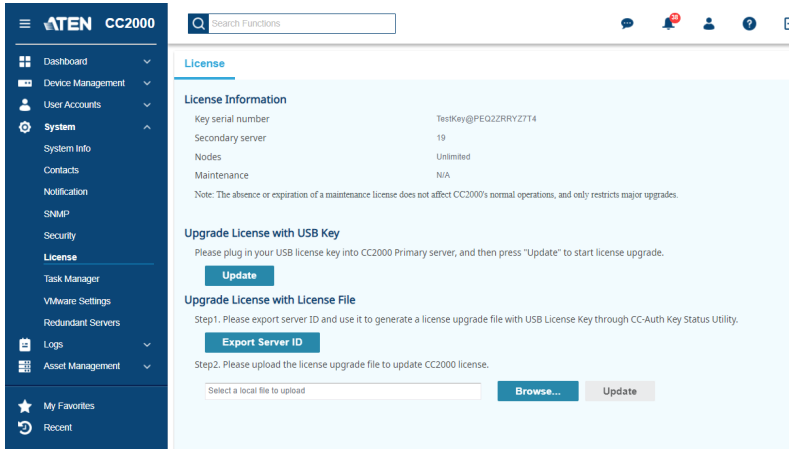
When logged in, the disclaimer message may look similar to the one below:



License

The CC2000 license controls the number of nodes permitted on the CC2000 server installation. The default license that comes with your purchase is a demo license for one Primary (no Secondaries), that allows 16 nodes. To add anything more (secondary servers and additional nodes), a purchased license and license update is required.

Select **License** from the System menu, a page similar to the one below appears:



The page items contained are described in the table below:

Section	Item	Description
License Information	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 CC2000 server. The license serial number can be found on the USB License key.
	Secondary server	The total number of secondary servers permitted (up to 31 units – depending on the license purchased).
	Nodes	The total number of nodes permitted on the installation according to the license purchased. **Note:** The number of nodes that can be licensed is unlimited.
	Maintenance	Indicates the valid period for updating the CC2000 software. When “N/A” is indicated, the maintenance license has not been applied to the license key. **Note:** ◆ With an expired maintenance license, the CC2000 system can still operate normally. However, updates will be limited to minor fixes, for example, from v4.0.109 to v4.0.201. ◆ A maintenance license is required for updating the system from v3.3 to v4.0 or later. To purchase or update a maintenance license, contact your local sales representative for more information..
Upgrade License with USB Key	Update	Click to upgrade license with the USB license key inserted.
Upgrade License with License File		This section is used to upgrade the license without directing inserting the USB License Key into the CC2000 server.

To update the license, contact your dealer to purchase a license key for the number of Secondaries and nodes desired. After receiving your purchased USB license key, you can update the license of the CC2000 through one of the two following methods:

- Upgrade license by directly inserting the license key into the server.
- Upgrade license without directly inserting the license key.

Upgrade License with USB Key

1. Insert the license key into a USB port on your primary server.
2. Click **Update** under Upgrade License with USB Key.

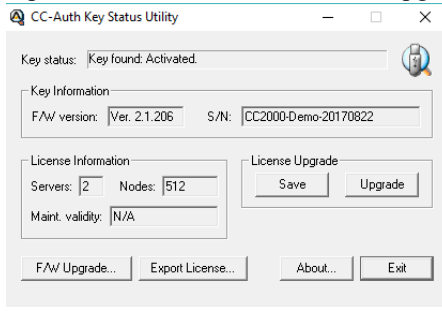
Note:

- Once the update has completed, it is no longer necessary to keep the license key plugged into the USB port. Remove the key and place it somewhere safe, since you will need it for future updates.
- If you lose the USB license key, contact your dealer 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.
- If the CC2000 is installed on a Windows Hyper-V virtual machine, the license may fail to update when using the USB license key. This is because Hyper-V cannot pass USB non-disk devices through to virtual machines. In this case, you can use a 3rd-party software such as USB Redirector to allow the virtual machine to access the USB license key for the update.

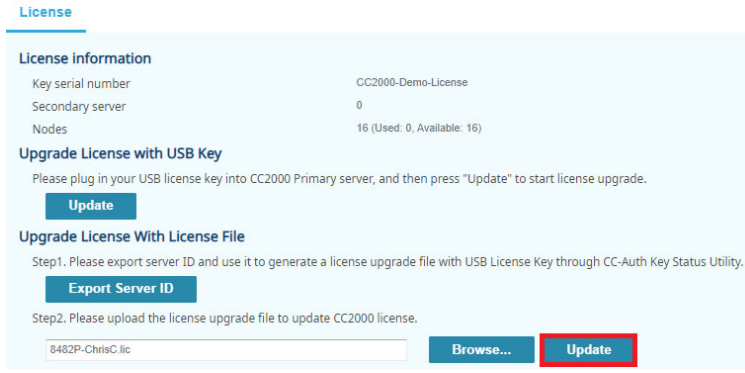
Upgrade License with License File

This method is useful when it is inconvenient to directly insert the USB license key into the CC2000 primary server, such as in a restricted area where USB connection is prohibited.

1. On the CC2000 primary server, click **Export Server ID** to generate a **.sid* server ID file, containing information about the server and its installation details. Export and save the file onto a separate PC.
2. On the separate PC, insert the USB license key.
3. Open CC-Auth Key Status Utility and click **Export License**, as illustrated below. You're asked to locate and select the server ID file generated from step 1. Once finished, a **.lic* license upgrade file is generated.



4. Import and save the **.lic* file into the CC2000 Primary's PC, and click **Browse** under Upgrade License with License File to locate it.
5. Click **Update** to initiate the license upgrade.



Note: The license upgrade file can only be used to upgrade the license of the CC2000 server from which the server id file was generated.

License Sharing

The number of licenses for authorized devices on a CC2000 installation is set on the primary server through the license key, and are shared by all the CC2000 servers. Information about the number of licenses is sent to each Secondary at the time that it registers with the Primary (see *View Properties*, page 270).

Although there is no limit to the number of devices that can be added to the CC2000 management system, only as many nodes as there are licenses for can actually be used for port management (see *Preliminary Procedures*, page 67).

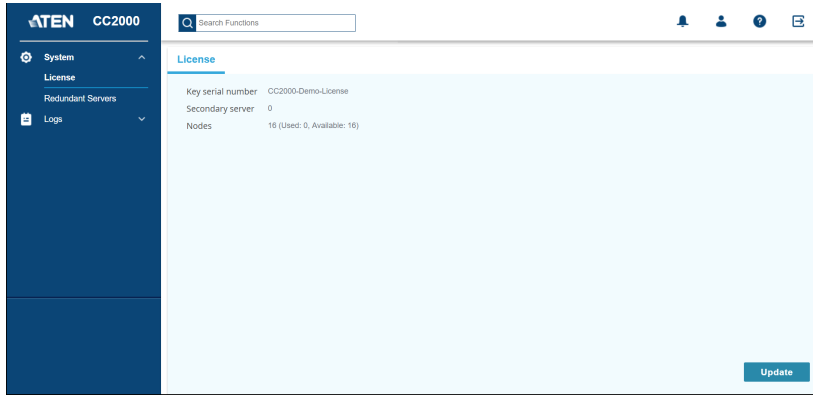
When devices are added to the CC2000 management system, their configurations are locked by default. Although having configuration information stored on the CC2000, they cannot be managed.

Locked ports can be unlocked either by selecting a physical port and unlocking it by clicking the **Unlock** button (see *Locking / Unlocking Devices*, page 124), or by making the port part of an aggregate device (see *Adding an Aggregate Device*, page 100).

If all of the license nodes are in use, only after a currently unlocked port is locked, or after an aggregate device is deleted – thereby freeing up the license it was using – can a locked port (or new aggregate device) be unlocked and managed by the CC2000 management system.

License Conflict

When there are two Primaries on the same network segment that have been upgraded with the same license key, a license conflict occurs. The Browser GUI of the CC2000 server that was the second one to be installed opens a page that looks similar to the one below:



To confirm that a conflict has occurred, click the **Logs** tab. The following sentence is displayed in the log file: A license violation has been detected at primary server. Remote CC server (IP: [the conflicting servers' IP]).

When this occurs, there are a number of ways to resolve the conflict:

1. On one of the two Primaries: either shut it down, stop service, disconnect it from the network, or uninstall the CC2000 entirely.
2. Register the conflicting CC2000 (the second one) with the normal one (the first one). The Registered CC2000 becomes a Secondary. (This assumes that there is a Secondary license available.)
3. If you would really like to have two independent CC2000 installations, contact your dealer to purchase a separate key for the second CC2000 server.

Task Manager

The **Task Manager** menu offers four configuration choices: **Add**, **Edit**, **Run Now**, and **Delete**. This page 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:

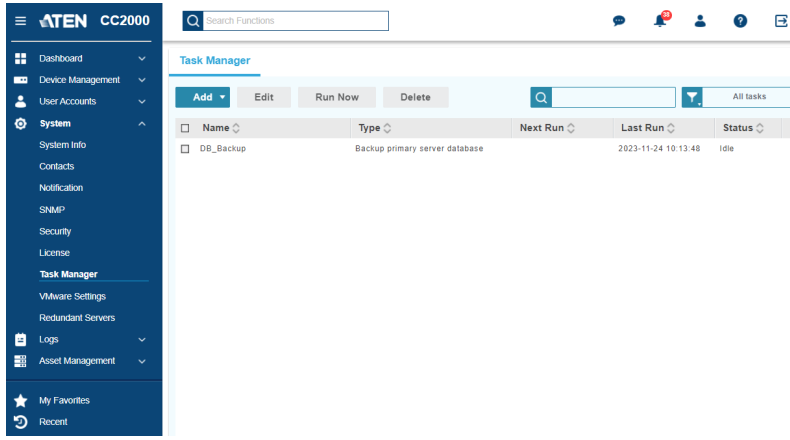
- Backup primary server database

Note: 1. This task is only available on a Primary CC2000

2. Restoring the database requires a separate utility and procedure. See *Restore*, page 373, for details.

- Power control a device
- Auto upgrade with the latest device firmware
- Upgrade device firmware
- Backup device configuration
- Export event logs
- Export device log
- Export serial console history

When you select **Task Manager** from the System menu, the following screen appears:



Note: This figure depicts a page for a primary server. The page for a secondary server is similar, except that it has a pre-configured default entry, *Replicate Database*, that replicates the database of the Primary it is connected to (see *Replicate Database*, page 266).

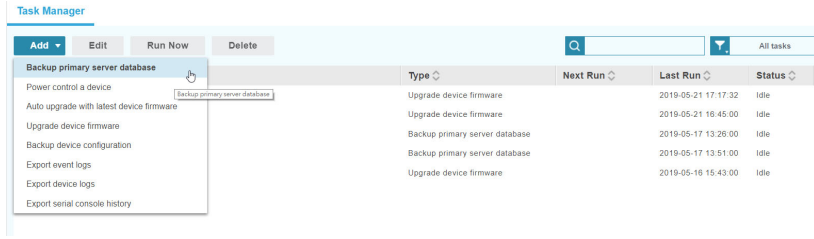
The **Task Manager** table lists all the tasks that have been configured. The meaning of each heading is explained in the table below:

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

Add

To add a task, do the following:

1. Click **Add**, a list of task choices is shown:

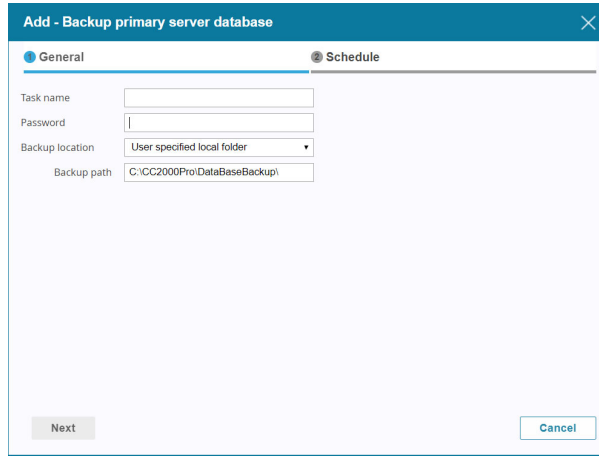


2. Click to select the task you want to add. A pop-up window appears containing contents based on the task selected.

While each task is different, most of the procedures involved in setting them are similar. The following examples take you through the various task procedures you may encounter.

Backup Primary Server Database

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



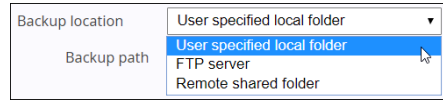
1. Provide a name and a password for the task.

Note: 1. This task is only available on the primary server.

2. Make a note of the password and store it somewhere safe. You will need it when restoring the database. (If you don't set a password, you can restore the database without one.) See *Restore*, page 373, for information on restoring the database.
3. The password cannot exceed 32 English alphanumeric characters.
4. The extension of the backup file is cbk (`*.cbk`).

---

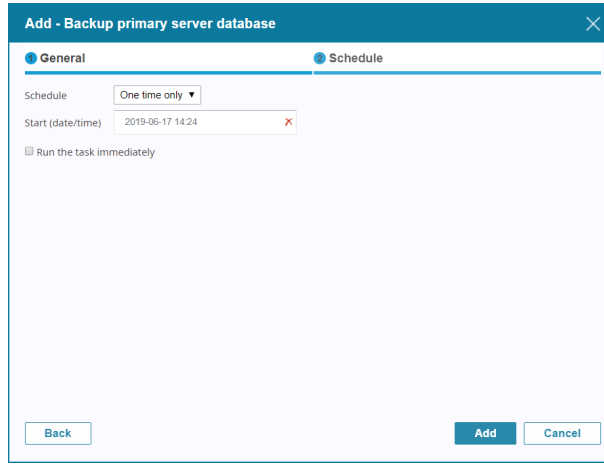
2. Select the **Backup location** where you want to store the backup file. There are three options to choose from, **User specified local folder**, **FTP server**, and **Remote shared folder**.



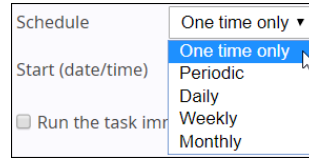
- By default, the backup file is stored in the local installation directory of the CC2000. For example, `C:\CC2000Pro\DataBaseBackup`.

- Fill in the rest of the fields if you choose FTP server or Remote shared folder.

3. When you have filled in all of the information, click **Next** for the Schedule page.



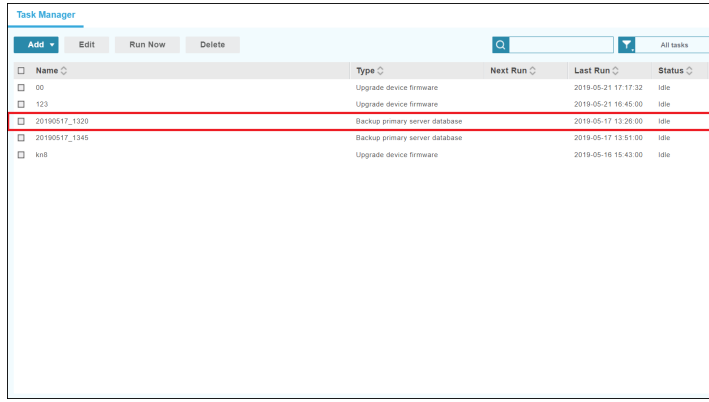
4. Use the drop-down menu Schedule to see a list of available choices.



Depending on schedule selection, further scheduling choices may appear. For examples, if you choose One time only, the Start (date/time) appears. If you choose Periodic, the Optional period field appears.

Note: If you set a time in the schedule for the backup to take place (Monthly, for example), but you want it to start from this month, make sure you set the start date or time to later than the date or time shown on the page and uncheck Run the task immediately. Since the time setting on the page shows the time that you accessed the page, it shall have passed by the time you save your changes, meaning the CC2000 will not execute the task until next month.

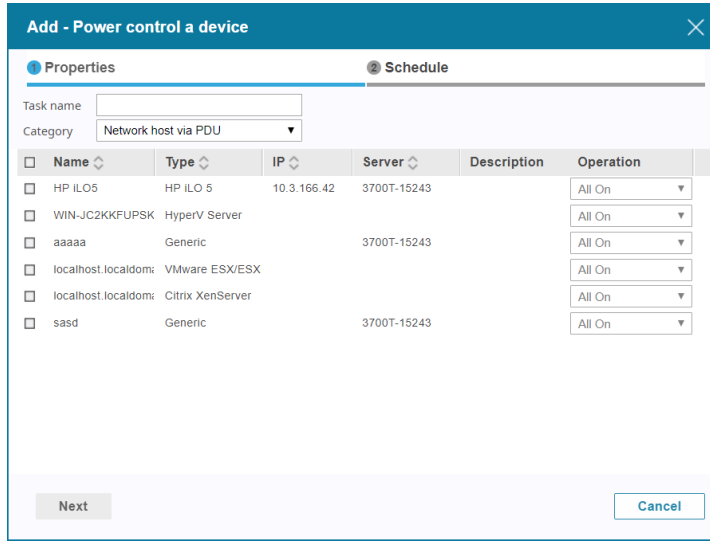
5. When you have finished making your schedule choices, click **Add**.
   The task is now added to the Task List on the main page.



Note: You can run a task (or tasks) at any time by checking the checkbox and click **Run Now**.

Power Control a Device

This task allows you to set a time schedule that automates turning power ports on and off.



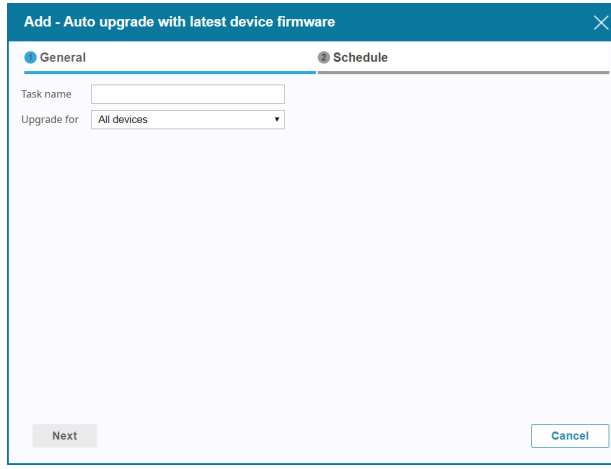
1. Provide a name for the task.
2. Choose to turn on or off for the selected device as a whole, or on a port-by-port basis by clicking and selecting from the Category drop-down menu.
3. Check the checkbox of the target devices or ports you want to control, or check the checkbox in front of Name at the top of the column to select all.
4. Select whether to turn the ports On or Off in the Operation column.
5. Click **Next**, and make your schedule choices in the Schedule page.

Note: Refer to *Backup Primary Server Database* on page 252 for schedule setting procedures.

6. Click **Add** to finish setting up the task.

Auto upgrade with the latest device firmware

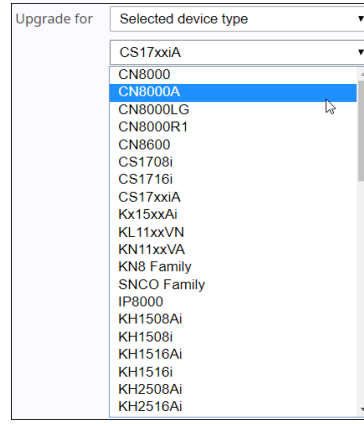
This task allows you to schedule auto device firmware upgrade with the newest available firmware.



1. Provide a name for the task.
2. Use the drop-down menu **Upgrade for** to choose which appliances will receive the auto upgrade from one of the three options, **All devices**, **Selected device type**, and **Selected device**.

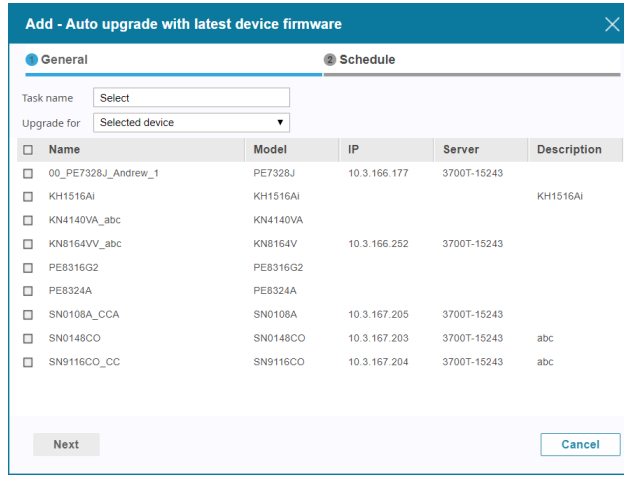
3. If you choose All devices (recommended), all the devices are automatically selected for the upgrade.

   If you choose Selected device type, use the drop-down menu to select the device type you want to upgrade.



   If you choose Selected device, check the checkbox of the device(s) you want to upgrade, or check the checkbox in front of Name at the top of the column to select all of them.

Note: The Device list is sortable by Name, Type, and IP.



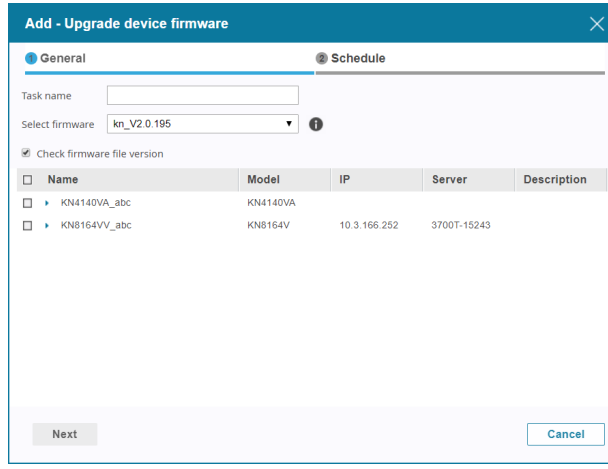
4. When finished, click **Next**, and make your schedule choices in the Schedule page.

Note: Refer to *Backup Primary Server Database* on page 252 for schedule setting procedures.

5. When finished, click **Add** to add the task.

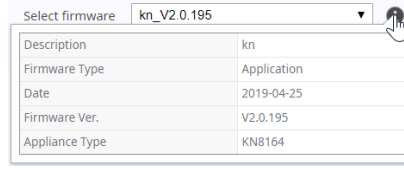
Upgrade device firmware

This task allows you to schedule the device firmware upgrade from the firmware repository.



1. Provide a name for the task.
2. Select the firmware file from the **Select firmware** drop-down menu. The firmware files are from the firmware repository.

   After selecting a firmware file, clicking the information icon will display the information of the firmware. An example is shown below:



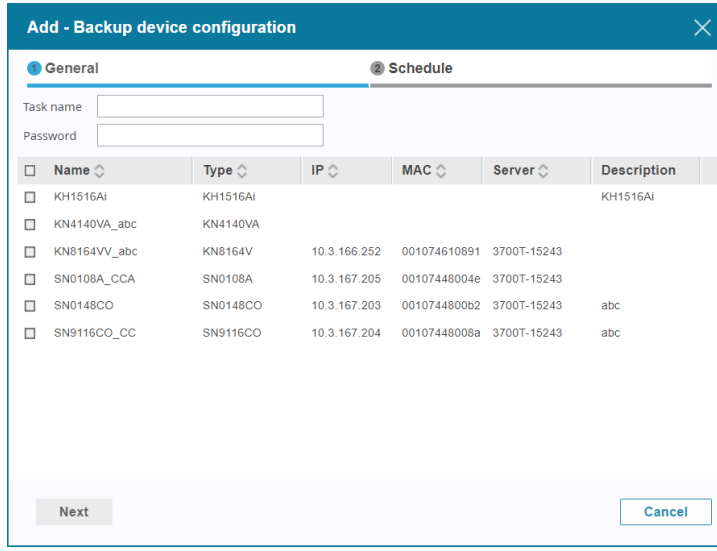
3. Selecting a firmware file will display all the devices available for firmware upgrade in the table below.
4. Check the checkbox(es) of the device you wish to upgrade and click **Next**.
5. When finished, click **Next**, and make your schedule choices in the Schedule page.

Note: Refer to *Backup Primary Server Database* on page 252 for schedule setting procedures.

6. When finished, click **Add** to add the task.

Backup Device Configuration

When you choose the Backup device configuration task, the following page appears:



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

Note: Make a note of the password and store it somewhere safe. You will need it for restoring the configuration. See *Restore Configuration*, page 152 for restoration details.

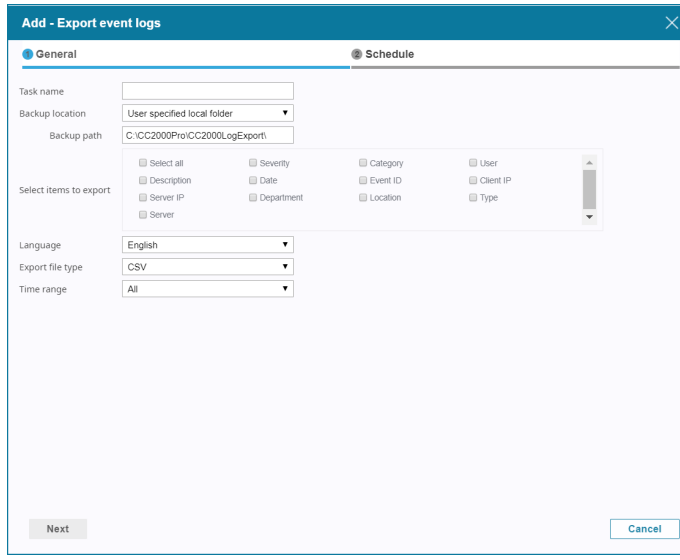
2. In the Device list, check the checkbox(es) of the device(s) you want to back up.

Note: When finished, click **Next**, and make your schedule choices in the Schedule page.Refer to *Backup Primary Server Database* on page 252 for schedule setting procedures.

3. When finished, click **Add** to add the task.

Export Event Logs

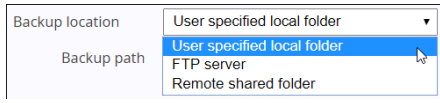
When you choose the Export event logs task, the following page appears:



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

Note: The Export event logs operation is performed on each server independently. To search for a server's records, you must look via its particular file. You can identify the file by the Task name you define.

2. Select the **Backup location** where you want to store the backup file. There are three options to choose from, **User specified local folder**, **FTP server**, and **Remote shared folder**.



   - By default, the backup file is stored in CC2000's local installation directory. For example, `C:\CC2000Pro\CC2000LogExport`.
   - Fill in the rest of the fields if you choose FTP server or Remote shared folder.

3. In the Select items to export table, check to select item(s) you want to include in the exported file.

Note: Check the Select all checkbox to select all items.

4. You can use the Language drop-down menu to select a different language.
5. In the Export file type drop-down menu, you can select your preferred export file type. If you choose one of the encryption options (Encrypt file with AES or Encrypt file with DES), define a password in the Password field.

Note: Make a note of the password – you will need it to import the file.

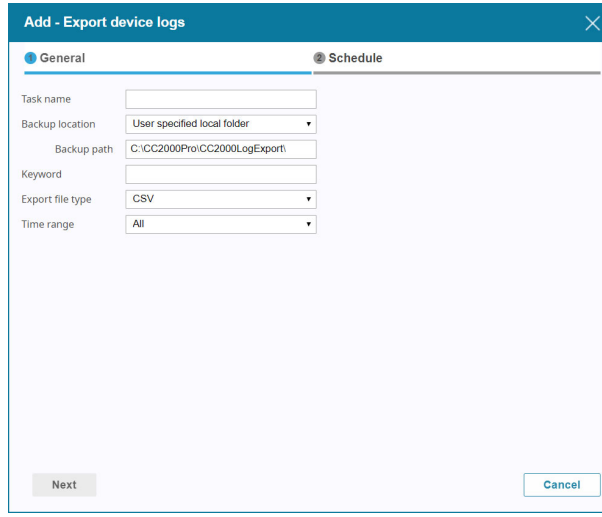
6. In the Time range drop-down menu, there are three options.
   - **All**: Exports all of the records in the database.
   - **Since the last time task run**: Exports all task records since the last time they were run.
   - **Select time range**: Export records within a particular time period, set the time parameters in the From and To fields.
7. When finished, click **Next**, and make your choices in the Schedule page.

Note: Refer to *Backup Primary Server Database* on page 252 for schedule setting procedures.

8. When finished, click **Add** to add the task.

Export Device Logs

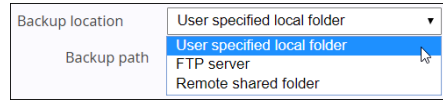
The CC2000 also acts as a log server for all ATEN KVM devices where CC2000 records the system events that take place on the devices in a database. This task allows you to export the device records from their databases as a file. When you choose the Export device logs task, the following page appears:



1. Provide an appropriate name for the task. For example, if you want to export the device log for all devices, you could name the task All-device-logs; if you want to export the device log for CN8000 devices on a weekly basis, you could name the task cn8000-weekly-device-log.

Note: The Export device logs operation is performed and stored on each server independently. To search for export log records, you must access each server individually.

2. Select the **Backup location** where you want to store the backup file. There are three options to choose from, **User specified local folder**, **FTP server**, and **Remote shared folder**.



- By default, the backup file is stored in CC2000's local installation directory. For example, `C:\CC2000Pro\CC2000LogExport`.

- Fill in the rest of the fields if you choose FTP server or Remote shared folder.

3. You can use the Keyword field as a filter to limit the scope of the log file. For example, to export a file that only contains event information for CN8000 devices, and all your CN8000 devices had CN8K as part of their names, you could key CN8K into the Keyword field.
4. In the Export file type drop-down menu, you can select your preferred export file type. If you choose one of the encryption options (Encrypt file with AES or Encrypt file with DES), define a password in the Password field.

Note: Make a note of the password – you will need it to import the file.

5. In the Time range drop-down menu, there are three options.
   - **All**: Exports all of the records in the database.
   - **Since the last time task run**: Exports all task records since the last time they were run.
   - **Include**: Export records within a particular time period, set the time parameters in the From and To fields.
   - **Exclude**: Export all records but exclude the records in the time period specified. Set the time parameters in the From and To fields.
6. When finished, click **Next**, and make your choices in the Schedule page.

Note: Refer to *Backup Primary Server Database* on page 252 for schedule setting procedures.

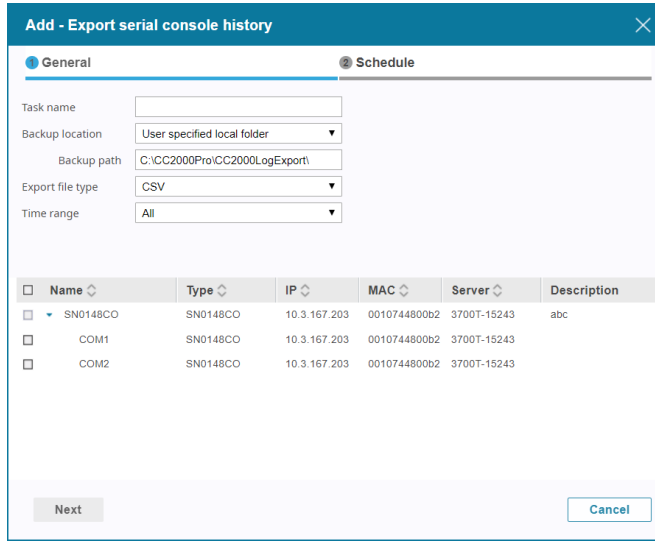
7. When finished, click **Add** to add the task.
8. When you have finished with this page, click **Next** at the bottom-left of the panel for the Schedule page.
9. Make your schedule choices in the Schedule page that comes up.

   Note: The schedule choices are similar to the ones described for the *Backup Primary Server Database* task.

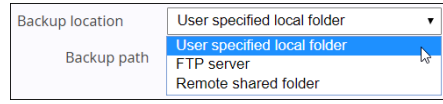
10. When you have finished making your schedule choices, click **Add**.

Export serial console history

The CC2000 keeps a record of all user sessions that take place (see page 276). This function lets you save and export the serial console history of each device. When you choose the Export serial console history task, the following page appears:



1. Provide a name for the task.
2. Select the **Backup location** where you want to store the backup file. There are three options to choose from, **User specified local folder**, **FTP server**, and **Remote shared folder**.



   - By default, the backup file is stored in CC2000's local installation directory. For example, `C:\CC2000Pro\CC2000LogExport`.
   - Fill in the rest of the fields if you choose FTP server or Remote shared folder.

3. In the Export file type drop-down menu, you can select your preferred export file type. If you choose one of the encryption options (Encrypt file with AES or Encrypt file with DES), define a password in the Password field.

Note: Make a note of the password – you will need it to import the file.

4. In the Time range drop-down menu, there are three options.
   - **All**: Exports all of the records in the database.
   - **Include**: Export records for a particular time period, set the time parameters in the From and To fields.
   - **Exclude**: Export all records but exclude the records in the time period specified. Set the time parameters in the From and To fields.
5. For the device list, check the checkbox(es) of the desired device(s), or check the checkbox in front of Name at the top of the column to select all.

Note: If you prefer to export the serial console history for selected ports only, instead of clicking the device's checkbox, click the arrowhead in front of its name to expand the port list to select individual ports.

6. When finished, click **Next**, and make your choices in the Schedule page.
7. Make your schedule choices in the Schedule page.

Note: Refer to *Backup Primary Server Database* on page 252 for schedule setting procedures.

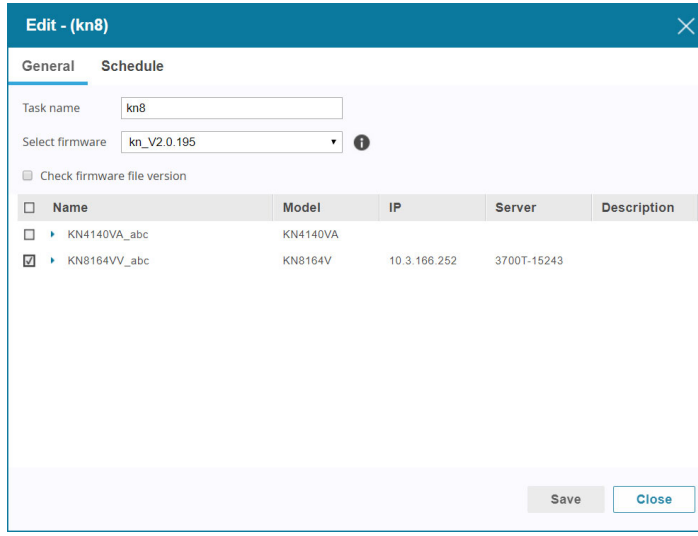
8. When finished, click **Add** to add the task.

Editing a Task

There are two categories you can edit: changing a task's General settings and its Schedule settings.

To edit a task, do the following:

1. In the Task Manager list, check the checkbox of the task you want to edit.
2. Click **Edit**. An Edit dialog box appears, as exemplified below:



For the different tasks and the editable parameters, refer to *Add* on page 251 for more information.

After editing the parameters, click **Save** to finish.

Run Now

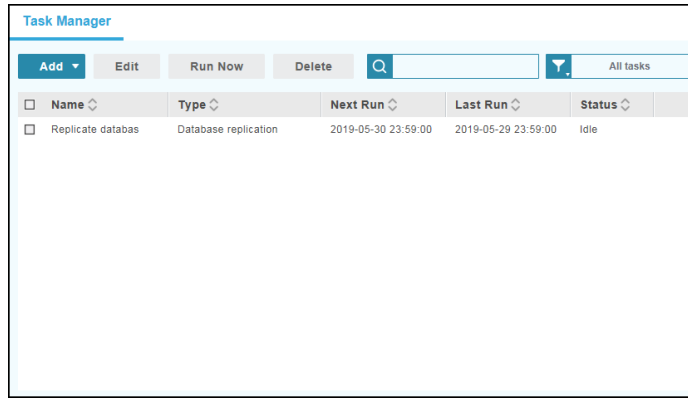
Use **Run Now** to immediately execute the task. Check the checkbox of the task and click **Run Now**.

Deleting a Task

Use **Delete** to delete task(s). Check the checkbox of the task and click **Delete**.

Replicate Database

The Task Manager page for a secondary server is similar to that of a primary server, except that it has a pre-configured default entry, Replicate Database, that replicates its database on the Primary it is connected to:



When you check the checkbox Replicate Database and click Edit, the Edit page comes up. The procedures are similar to the ones described for Editing a task. Refer back to page 265 for details.

Note: 1. Each CC2000 server maintains its own individual database for its accounts, logs, devices, and access rights that are configured on it. By replicating, it sends all of the information contained to be incorporated into the Primary's database and made available to the rest of the CC2000 management system.

2. When the Secondary registers with a Primary, its database is automatically replicated.

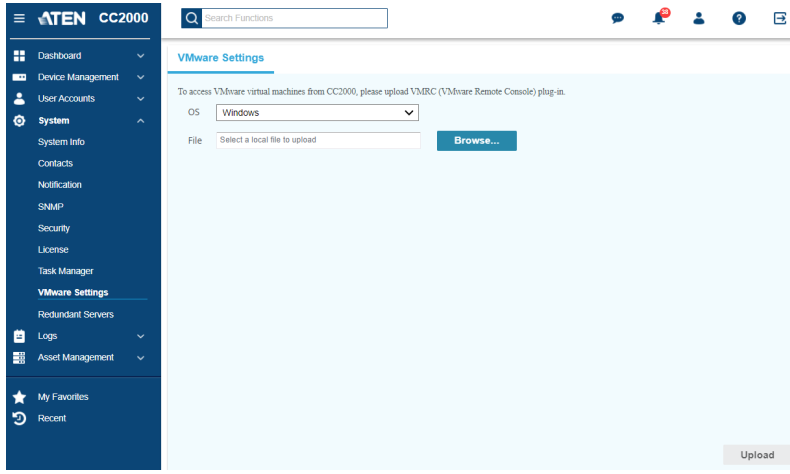
3. By default, the database is automatically replicated once a day at 00:00. You can use this page to change the replication schedule, but be aware that setting a replication schedule that performs database replication too frequently may adversely influence your system performance. If you set the schedule to too large of an interval, there can be a long time period when the databases don't match.

When you have made the schedule choices you want, click **Save**.

VMware Settings

VMRC Plugin

The VMware Remote Console (VMRC) plugin lets you access a VMware virtual machine from the browser. You will need to install this plugin if you have added a VMware virtual machine to your CC2000 management system. When you select the VMware Settings Panel Menu entry, a page similar to the one below appears:



To install the plugin, do the following:

1. Download the plugin from the VMware website.
2. Use the OS drop-down menu to select the operating system.
3. Click **Browse** to select the file downloaded from step one.
4. Click the **Upload** button.

Installing Xterm

If the operating system of the port you are accessing is running Ubuntu 18.04_x64, CentOS 7.5_x64, or Debian 9.5_x64, you must install Xterm to run VMRC properly.

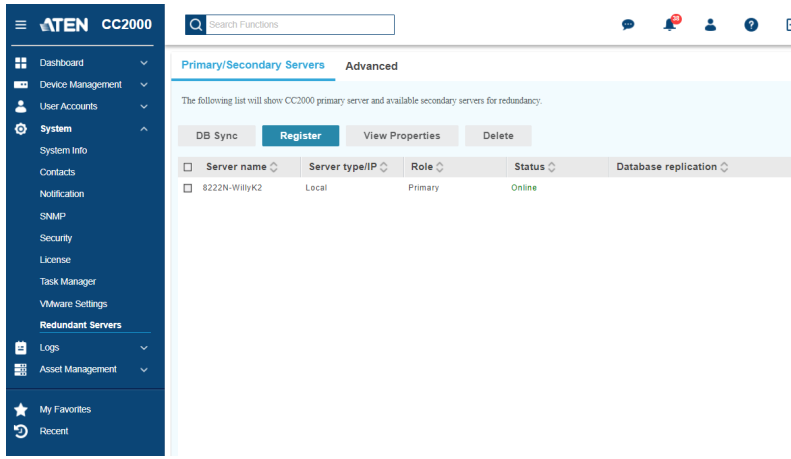
On the terminal, execute the following commands:

```
sudo apt-get update
```

```
sudo apt-get install xterm
```

Redundant Servers

The **Redundant Servers** menu offers two tab menu choices: **Primary/ Secondary Servers** and **Advanced**, as displayed below:



Primary/Secondary Servers

The Interactive Display Panel provides a table listing the CC2000 servers, along with some corresponding basic information. A green online status means that the server is currently accessible. A red offline status means that it is currently inaccessible.

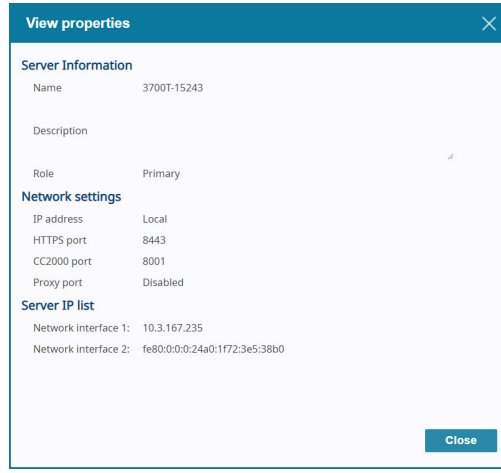
The definitions of the Server table headings are explained below:

Heading	Meaning
Server Name	The name given to the server.
Server Type /IP	*Local* indicates the CC2000 that you have logged into. For other CC2000s on the installation, the term *Remote* and the CC2000's IP address appears.

Heading	Meaning
Role	The two major roles in the CC2000 management system are Primary and Secondary. In addition, there is a third role, *Substitute Primary*, in which one of the Secondaries temporarily takes over the Primary's role should the Primary become disconnected from the system (due to network problems, for example). The Substitute Primary returns to its Secondary status when the Primary comes back online. **Note:** 1. The CC2000 that acts as the Substitute Primary is automatically chosen by the CC2000 management system. The choice is based on the CC2000 registration sequence (the earliest secondary CC2000 to register with the Primary becomes the Substitute Primary). 2. The Substitute Primary takes the Primary's role in regard to providing centralized management control – it cannot be used to add or delete devices; it cannot register secondary servers; Secondaries cannot replicate their databases to the Substitute Primary.
Status	Indicates whether the CC2000 is online or offline

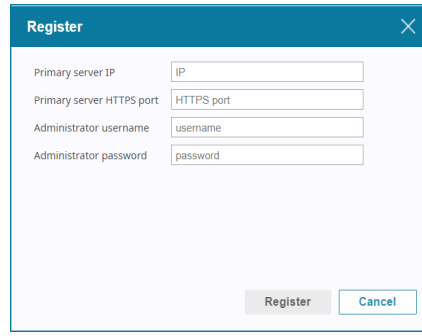
View Properties

To view the properties of each server, check the checkbox of the server you want to view and click **View Properties**.



Register

The **Register** button is used to integrate a CC2000 server as a Secondary into a larger CC2000 network. Click **Register** for the following page.



Fill in the details of the primary server and click **Register**.

After the registration completes, you are automatically logged out. When you log back in, your server now appears as a Secondary on the Primary's installation.

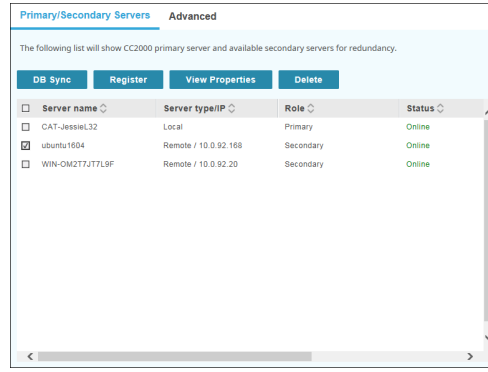
Note: 1. For the *Administrator username* and *Administrator password* fields, you must use a valid Super Administrator's or System Administrator's username and password.

2. After registration, most of the original data on the formerly independent CC2000 (Primary or Secondary) is lost. As a secondary server, it will now get the majority of its data from the primary server it is registered with. Any devices that are connected to the newly registered Secondary have to be added again.

3. Users logged into other CC2000 servers on the installation may not see your CC2000 right away. Refreshing the page may be needed such as leaving the System Management page and come back to it again.

4. In some cases, you may have to clear your browser cache in order to see the change.

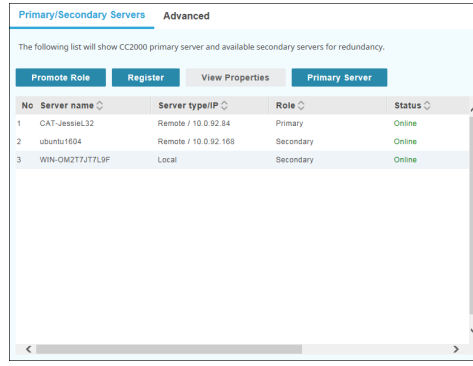
Primary Server View



To delete secondary server(s), check the checkbox of the secondary server(s) and click **Delete**.

To synchronize primary server database to secondary server(s), check the secondary server(s) and click **DB Sync**.

Secondary Server View



■ Promote

The **Promote** button is used to transform a Secondary CC2000 to a Primary. When you click this button, the change takes place automatically with the former Primary now becoming a Secondary and all other online Secondaries automatically recognizing the new Primary.

Note: 1. To see the newest changes, refresh the page such as going to a different page and come back.

2. We recommend all CC2000 servers on the installation to be online at the time of role promotion. If any Secondaries are offline at the time of role promotion, they must perform the Primary Settings procedure again. (See *Primary Server*, page 273, for details.) If the old Primary is offline at the time of role promotion, it must Register with the new Primary when it comes back online. See *Register* on page 271 for details.

■ Primary Server

This function is used for the following scenarios:

- If the Primary's IP address changes.
- If the Secondary is offline at the time the Primary's CC Port or HTTPS Port changes.
- If the Secondary is offline at the time that a different CC2000 is promoted from Secondary to Primary.

When these situations occur, there is no need to go through the *Register* procedure to maintain the Primary/Secondary connection. The administrator can use this function to update the information accordingly.

To maintain the connection, simply type the new IP address and/or port settings (of the Primary) and click **Save**.

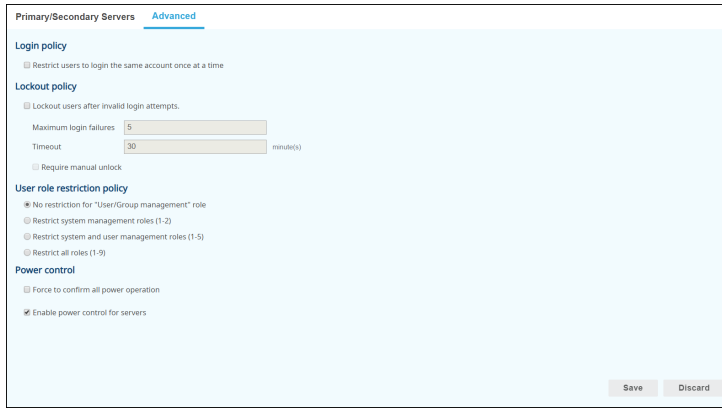
Note: 1. Since the IP address change is made at the OS level (not the CC2000 service level), the CC2000 system is unaware of the change. Thus the Primary can't change this information on the Secondaries automatically. It must be done manually on all Secondaries.

2. Any CC2000 Secondary that is offline will not be automatically notified at the time of change, therefore this procedure must be performed at the time the Secondary comes back online.

3. This procedure allows any changes in the database that occurred when the Secondary was not in communication with the Primary to be merged into a common database. This is preferable for CC2000s that were originally part of the same system but temporarily lost communication with each other. Using this function would prevent losing any updated database information it added while it was separated from the primary server.

Advanced

The Advanced tab offers four setting categories: Login policy, Lockout policy, User role restriction policy and Power control.



Login policy

Check the Restrict users to login the same account once at a time checkbox if you don't want users to be able to log in more than once at the same time.

Note: Default setting for Login policy allows users to log in with the same account more than once at a time.

Lockout Policy

- To lock users out after a specified number of failed login attempts, check the checkbox in front of Lockout users after invalid login attempts. 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, we recommend that you enable the lockout policy.

- Key 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.

- Key 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 *Unblocking User Accounts*, page 180, for details. The default is disabled (no check in the checkbox).

User role restriction policy

This setting category allows an administrator to create user accounts with either no role restrictions or with one of three pre-set role restriction policies. Options are as follows:

- No role restrictions
- Restrict system management roles (1–2)
- Restrict system and user management roles (1–5)
- Restrict all roles (1–9)

Note: For full details of roles 1–9, please see the table under *System User Types*, page 182.

Power control

This setting category allows an administrator to set power control over devices and servers for users.

Enabling Force to confirm all power operation means the users are forced to make power operation confirmation on all of the connected devices regardless of the setting on the outlet.

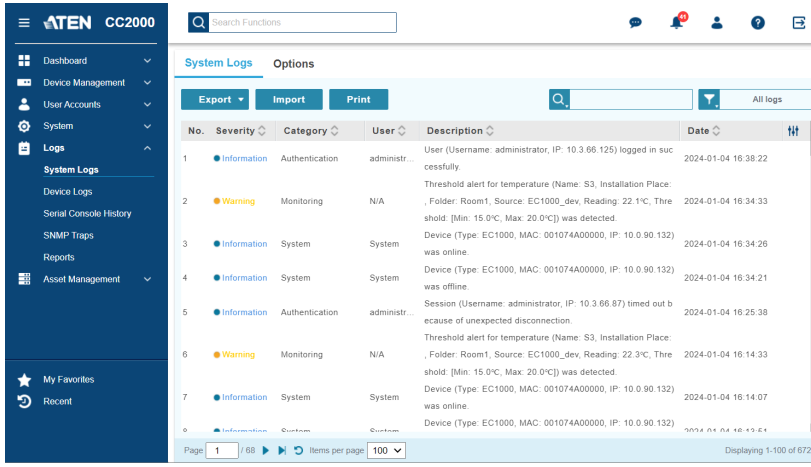
Enabling Enable power control for servers means if the third-party servers supports power control, they are allowed to perform power control. Otherwise, the related power control functions will be removed from the menu.

Chapter 8
Logs

Overview

The CC2000 keeps an extensive record of all of the actions that take place on management system. The Logs page provides a powerful array of filters and functions that allow you to view and export the desired log file data, as well as receive email notifications of specified events as they occur.

When you click the Logs menu, the CC2000 directs you to the System Logs page, as exemplified below:

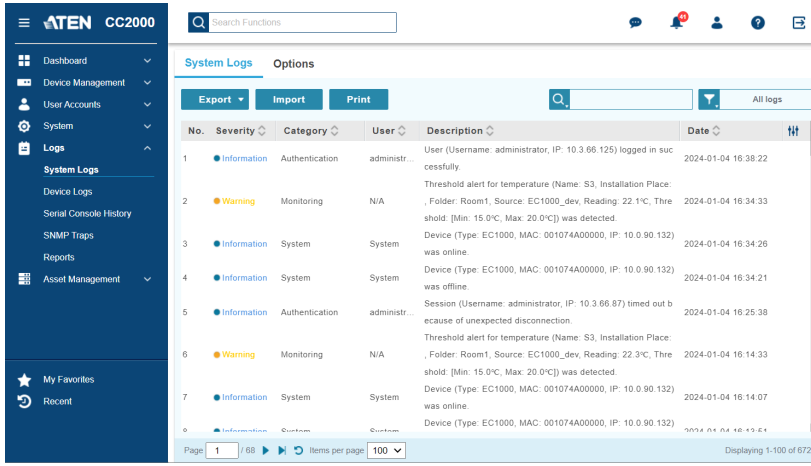


System Logs

The System Logs menu offers two tab menu choices: System Logs and Options.

System Logs

The System Logs tab is the default page and it looks similar to the one below:



- The default layout shows information concerning all of the events that have taken place on the entire CC2000 installation, displayed in reverse chronological order.
- The sort order of the list can be changed by clicking the column headings.
  - Clicking the Date column heading changes the sorting order between standard and reverse chronological order.
  - Clicking the Description column heading changes the sorting order between standard and reverse alphabetical order.

Note: In general, a blank page indicates that there were no log events recorded for that category.

Export

The Export button offers three options: Logs in current page, All logs, and Custom logs.

■ Logs in current page

Select **Logs in current page** to automatically download all logged event records currently displayed on the system logs page.

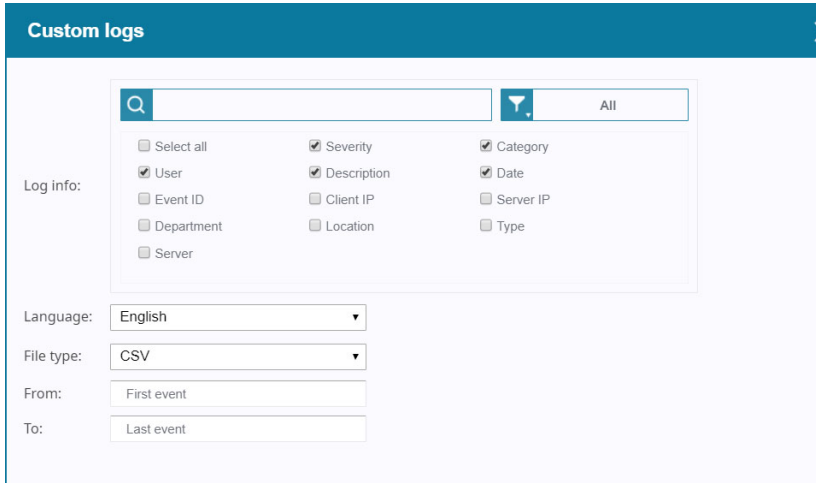
Note: The amount of logs downloaded for Logs in current page is determined by the Items per page drop-down menu.

■ All logs

Select **All logs** to automatically download all system logs.

■ Custom logs

The Custom Logs page is used to download only the specified logged event records. When you click **Custom logs**, a page similar to the one below appears:



To save specified logged events to a file, do the following:

1. Select the log info item(s) that you want to include in the exported file in the **Log info** table.

Note: Severity, Category, User, Description, and Date are enabled by default.

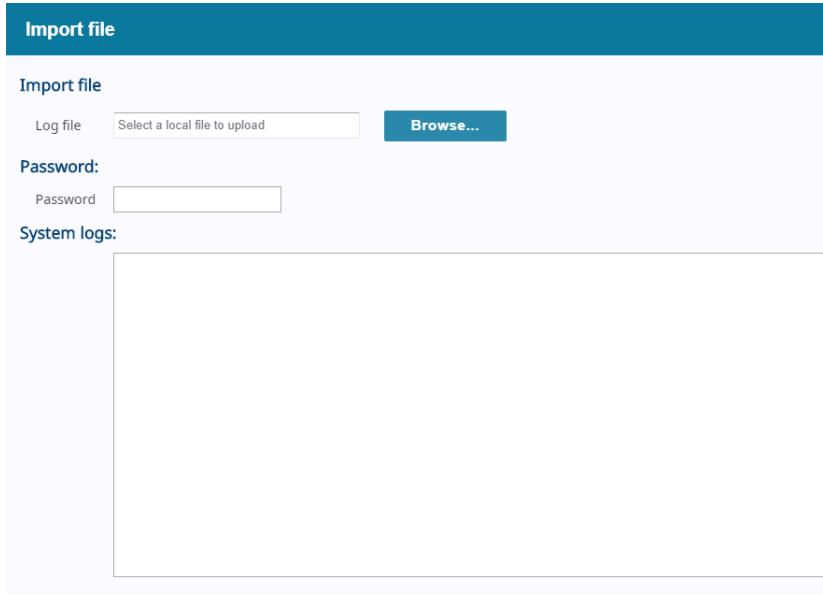
2. Use the **Language** drop-down menu for a list of languages available. English is used by default. Select and confirm to have the file exported in the language that your set to.
3. Use the **File type** drop-down menu to select your preferred export file type. If you choose one of the encryption options (Encrypt file with AES or Encrypt file with DES), define a password in the Password field.

Note: Make a note of the password – you will need it to import the file.

4. Set the time parameters in the **From** and **To** fields to export logged event records within a particular time period.
5. When you have finished with this page, click **Export** at the bottom-right of the panel.

Import

The Import page is used to open previously saved log files for viewing. When you click **Import**, a page similar to the one below appears:



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

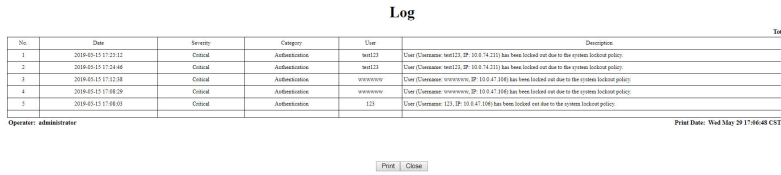
1. Either type the full file path in the **Log file** field, or click **Browse** to locate it.
2. If the file has been encrypted, type the password defined in the **Password** field.
3. Click **Import** at the bottom-right of the panel.

When the file is imported, its contents appear in the System logs main page.

Print

To print out the Log list, select **Print**.

Note: Only the list that is displayed (all, or a filtered choice) is printed.



Log

Total: 5

No.	Date	Severity	Category	User	Description
1	2019-05-15 17:23:12	Critical	Authentication	test123	User (Username: test123, IP: 10.0.74.231) has been locked out due to the system lockout policy.
2	2019-05-15 17:24:46	Critical	Authentication	test123	User (Username: test123, IP: 10.0.74.231) has been locked out due to the system lockout policy.
3	2019-05-15 17:12:38	Critical	Authentication	wwwwww	User (Username: wwwwww, IP: 10.0.47.106) has been locked out due to the system lockout policy.
4	2019-05-15 17:08:29	Critical	Authentication	wwwwww	User (Username: wwwwww, IP: 10.0.47.106) has been locked out due to the system lockout policy.
5	2019-05-15 17:08:03	Critical	Authentication	123	User (Username: 123, IP: 10.0.47.106) has been locked out due to the system lockout policy.

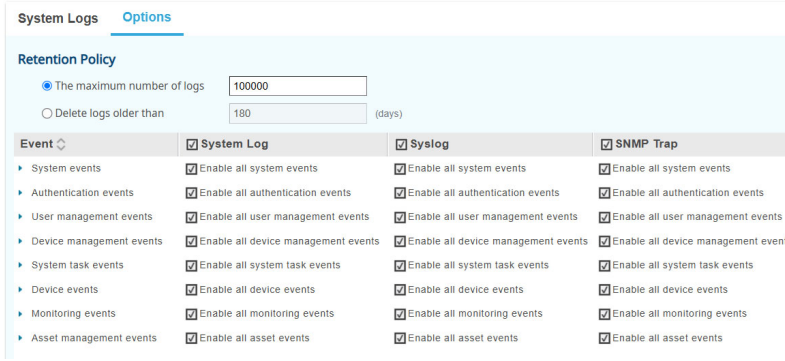
Operator: administrator

Print Date: Wed May 29 17:06:48 CST 2019

Print Close

Options

The Options page provides the settings of the system log file's Retention Policy. When you select Options, a page similar to the one below appears:



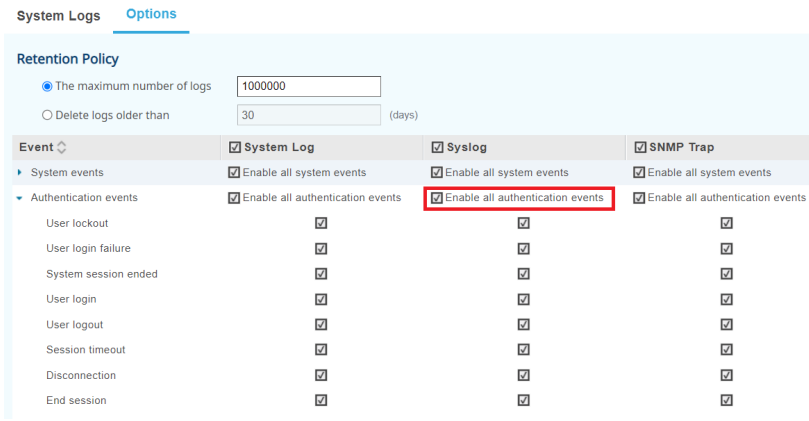
To adjust the system log file's Retention Policy, do the following:

1. For the Retention Policy, click on the radio button to select between **The maximum number of logs** and **Delete logs older than** options.
   - Select **The maximum number of logs** if you want to maintain the log database on a log records basis.
   - Select **Delete logs older than** if you want to maintain the log database on a temporal basis.

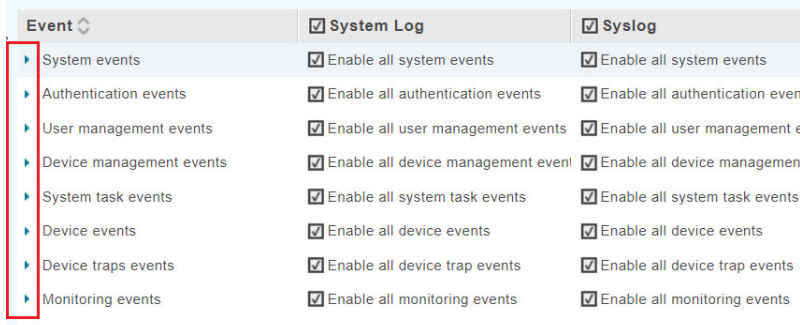
Note:
- When the number of days and records is reached, events are discarded on a "first in first out" basis.
- The valid range of maximum number of logs is from 10,000 - 1,000,000 logs.
- The valid range of number of days is from 30 - 1096 days.

---

2. For Event, it lets you select the events you want to track, and whether to record them in the System Log, Syslog, SNMP Trap, or all. Check the checkboxes of the events you want to enable.
   - There are 7 event categories and each category contains a list of separate events. To record all of the events for a category, check the checkbox in front of the **Enable all... events** entry, as exemplified below.



- 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.



3. When you have finished with this page, click **Save** at the bottom-right of the panel.

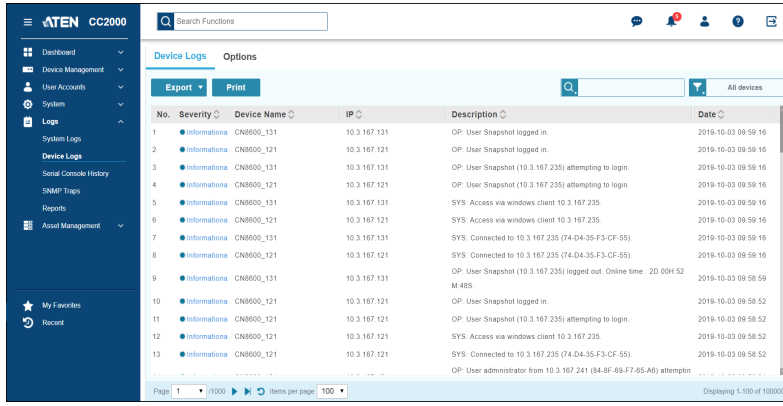
Device Logs

The CC2000 acts as a log server for all ATEN/Altusen devices, recording the system events that take place on those devices in a database.

The Device Logs menu offers two tab menu choices: Device Logs and Options.

Device Logs

The Device Logs is the default page, and it looks similar to the one below:



- The default layout shows log information for all of the devices on the entire CC2000 installation, displayed in reverse chronological order.
- The sort order of the list can be changed by clicking the column headings.
  - Clicking the Date column heading changes the sorting order between standard and reverse chronological order.
  - Clicking the Description column heading changes the sorting order between standard and reverse alphabetical order.

Note: In general, a blank page indicates that there were no log events recorded for that category.

Export

The Export tab offers two panel sub-menus: Logs in current page and All logs.

■ Logs in current page

Select **Logs in current page** to automatically download all logged event records currently displayed on the device logs page.

Note: The amount of logs downloaded for Logs in current page is determined by the Items per page option.

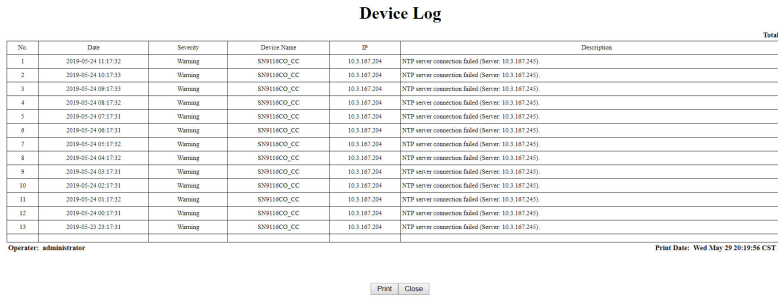
■ All logs

Select **All logs** to automatically download all logged event records from the device logs.

■ Print

To print out the Device Log list, select **Print**.

Note: Only the list that is displayed (all, or a filtered choice) is printed.



Device Log

Total: 13

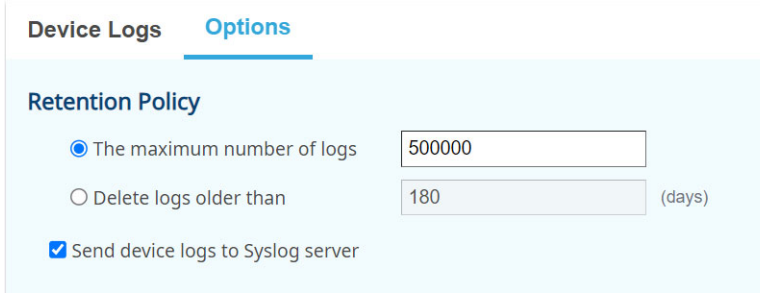
No.	Date	Severity	Device Name	IP	Description
1	2019-05-24 11:17:32	Warning	SN9116CO_CC	10.3.167.204	NTP server connection failed (Server: 10.3.167.245).
2	2019-05-24 10:17:33	Warning	SN9116CO_CC	10.3.167.204	NTP server connection failed (Server: 10.3.167.245).
3	2019-05-24 09:17:33	Warning	SN9116CO_CC	10.3.167.204	NTP server connection failed (Server: 10.3.167.245).
4	2019-05-24 08:17:32	Warning	SN9116CO_CC	10.3.167.204	NTP server connection failed (Server: 10.3.167.245).
5	2019-05-24 07:17:31	Warning	SN9116CO_CC	10.3.167.204	NTP server connection failed (Server: 10.3.167.245).
6	2019-05-24 06:17:31	Warning	SN9116CO_CC	10.3.167.204	NTP server connection failed (Server: 10.3.167.245).
7	2019-05-24 05:17:32	Warning	SN9116CO_CC	10.3.167.204	NTP server connection failed (Server: 10.3.167.245).
8	2019-05-24 04:17:32	Warning	SN9116CO_CC	10.3.167.204	NTP server connection failed (Server: 10.3.167.245).
9	2019-05-24 03:17:31	Warning	SN9116CO_CC	10.3.167.204	NTP server connection failed (Server: 10.3.167.245).
10	2019-05-24 02:17:31	Warning	SN9116CO_CC	10.3.167.204	NTP server connection failed (Server: 10.3.167.245).
11	2019-05-24 01:17:32	Warning	SN9116CO_CC	10.3.167.204	NTP server connection failed (Server: 10.3.167.245).
12	2019-05-24 00:17:31	Warning	SN9116CO_CC	10.3.167.204	NTP server connection failed (Server: 10.3.167.245).
13	2019-05-23 23:17:31	Warning	SN9116CO_CC	10.3.167.204	NTP server connection failed (Server: 10.3.167.245).

Operater: administrator **Print Date: Wed May 29 20:19:56 CST 2019**

Print Close

Options

The Options page provides settings of device log file's Retention Policy. When you select Options, a page similar to the one below appears:



To adjust the device log file's Retention Policy, do the following:

1. For the Retention Policy, click on the radio button to select between **The maximum number of logs** and **Delete logs older than** options.
   - Select **The maximum number of logs** if you want to maintain the log database on a log records basis.
   - Select **Delete logs older than** if you want to maintain the log database on a temporal basis.

Note:

- When the number of days or records is reached, events are discarded on a "first in first out" basis.
- The valid range of maximum number of logs is from 10000 - 1,000,000 logs.
- The valid range of number of days is from 30 - 1096 days.

2. Check the check box **Send device logs to Syslog server** to enable Syslog function. When enabled, the CC2000 sends Device logs to the Syslog server.

Note: CC2000 Send device logs to Syslog is enable by default.

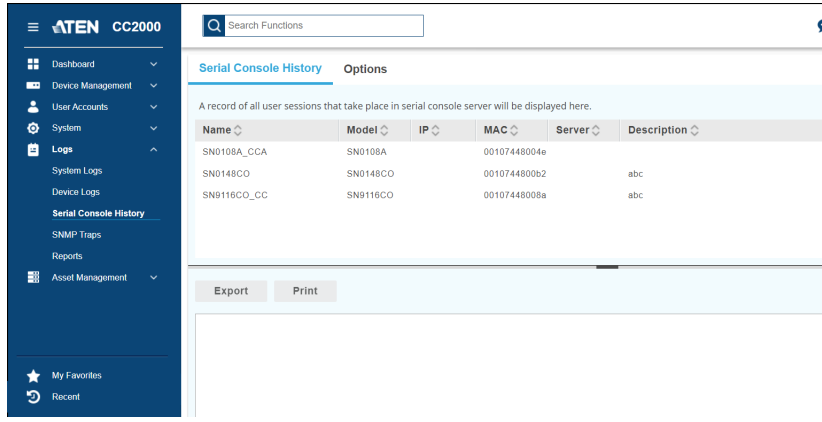
3. When you have finished with this page, click **Save** at the bottom-right of the page.

Serial Console History

The CC2000 keeps a record of all of the user sessions that take place on the serial console servers connected. The Serial Console History menu offers two Panel Menu choices: Serial Console History, and Options.

Serial Console History

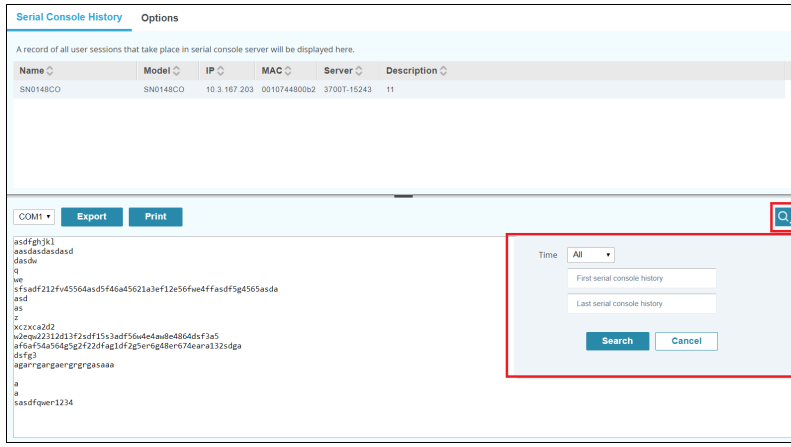
The Serial Console History is the default page, and it looks similar to the one below:



- The sort order of the Serial Console History list can be changed by clicking the column headings.
  - Clicking the Name column heading changes the sorting order between standard and reverse chronological order.
  - Clicking the Description column heading changes the sorting order between standard and reverse alphabetical order.

To search for Serial Console History records, do the following:

1. Click to choose a Model and click the search icon, a page similar to the one below appears:

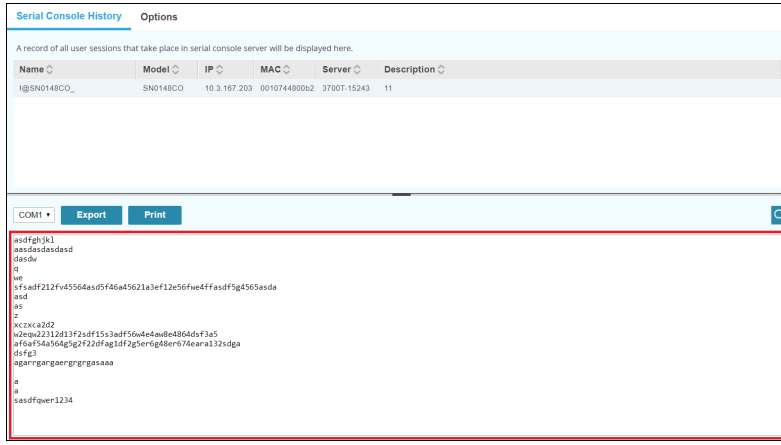


2. Use the **Time** drop-down menu to select one of the three options from All, Exclude, and Include. To search for records within a particular time period, select either **Include** or **Exclude** from the drop-down menu, and set the time parameters with the **First serial console history** and **Last serial console history** fields.

- Select **All** to search for all records in the database.
- Select **Include** to search all records that fall within the specified time range.
- Select **Exclude** to search all records that fall outside of the specified time range.

3. When you have finished with this page, click **Search** at the bottom of the panel.

The search results are displayed in the Serial Console History table in reverse chronological order in the main panel.



Export

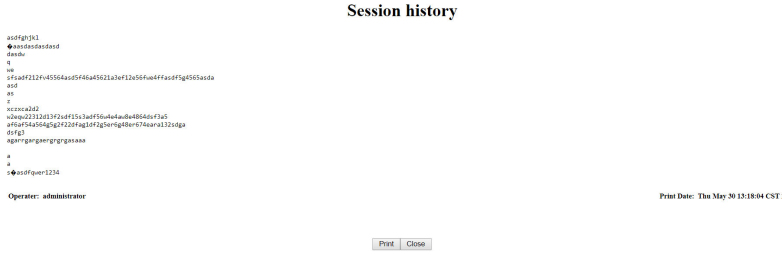
To Export the Serial Console History, do the following:

1. Select a Model from the Serial Console History list.
2. Use the drop-down menu to select the device's USB port number.
3. Click **Export** to export your Serial Console History.

Print

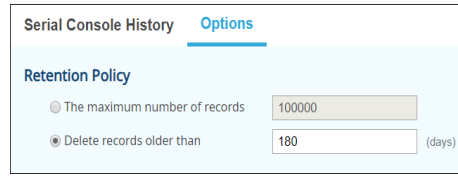
To Print the Serial Console History, do the following:

1. Select a Model from the Serial Console History list.
2. Use the drop-down menu to select the device's USB port number.
3. Click **Print** to print.



Options

The Options page provides the settings of serial console history's Retention Policy. When you select Options, a page similar to the one below appears:



To adjust the serial console history's Retention Policy, do the following:

1. For the Retention Policy, click on the radio button to select between **The maximum number of records** and **Delete records older than** options.
   - Select **The maximum number of records** if you want to maintain the serial console history database on a records basis.
   - Select **Delete records older than** if you want to maintain the serial console history database on a temporal basis.

Note:
- When the number of days or records is reached, events are discarded on a "first in first out" basis.
- The valid range of the maximum number of records is from 10000 - 1,000,000 serial console history records.
- The valid range of number of days is from 30 - 1096 days.

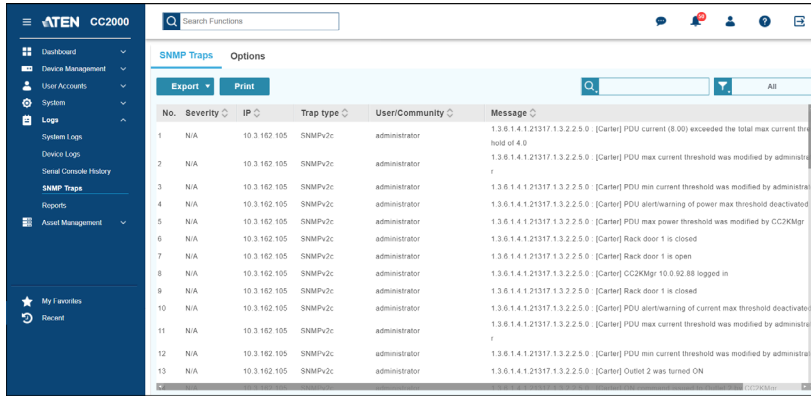
2. When you have finished with this page, click **Save** at the bottom-right of the page.

SNMP Traps

The SNMP Traps menu offers two tab menu choices: SNMP Traps, and Options. Which allows you to search for SNMP trap events and set further options for the search and display function.

SNMP Traps

The SNMP Traps is the default page, as exemplified below:



- The default layout shows all of the SNMP traps that have taken place on the entire CC2000 system, displayed in reverse chronological order.
- The sort order of the list can be changed by clicking the column headings.
  - Clicking the Date column heading changes the sorting order between standard and reverse chronological order.
  - Clicking the Severity column heading changes the sorting order between standard and reverse alphabetical order.

Export

The Export tab offers two options: SNMP traps in current page, and All SNMP traps.

■ SNMP traps in current page

Select **SNMP traps in current page** to automatically download all SNMP trap records currently displayed on the SNMP Traps page.

Note: The amount of traps downloaded in current page is determined by the Items per page drop-down menu.

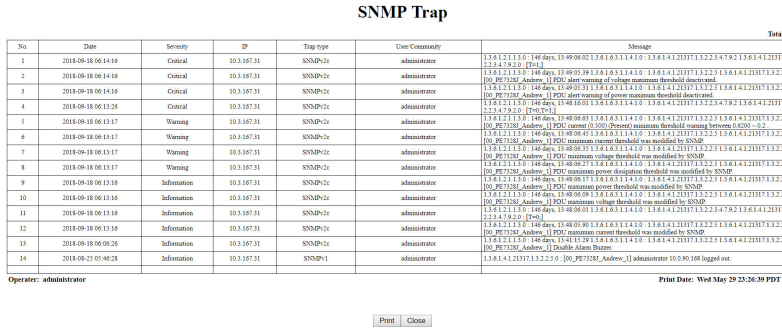
■ All SNMP traps

Select **All SNMP traps** to automatically download all SNMP trap records.

Print

To print out the SNMP Trap list, select **Print**.

Note: Only the list that is displayed (all, or a filtered choice) is printed.



SNMP Trap

Total: 14

No.	Date	Severity	IP	Trap type	User/Community	Message
1	2018-09-18 06:14:16	Critical	10.3.167.31	SNMPv2c	administrator	1.3.6.1.2.1.1.3.0 : 146 days, 13:49:06.02 1.3.6.1.6.3.1.1.4.1.0 : 1.3.6.1.4.1.213317.1.3.2.2.3.4.7.9.2.1.3.6.1.4.1.213317.1.3.2.2.3.4.7.9.2.0 : [Trt=1]
2	2018-09-18 06:14:16	Critical	10.3.167.31	SNMPv2c	administrator	1.3.6.1.2.1.1.3.0 : 146 days, 13:49:05.39 1.3.6.1.6.3.1.1.4.1.0 : 1.3.6.1.4.1.213317.1.3.2.2.5 1.3.6.1.4.1.213317.1.3.2.2.5.0 : [00_PE732SI_Andrew_1] PDU alert-warning of voltage maximum threshold deactivated.
3	2018-09-18 06:14:16	Critical	10.3.167.31	SNMPv2c	administrator	1.3.6.1.2.1.1.3.0 : 146 days, 13:49:05.31 1.3.6.1.6.3.1.1.4.1.0 : 1.3.6.1.4.1.213317.1.3.2.2.5 1.3.6.1.4.1.213317.1.3.2.2.5.0 : [00_PE732SI_Andrew_1] PDU alert-warning of power maximum threshold deactivated.
4	2018-09-18 06:13:26	Critical	10.3.167.31	SNMPv2c	administrator	1.3.6.1.2.1.1.3.0 : 146 days, 13:48:16.03 1.3.6.1.6.3.1.1.4.1.0 : 1.3.6.1.4.1.213317.1.3.2.2.3.4.7.9.2.1.3.6.1.4.1.213317.1.3.2.2.3.4.7.9.2.0 : [Trt=0,Trt=1]
5	2018-09-18 06:13:17	Warning	10.3.167.31	SNMPv2c	administrator	1.3.6.1.2.1.1.3.0 : 146 days, 13:48:06.63 1.3.6.1.6.3.1.1.4.1.0 : 1.3.6.1.4.1.213317.1.3.2.2.5 1.3.6.1.4.1.213317.1.3.2.2.5.0 : [00_PE732SI_Andrew_1] PDU current (0.500) (Present) minimum threshold warning between 0.6200 ~ 0.2
6	2018-09-18 06:13:17	Warning	10.3.167.31	SNMPv2c	administrator	1.3.6.1.2.1.1.3.0 : 146 days, 13:48:06.45 1.3.6.1.6.3.1.1.4.1.0 : 1.3.6.1.4.1.213317.1.3.2.2.5 1.3.6.1.4.1.213317.1.3.2.2.5.0 : [00_PE732SI_Andrew_1] PDU minimum current threshold was modified by SNMP.
7	2018-09-18 06:13:17	Warning	10.3.167.31	SNMPv2c	administrator	1.3.6.1.2.1.1.3.0 : 146 days, 13:48:06.35 1.3.6.1.6.3.1.1.4.1.0 : 1.3.6.1.4.1.213317.1.3.2.2.5 1.3.6.1.4.1.213317.1.3.2.2.5.0 : [00_PE732SI_Andrew_1] PDU minimum voltage threshold was modified by SNMP.
8	2018-09-18 06:13:17	Warning	10.3.167.31	SNMPv2c	administrator	1.3.6.1.2.1.1.3.0 : 146 days, 13:48:06.27 1.3.6.1.6.3.1.1.4.1.0 : 1.3.6.1.4.1.213317.1.3.2.2.5 1.3.6.1.4.1.213317.1.3.2.2.5.0 : [00_PE732SI_Andrew_1] PDU maximum power dissipation threshold was modified by SNMP.
9	2018-09-18 06:13:16	Information	10.3.167.31	SNMPv2c	administrator	1.3.6.1.2.1.1.3.0 : 146 days, 13:48:06.17 1.3.6.1.6.3.1.1.4.1.0 : 1.3.6.1.4.1.213317.1.3.2.2.5 1.3.6.1.4.1.213317.1.3.2.2.5.0 : [00_PE732SI_Andrew_1] PDU maximum power threshold was modified by SNMP.
10	2018-09-18 06:13:16	Information	10.3.167.31	SNMPv2c	administrator	1.3.6.1.2.1.1.3.0 : 146 days, 13:48:06.09 1.3.6.1.6.3.1.1.4.1.0 : 1.3.6.1.4.1.213317.1.3.2.2.5 1.3.6.1.4.1.213317.1.3.2.2.5.0 : [00_PE732SI_Andrew_1] PDU maximum voltage threshold was modified by SNMP.
11	2018-09-18 06:13:16	Information	10.3.167.31	SNMPv2c	administrator	1.3.6.1.2.1.1.3.0 : 146 days, 13:48:06.01 1.3.6.1.6.3.1.1.4.1.0 : 1.3.6.1.4.1.213317.1.3.2.2.3.4.7.9.2.1.3.6.1.4.1.213317.1.3.2.2.3.4.7.9.2.0 : [Trt=0,]
12	2018-09-18 06:13:16	Information	10.3.167.31	SNMPv2c	administrator	1.3.6.1.2.1.1.3.0 : 146 days, 13:48:05.90 1.3.6.1.6.3.1.1.4.1.0 : 1.3.6.1.4.1.213317.1.3.2.2.5 1.3.6.1.4.1.213317.1.3.2.2.5.0 : [00_PE732SI_Andrew_1] PDU maximum current threshold was modified by SNMP.
13	2018-09-18 06:06:26	Information	10.3.167.31	SNMPv2c	administrator	1.3.6.1.2.1.1.3.0 : 146 days, 13:41:17.29 1.3.6.1.6.3.1.1.4.1.0 : 1.3.6.1.4.1.213317.1.3.2.2.5 1.3.6.1.4.1.213317.1.3.2.2.5.0 : [00_PE732SI_Andrew_1] Double Alarm Buzzer.
14	2018-08-25 05:40:28	Information	10.3.167.31	SNMPv1	administrator	1.3.6.1.4.1.213317.1.3.2.2.5.0 : [00_PE732SI_Andrew_1] administrator 10.0.90.168 logged out.

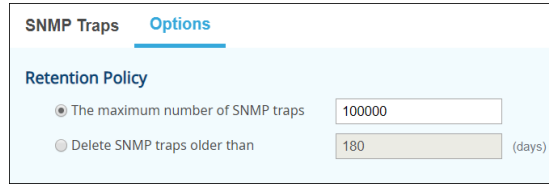
Operater: administrator

Print Date: Wed May 29 23:26:39 PDT 2019

Print Close

Options

The Options page provides settings of the SNMP trap's Retention Policy. When you select Options, a page similar to the one below appears:



To adjust the SNMP trap's Retention Policy, do the following:

1. For the Retention Policy, click on the radio button to select between **The maximum number of SNMP traps** and **Delete SNMP traps older than** options.

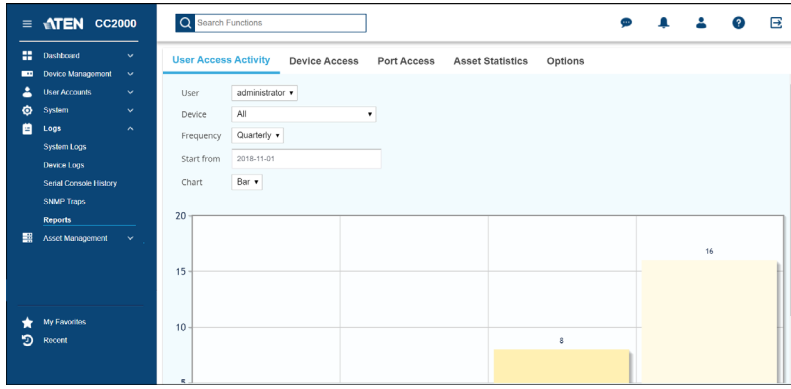
- Select **The maximum number of SNMP traps** if you want to maintain the SNMP trap database on a records basis.
- Select **Delete SNMP traps older than** if you want to maintain the SNMP trap database on a temporal basis.

Note:
- When the number of days or records is reached, events are discarded on a “first in first out” basis.
- The valid range of maximum number of records is from 10000 - 1,000,000 SNMP traps.
- The valid range of number of days is from 30 - 1096 days.

2. When you have finished with this page, click **Save** at the bottom-right of the panel.

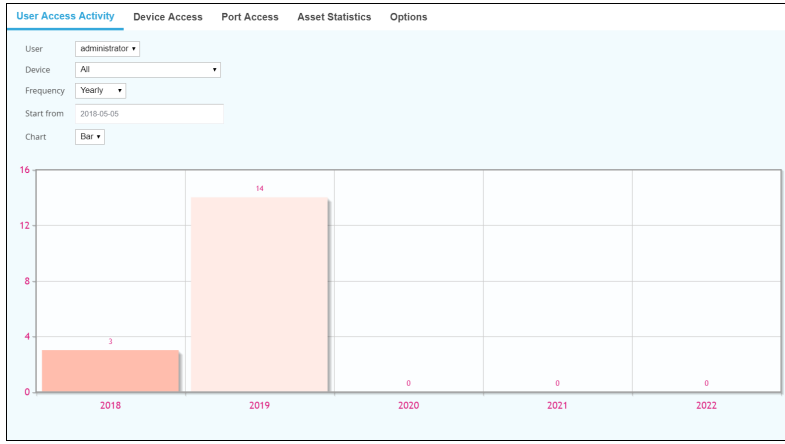
Reports

The Reports tab offers five tab menus: User Access Activity, Device Access, Port Access, Asset Statistics, and Options. You can view access-associated statistics about the users and devices of the CC2000 system and configure for how the reports are displayed.



User Access Activity

This page provides statistics of the Device/Port Access Per User. The User Access Activity is the default page, and it looks similar to the one below:



Fill in the fields from the main panel to build and display either a pie or bar chart, or both, according to the parameters set.

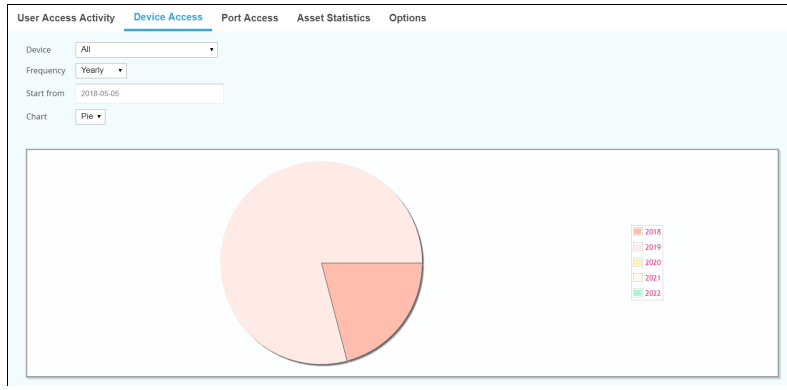
The meanings of each fields are described in the table below:

Item	Description
User	Use the User drop-down menu for a list of users to select from and to display their access statistics.
Device	Select All or an individual port/device to display its statics. This will display a graph with the number of times a user has accessed the device(s), according to the Frequency you select. The numbers displayed within each chart color show the number of times the device was accessed (on that day/week/month/quarter/year) and its usage percentage.
Frequency	Select the amount of time that the chart is divided into. The chart will display how many times the Device was accessed within a given time span, divided by the selected period: ◆ Daily: Displays how many times the device was accessed each day, for a span of 7 days, beginning from the Start From date. ◆ Weekly: Displays how many times the device was accessed each week, for a span of 4 weeks, beginning from the Start From date. The format 2013-W42 represents week 42 of the year 2013. ◆ Monthly: Displays how many times the device was accessed each month, for a span of 12 months, beginning from the Start From date. ◆ Quarterly: Displays how many times the device was accessed each quarter, for 4 quarters of a year, beginning from the Start From date. ◆ Yearly: Displays how many times the device was accessed each year, for a span of 5 years, beginning from the Start From date. **Note:** If the device was not accessed, no data is shown.
Start From	Click the calendar to select a start date for the span of time that will be represented in the chart.
Chart	Select the type of chart you would like to use to display the information: ◆ Pie: Shows a round chart divided into the time period selected. ◆ Bar: Shows individual bars in a graph divided into the time periods selected. ◆ All: Displays both a pie and bar chart.

Device Access

The Device Access page provides statistics for Device Access.

Fill in the fields from the main panel to build and display either a pie or bar chart, or both, according to the parameters set. When **Pie** is selected for **Chart**, the Device Access page looks similar to the one below:



The meanings of each fields are described in the table below:

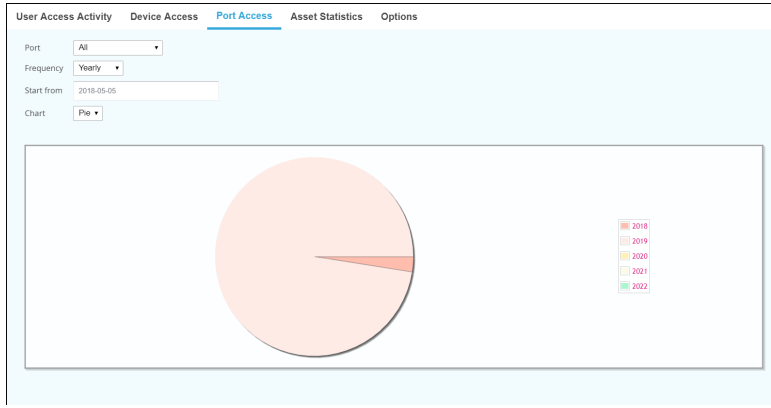
Item	Description
Device	Select All, Top 10 port, or a specific device to display the corresponding access stats. This will display a graph with the number of times the device(s) have been accessed, according to the Frequency you select. ◆ Top 10 port: Display the stats of the top 10 devices. The numbers displayed with each chart color show the number of times the device was accessed (on that day/week/month/quarter/year) and its usage percentage.
Frequency	Select the amount of time that the chart will be divided into. The chart will display how many times the Device was accessed within a given time span, divided by the selected period: ◆ Daily: Displays how many times the device was accessed each day, for a span of 7 days, beginning from the Start From date. ◆ Weekly: Displays how many times the device was accessed each week, for a span of 4 weeks, beginning from the Start From date. The format 2013-W42 represents week 42 of Year 2013. ◆ Monthly: Displays how many times the device was accessed each month, for a span of 12 months, beginning from the Start From date. ◆ Quarterly: Displays how many times the device was accessed each quarter, for 4 quarters of a year, beginning from the Start From date. ◆ Yearly: Displays how many times the device was accessed each year, for a span of 5 years, beginning from the Start From date. **Note:** If the device was not accessed, no data is shown.

Item	Description
Start From	Click the calendar to select a start date for the span of time that will be represented in the chart.
Chart	Select the type of chart you would like to use to display the information: ◆ Pie: Shows a round chart divided into the time period selected. ◆ Bar: Shows individual bars in a graph divided into the time periods selected. ◆ All: Displays both a pie and bar chart.

Port Access

The Port Access page provides the statistics for Port Access.

Fill in the fields from the main panel to build and display either a pie or bar chart, or both, according to the parameters set. The Port Access page looks similar to the one below:



The meanings of each fields are described in the table below:

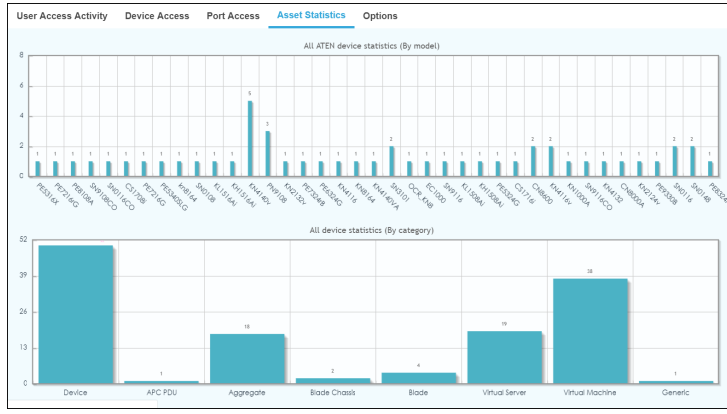
Item	Description
Port	Select All, Top 10 port, or a specific port that you want to display statics for. This will display a graph with the number of times the port(s) was accessed, according to the Frequency you select. ◆ Top 10 port: Display the stats of the top 10 ports. The numbers displayed with each chart color show the number of times the port was accessed (on that day/week/month/quarter/year) and its usage percentage.

Item	Description
Frequency	Select the amount of time that the chart will be divided into. The chart will display how many times the Port was accessed within a given time span, divided by the selected period: ◆ Daily: Displays how many times the port was accessed each day, for a span of 7 days, beginning from the Start From date. ◆ Weekly: Displays how many times the port was accessed each week, for a span of 4 weeks, beginning from the Start From date. The format 2013-W42 represents week 42 of Year 2013. ◆ Monthly: Displays how many times the port was accessed each month, for a span of 12 months, beginning from the Start From date. ◆ Quarterly: Displays how many times the port was accessed each quarter, for 4 quarters of a year, beginning from the Start From date. ◆ Yearly: Displays how many times the port was accessed each year, for a span of 5 years, beginning from the Start From date. **Note:** If the port was not accessed, no data is shown.
Start From	Click the calendar to select a start date for the span of time that will be represented in the chart.
Chart	Select the type of chart you would like to use to display the information: ◆ Pie: Shows a round chart divided into the time period selected. ◆ Bar: Shows individual bars in a graph divided into the time periods selected. ◆ All: Displays both a pie and bar chart.

Asset Statistics

The Asset Statistics page displays all the assets that have been added to the CC2000 installation, shown in two charts: **All ATEN device statistics (By model)**, and **All device statistics (By category)**.

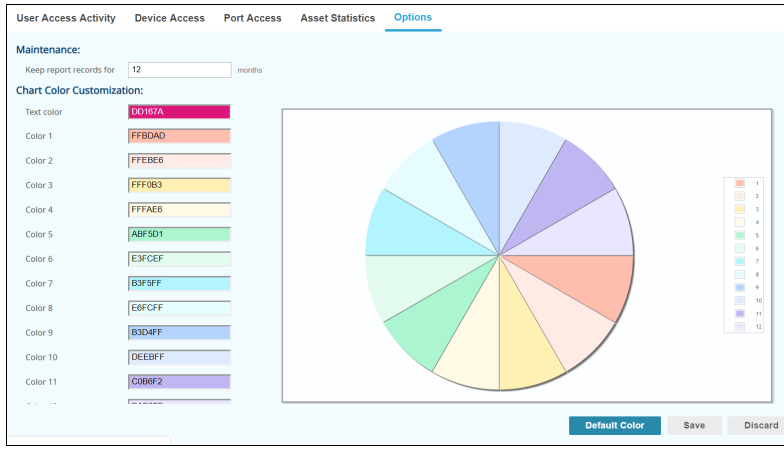
The Port Access page looks similar to the one below:



- **All ATEN device statistics (By model)** shows the number of ATEN devices by model, that are currently associated with the CC2000 installation.
- **All device statistics (By category)** shows all devices associated with the CC2000 installation by category: Devices (ATEN devices), APC PDU, Aggregate, Blade Chassis, Blade, Virtual Server, Virtual Machine, and Generic.

Options

The Options page provides options for customizing the report colors and for saving report records, as exemplified below:



To customize the report, do the following:

1. Fill in the **Keep report records for months** field under **Maintenance**.
2. Adjust the color fields under **Chart Color Customization**.
3. When you have finished with this page, click **Save** at the bottom-right of the panel.

The meanings of each fields are described in the table below:

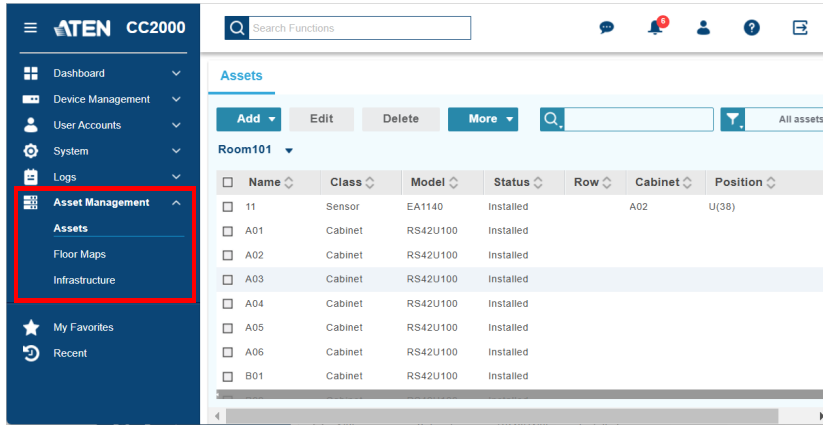
Item	Description
Maintenance	Enter the number of months you would like the system to keep report records for before deleting.
Chart Color Customization	◆ Text color: Click the box to bring up a small window and choose the color you would like to use for the texts displayed within the reports. ◆ Color 1~12: Click the boxes to bring up a small window to choose the color you would like to use for each key in the charts. When selecting a color, the test chart at the right will change accordingly so you can see how your graph will look like.

◆ Default Color tab: Click to return all colors back to their default settings.

Chapter 9
Asset Management

Overview

This chapter provides information on how to manage CC2000's physical assets using an infrastructure map, an asset list, and floor maps. On top of the system-managed devices (that are added to the device list), the physical assets here also include cabinets, servers, storages, networking devices, and patch panels. To access these features, log in to the CC2000 browser GUI, and go to **Asset Management**.



Refer to the table below to find out the function and purpose of these asset management tools.

Control on CC2000 Browser GUI	Main Function
Assets	Use this page to add assets to the room where they are installed so that they can be used to create a 2D location map, the floor map. For full details, see *Assets Page*, page 307.
Floor Maps	Use this page to create a floor map and define asset locations for each room. Note that assets need to be added to the asset list (page 307) first for them to be available for allocation. For full details, see *Floor Maps*, page 328.
Infrastructure	Use this page to delineate the managed data centers in terms of buildings, floors, and rooms. For full details, see *The Infrastructure Map*, page 302.

Getting Started Tasks

1. Familiarize the following features.
   - infrastructure maps

     For details, see *Understanding the Infrastructure Map*, page 302.
   - floor maps

     For details, see *Understanding Floor Maps*, page 328.
2. Basic configuration and preparation.

   a) Configure an infrastructure map.

   For details, see *Configuring the Infrastructure Map*, page 305.

   b) Import images to Image Library.

   For details, see *Importing Images to Image Library*, page 327.

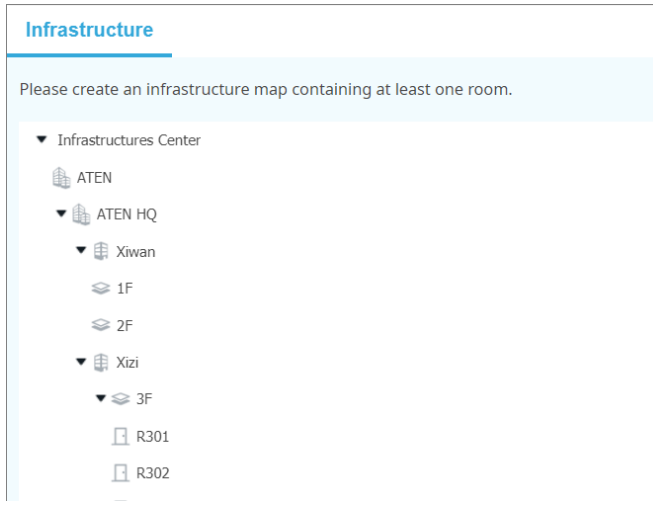
   c) Import model specifications to Model Library.

   For details, see *Importing Device Specifications to Model Library*, page 323.
3. Add cabinets and other types of assets to each room. For details, see any of the following topics:
   - *Adding Assets*, page 309
   - *Adding Cabinets, UPS, or Sensors*, page 330
4. Allocate assets to their physical location on the floor map. For details, see *Allocating Cabinets, UPS, or Sensors on a Floor Map*, page 331.

The Infrastructure Map

Understanding the Infrastructure Map

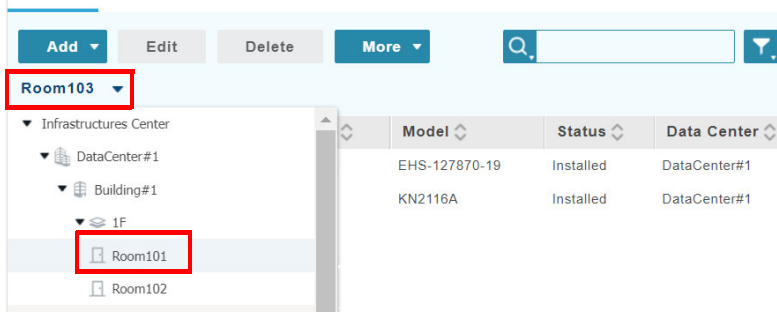
The infrastructure map is used to specify the CC2000 deployment site in terms of four hierarchical levels—data center , building , floor , and room . For example, an infrastructure map may look like this:



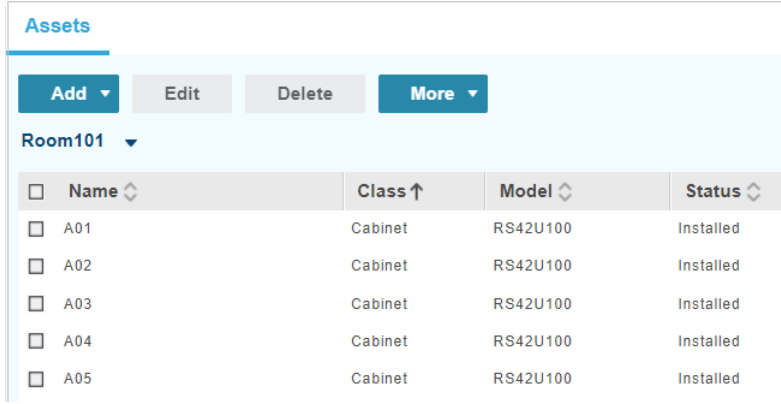
Organizing Assets and Floor Maps

The CC2000 system also uses this information to organize assets and floor maps, displaying added assets and floor maps by room. For example, the user needs to select a particular room to see created assets for the room, as shown below.

1. Use the Room drop-down list to open the infrastructure map and select a room to access assets in the room.

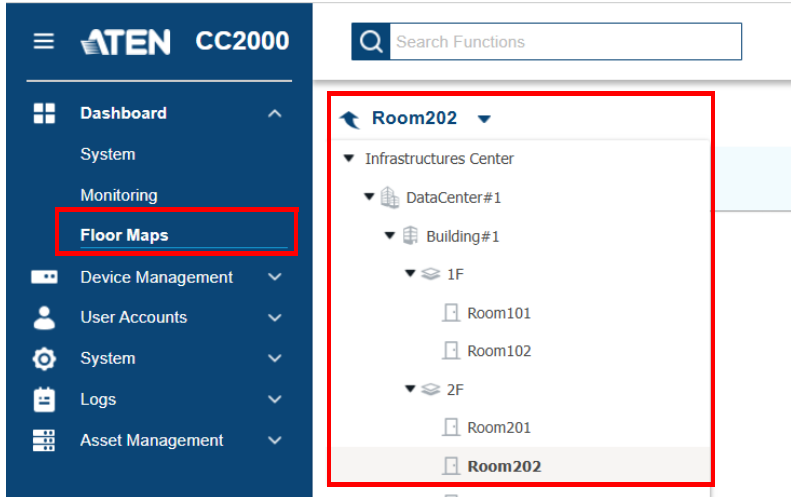


2. This Asset page for Room 101 appears.



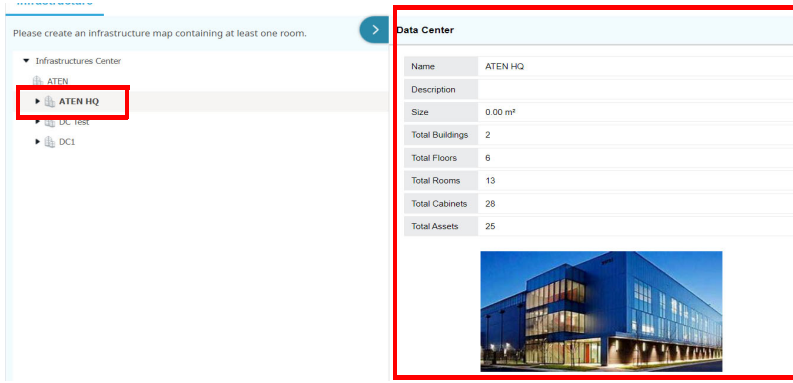
Selector for Dashboard Floor Maps

The CC2000 system then adopts and applies the infrastructure map to the GUI where the map is clickable for switching floor maps of different rooms.

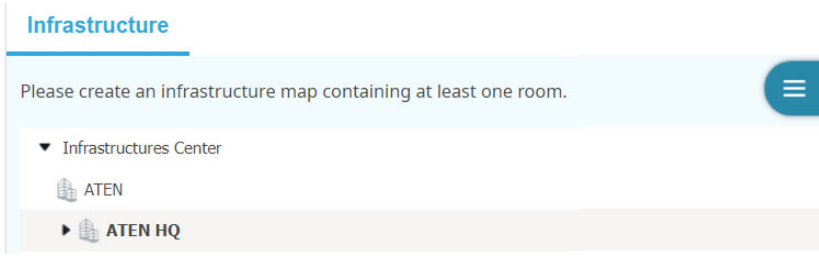


Viewing the Basic Information for Each Infrastructure Level

You can view created information for each level by clicking on the target level, and the information appears on the right:



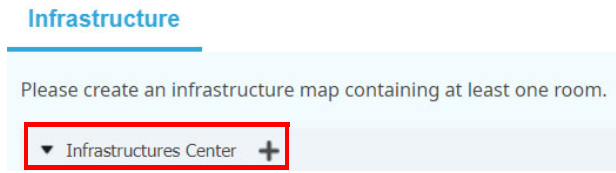
To close the information panel, click . To open the information panel, click .



Configuring the Infrastructure Map

1. In CC2000 browser GUI, go to **Asset Management** > **Infrastructure**.
2. Create an infrastructure map that resembles your deployment site.

   a) Mouse over Infrastructure Center and click + to add a data center.



   b) In the pop-up Data Center dialog box, fill in the information for the data center as needed.

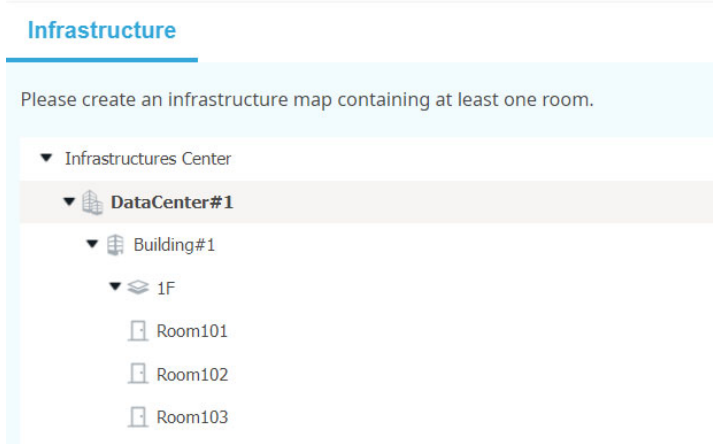
   c) Mouse over the data center you just created and click + to add one or more buildings. Fill in the information in the pop-up dialog as needed.

   d) Under each created building, click + to add one or more floors. Fill in the information in the pop-up dialog as needed.

   e) Under each created floor, click + to add one or more rooms. Fill in the information in the pop-up dialog as needed.

Note: To upload an image for the created data centers, buildings, floors, or rooms, click on the Image field to browse from the Image Library.

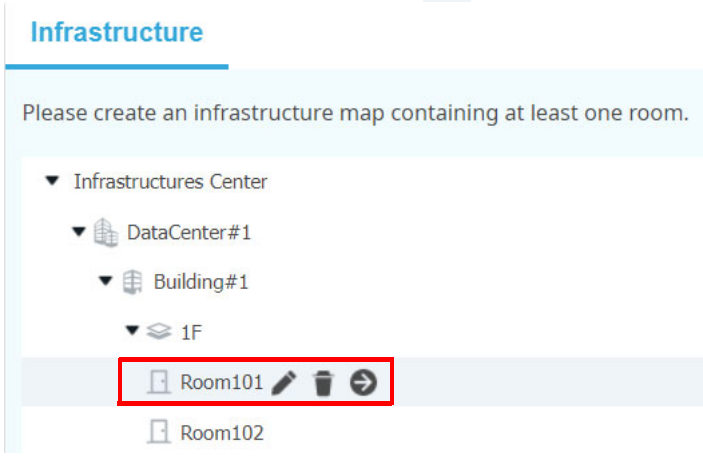
An infrastructure map may look like this:



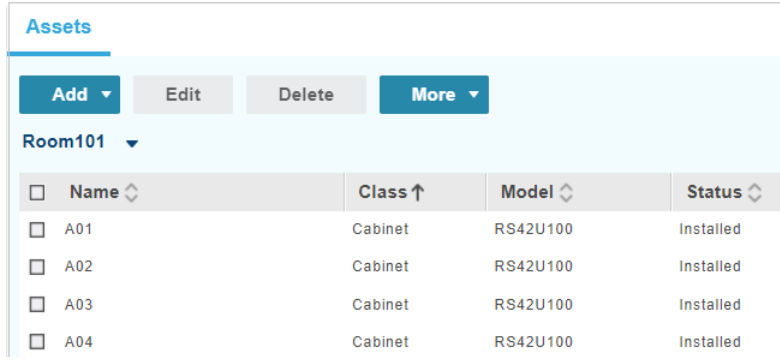
Accessing the Assets Page of a Room

You can quickly access the assets page of a room from the infrastructure map.

1. You may mouse over a room and click .



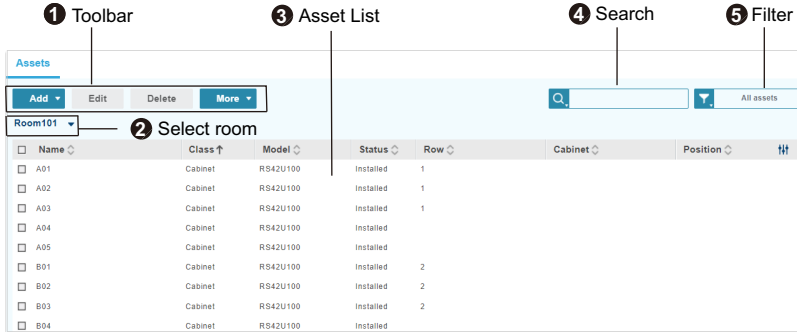
2. The Assets page for Room 101 appears.



Assets Page

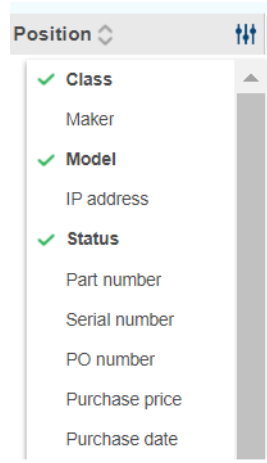
The Assets page displays a list of added assets along with their basic information, such as class, model, cabinet location. Use this page to centrally maintain assets.

To visit the page, go to **Asset Management** > **Assets**. The Assets page appears.



The assets page provide the following controls:

No.	Name	Description
1	Tool Bar	Use the toolbar to: ◆ Add, edit, or remove assets to the room. For detailed information, see *Adding Assets*, page 309. ◆ Add, edit, or remove models from Model Library. For detailed information, see *Model Library*, page 322. ◆ Add, edit, or remove images from Image Library. For detailed information, see *Model Library*, page 322. ◆ View specifications of a selected asset. For detailed information, see *Viewing Asset Specifications*, page 317. ◆ Re-allocate an asset to another room. For detailed information, see *Exporting an Asset List*, page 318. ◆ Export asset lists. For detailed information, see *Exporting an Asset List*, page 318.
2	Select Room	The assets page displays added assets in a room that you select. Click the drop-down button to select another room.

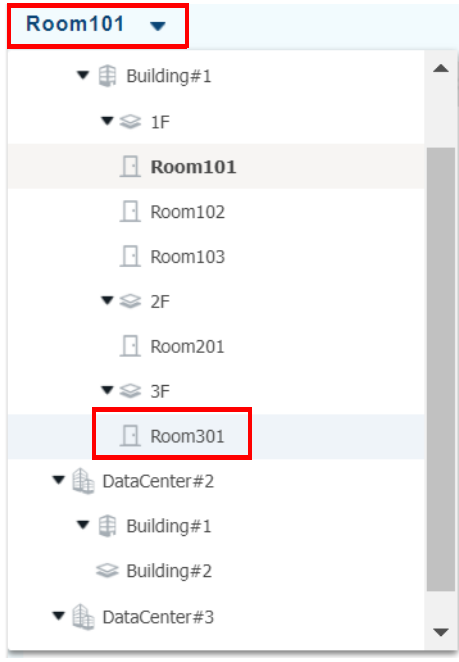
No.	Name	Description
3	Asset List	◆ This panel shows the information of the assets added to the room. ◆ To sort the list in alphabetical ↑ or reverse alphabetical order ↓ (ascending or descending order for numerical data) of a table header, click on the table header. ◆ To add or remove information fields, click and click to select/unselect pieces of information for display. 
4	Search	Type one or more key words to search within all columns of the asset list. For more details, see *Searching Assets by Keywords*, page 319.
5	Filter	Apply filters to refine the asset list. For more details, see *Filtering the Asset List*, page 320.

Adding Assets

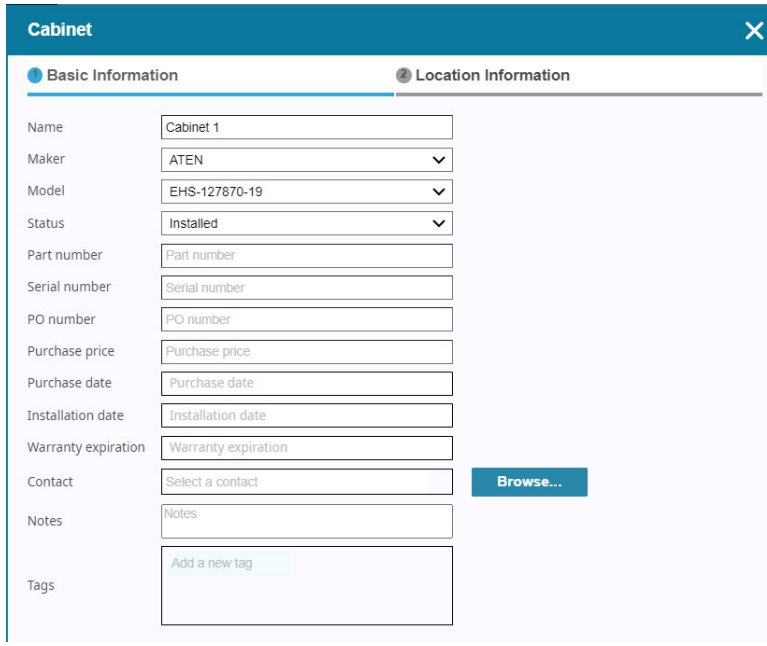
Adding a Cabinet

1. In CC2000 browser GUI, go to **Asset Management** > **Assets**.
2. Using the drop-down list, select a room to which you want to add the cabinet.

   For example:



3. Click **Add** and select **Cabinet**. This window appears.



4. Configure the basic information.

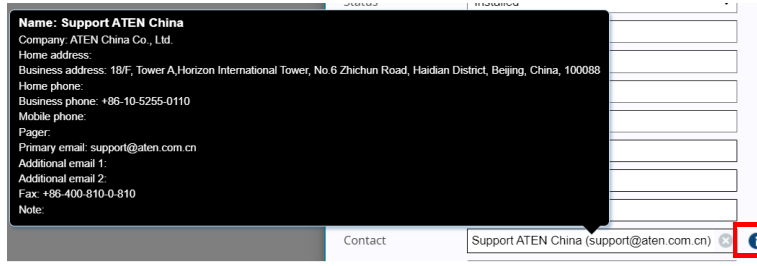
   a) Configure the Name, Maker, Model, and Status fields.

   - **Maker & Model:** The maker and model options are centrally stored in the Model Library. To add more models and makers, go to the Model Library. For more information, see *Model Library*, page 322.

   b) Optionally configure the rest.

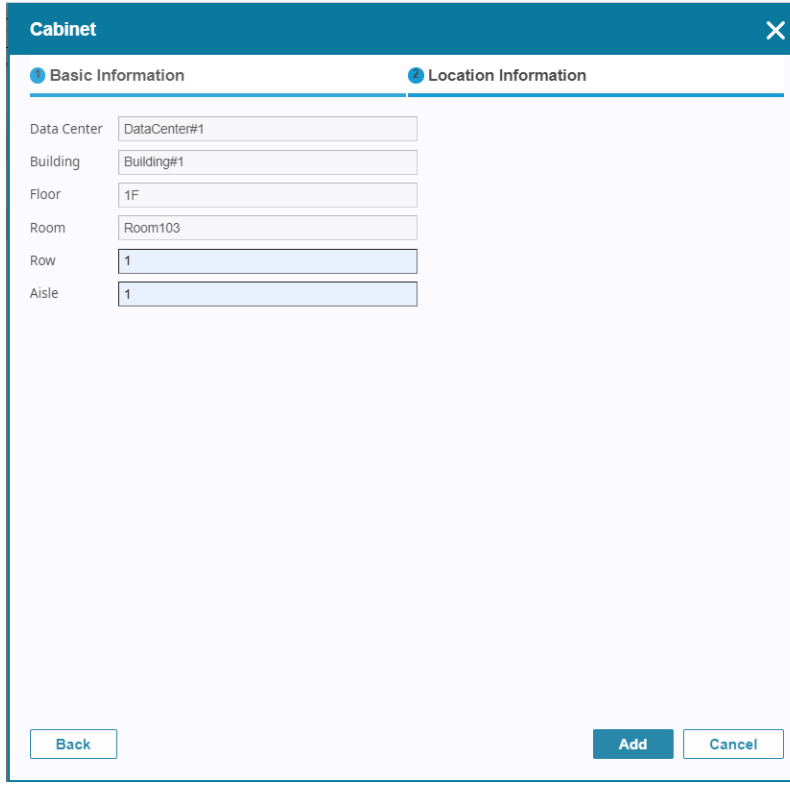
   - **Contact:** Browse to add contact. To add more contact options, go to **System** > **Contacts**.

     To view contact details, click the info tip. The contact info appears.

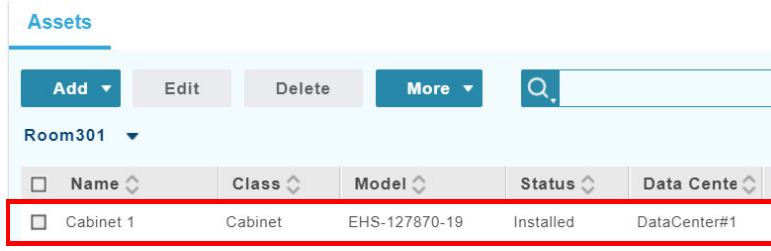


- **Tag:** Create up to 5 tags for the asset. To add a tag, type the tag and click **Add**, or select from the drop-down list, where previously created tags are shown.

5. Click **Next** and configure the location information.



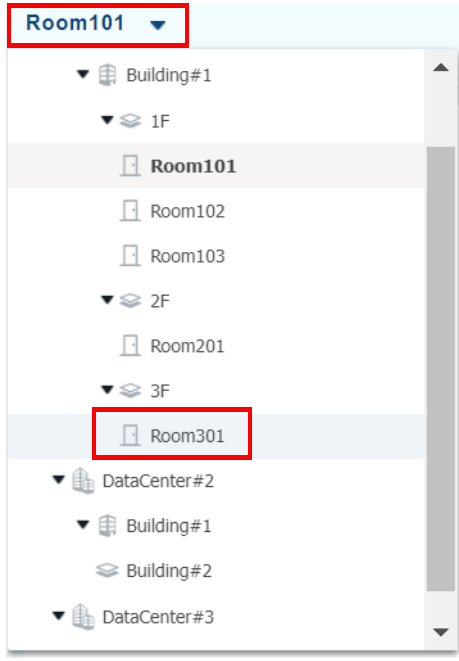
6. Click **Add**. The cabinet is added to the room.



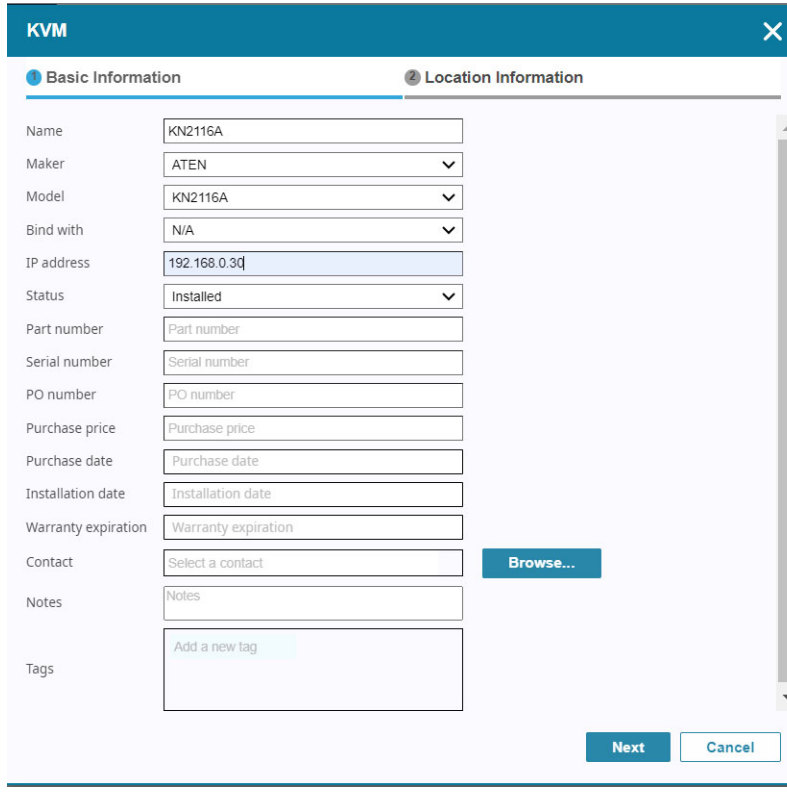
Adding Other Asset Types

To add a server, storage, networked device, KVM switch, serial console, PDU, or UPS, sensor, or patch panel, follow the steps below.

1. In CC2000 browser GUI, go to **Asset Management** > **Assets**.
2. Using the drop-down list, select a room to which you want to add assets.
   For example:



3. Click **Add** and select a class for the asset. The basic information window appears. For example:



4. Configure the basic information.

   a) Configure the following fields.

   - **Maker & Model:** The maker and model options are centrally stored in the Model Library. To add more models and makers, go to the Model Library. For more information, see *Model Library*, page 322.
   - **Bind with:**

     Use this setting for the following scenarios.

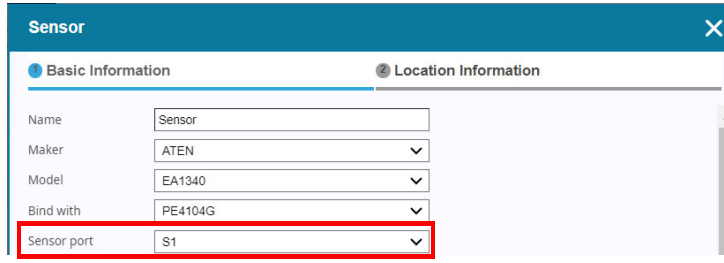
     - To specify to which device and port a sensor is installed.

     - To associate an asset (except for sensors) with its actual device (that you have added to **Device Management** > **Devices**) so that the system can automatically synchronized for its current IP address information.

- Select **N/A** if none of the above scenario applies to the asset you are adding. Type the IP address of the asset in the next field.

- **Sensor Port:** (Only applicable to sensor devices) Specify the port of the device to which the sensor is installed.

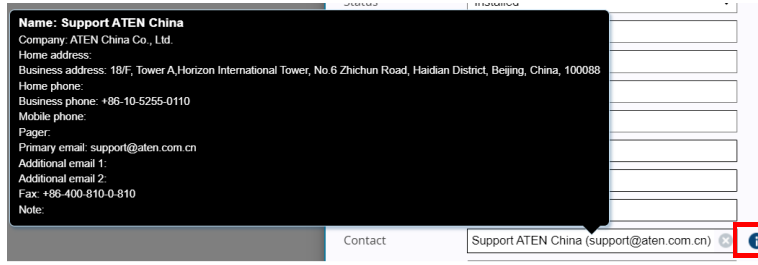
  For example:



b) Optionally configure the rest.

- **Contact:** Browse to add contact. To add more contact options, go to **System** > **Contacts**.

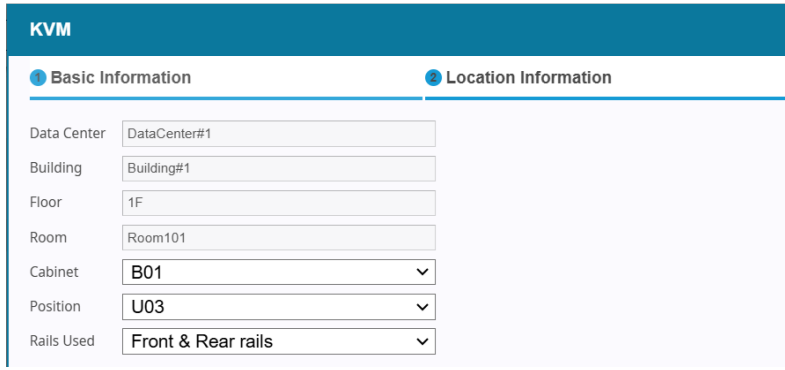
  To view contact details, click the info tip. The contact info appears.



- **Tag:** Create up to 5 tags for the asset. To add a tag, type the tag and click Add, or select from the drop-down list, where previously created tags are shown.

5. Click **Next**.

6. Configure the location information.

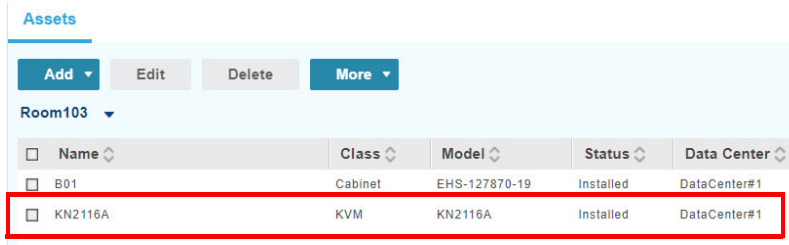


- **Cabinet:** Specify where the asset is installed. Select **N/A** if the asset is not installed to any cabinet. To add more options to this drop-down list, add cabinets to this room. For details, see *Adding a Cabinet*, page 309.
- **Position:** Specify the unit space where the asset is installed. The listed options vary depending on your chosen cabinet. If there is no suitable description for the selected cabinet, this field is indicated as **N/A**. In this case, use the **Note** field to add the information.
- **Rails Used:** If the asset is installed to a cabinet (with the cabinet setting configured), select from the drop-down menu to specify the part of the rail that the asset occupies.

Note: For a UPS or sensor, if its cabinet and position are indicated as **N/A**, it is not installed to any cabinet and can be allocated individually on the floor map.

---

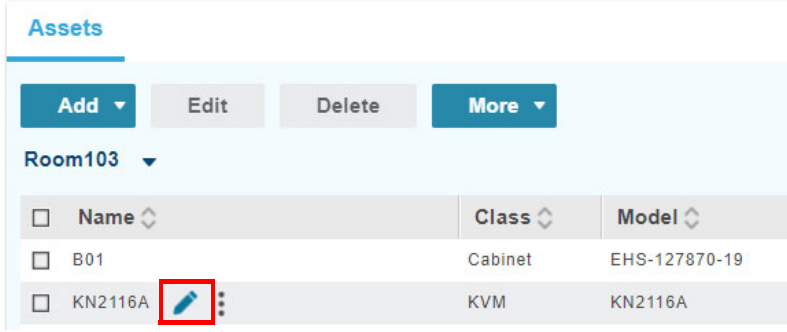
7. Click **Save**. The asset is added to the room.



Editing an Asset

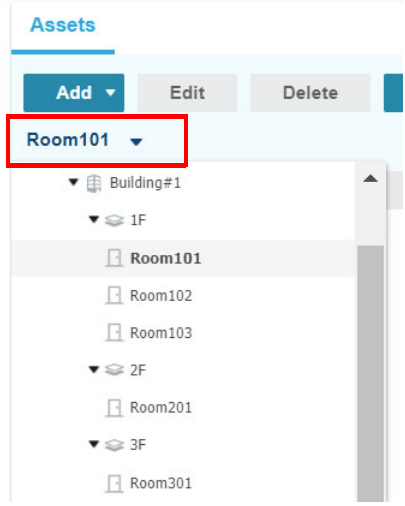
To edit specifications of an asset

1. Locate the asset in the Assets page.
2. Mouse over the asset and click , or tick the asset in the list and click Edit.



Moving an Asset to Another Room

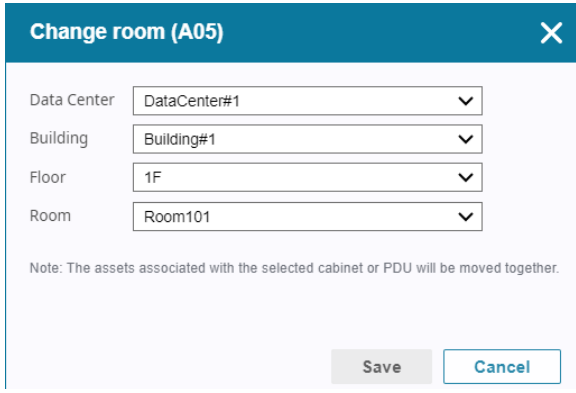
1. On the Assets page, click the Room drop-down list to display the target asset.



2. From the displayed list, select one or more assets you want to move.

Note: If a cabinet is moved, the assets allocated to that cabinet will be moved together. If an asset that is already allocated to a cabinet is moved, the asset will be moved individually.

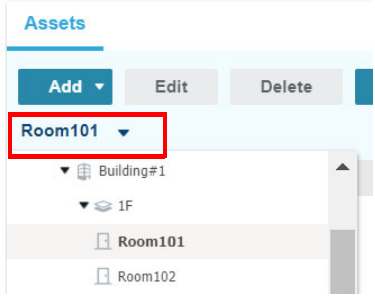
3. From the toolbar, click **More**, and then select **Change Room**.
4. In the pop-up dialog box, use the drop-down lists to select a target room.



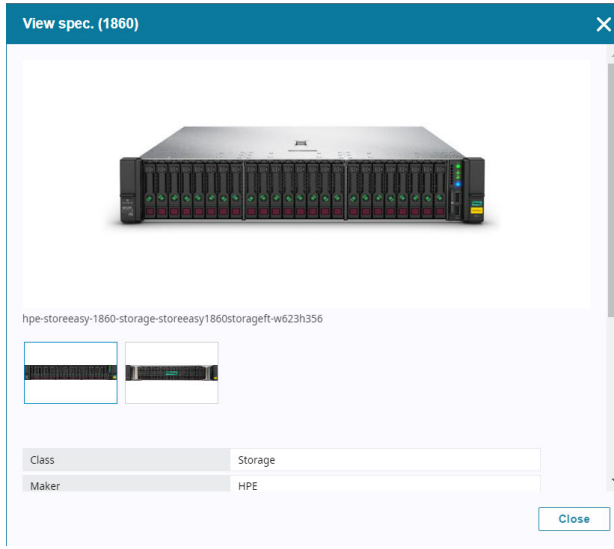
5. Click **Save** to apply the changes. The asset is now moved and becomes unallocated.
6. Configure the following as needed.
   - Allocate the asset on the floor map
   - If the asset is installed to a cabinet, specify the cabinet and its location (within the cabinet).

Viewing Asset Specifications

1. On the Assets page, click the Room drop-down list to display the target asset.



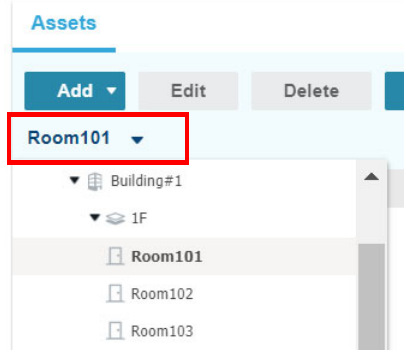
2. Select the target asset from the list.
3. Click **More** and select **View specs**. Specifications for the selected asset appears in a separate window.



Exporting an Asset List

Note that asset information can only be exported by room.

1. On the Assets page, click the Room drop-down list to select a room.

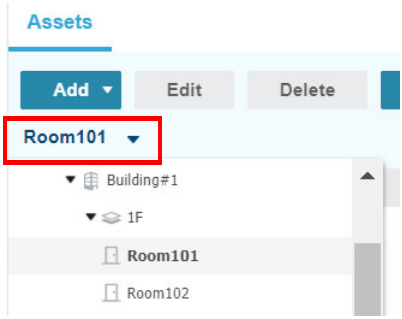


2. From the toolbar, click **More**, and then select **Export asset list**. Information for the assets in this room are exported as an excel file. All the fields in the  .

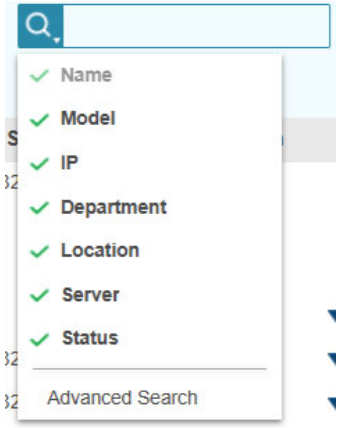
Searching Assets by Keywords

The CC2000 system can perform a keyword search in the listed fields of the device list. Note that the search is carried out to assets in the selected room.

1. On the Assets page, click the Room drop-down list to select the target room.



2. In the search box , type the keyword and press **Enter**. To change scope of search, click and click from the pop-up menu to add or remove the search items.

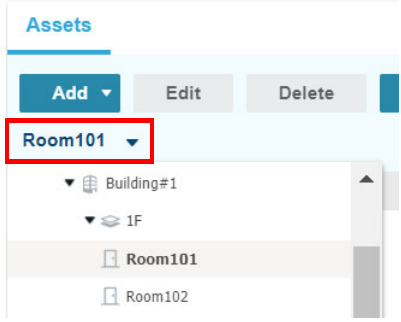


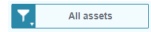
3. In the search box, type one or more keywords and press **Enter**.

Filtering the Asset List

Note that the filters are applied to assets in the selected room.

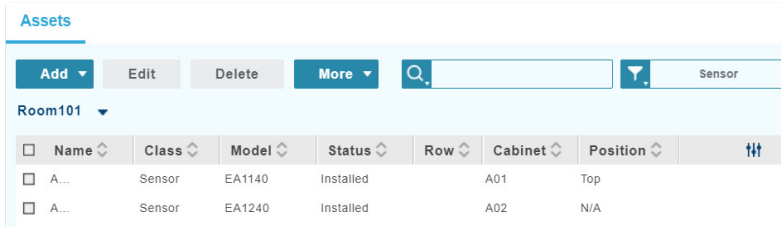
1. On the Assets page, click the Room drop-down list to select the target room.



2. Click on the filter 

. All filter options, including tags appear.

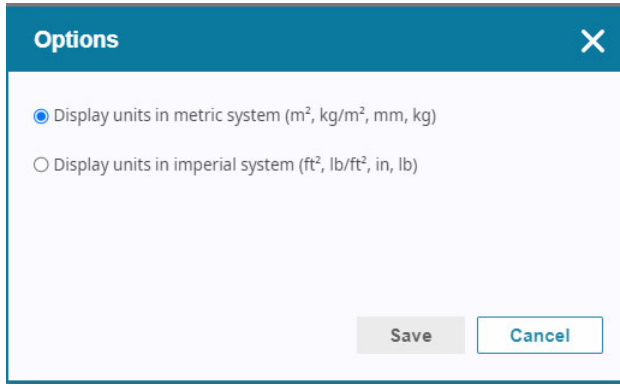
3. Click to select a filter. The filter is immediately applied, with your chosen filter identified in the filter box.



Changing the Measurement System

The system supports display of specifications in metric or imperial system. To change the measurement system:

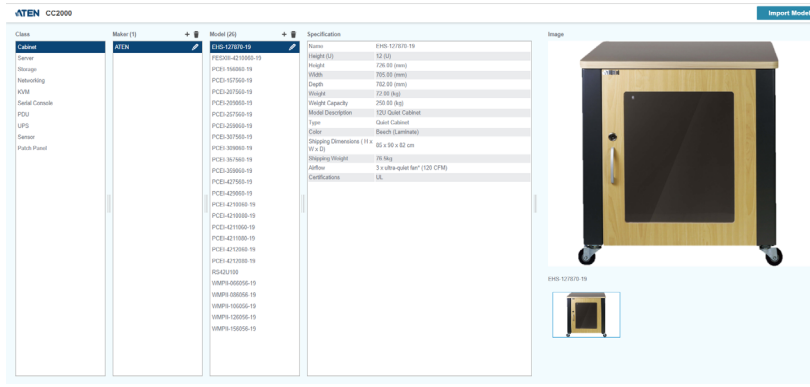
1. In CC2000 browser GUI, go to **Asset Management** > **Assets**.
2. From the tool bar, click More and select **Option**. This dialog box appears.



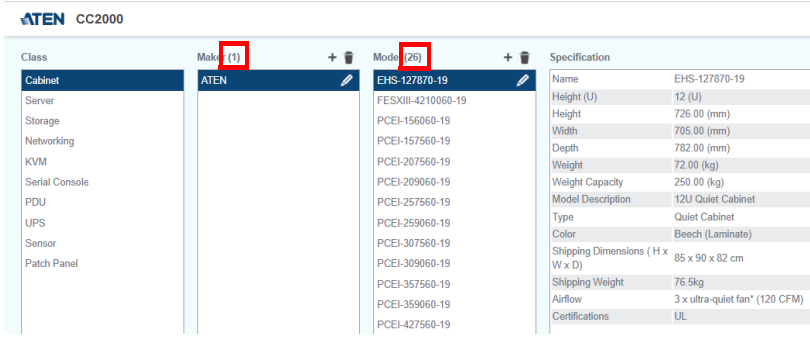
3. Select an option and click **Save** to apply the setting.

Model Library

A model library is repository of device specifications and photos that you can reuse when adding or configuring assets. The information is organized by device class, maker (brand), and model. To preview device specifications and photos, click on the class, maker, and model of the device.



The number in brackets indicates the total number of added makers or models.



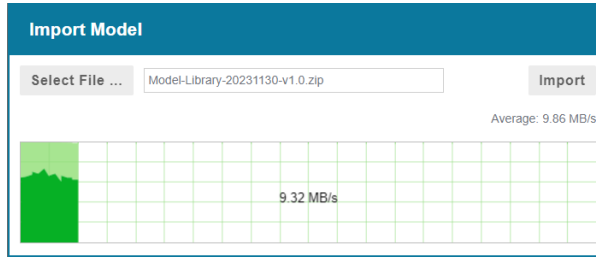
Importing Device Specifications to Model Library

1. Download device specifications package.
   a) Go to the ATEN CC2000 v4.0 product page.
   b) In the **Support and Downloads** tab, download the **ATEN Model Data Package** file.

   Note: Keep the downloaded file in the zip format.

2. Import the downloaded file to Model Library.
   a) In CC2000 browser GUI, go to **Asset Management** > **Assets**.
   b) From the tool bar, click More and select **Model library**. The Model Library appears in a separate browser page.
   c) Click Import Model . This dialog box appears.

   d) Browse the downloaded zip file and click **Import** to start the process. A progress dialog box appears.

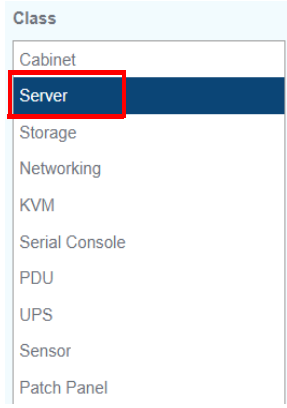


   e) When the progress bar indicates completion, wait for a little while for the change to take effect.

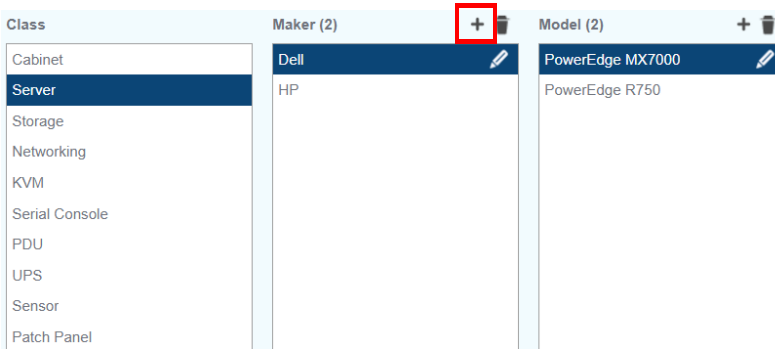
Adding a Device to Model Library

1. In CC2000 browser GUI, go to **Asset Management** > **Assets**.
2. From the tool bar, click More and select **Model library**. The Model Library appears in a separate browser page.
3. In the Model Library, select the class of the device you are adding.

   For example:

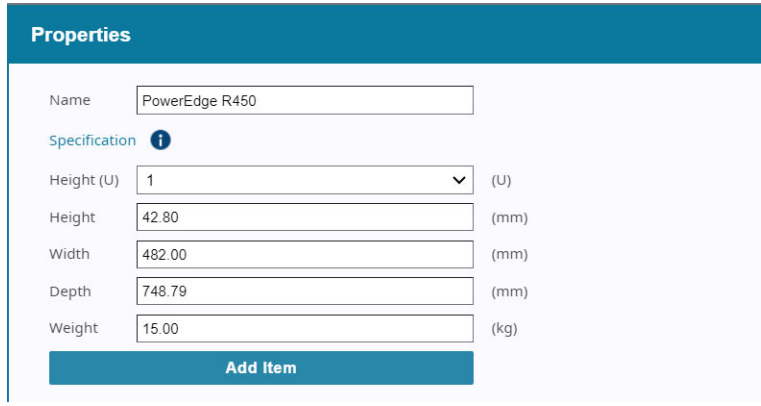


4. In the Maker column, select a maker or create a new one by clicking +, and type the maker for the device in the pop-up window.

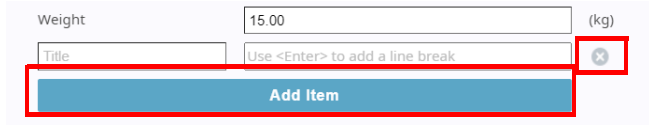


5. In the Model column, click + . A Properties window appears.
   a) Fill in the model and specifications for the device.

      Note: Specifications without a remove button ⊗ at the end are required. Make sure to fill in these fields before saving.



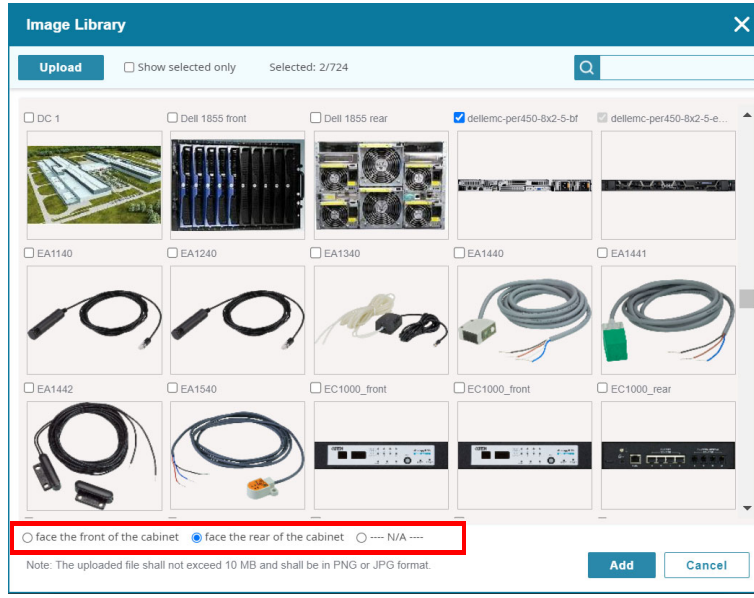
   - To add another specification, click **Add Item**. To remove an added specification, click ⊗ at the end of the specification.



   - To change the measurement system (imperial or metric), go to **Asset Management** > **Assets** > More > **Option**.

   b) To add device photos, click **+Add**. The Image Library window appears.

c) Select a photo from the Image Library. To add more photos to the image library, click **Upload**.



d) Select one of the following options to define the facing of this asset photo. The CC2000 uses this information to decide which photo to display when you view the install sites from different angles on dashboard.

- **face the front of the cabinet:** Select this option for a photo that shows the front panel of the asset.
- **face the rear of the cabinet:** Select this option for a photo that shows the rear panel of the asset.
- **N/A:** Select this option if the photo is neither showing a view from the front or rear of the cabinet.

Image Library

The image library is a repository of images used in CC2000 browse GUI. Use Image Library to store and edit the images you need for the system.

Importing Images to Image Library

1. In CC2000 browser GUI, go to **Asset Management** > **Assets**.
2. From the tool bar, click More and select **Image library**. The Image Library appears in a separate browser page.
3. Add, edit, or delete images as required.

Control	Description
Add	Click this button to browse for and upload one or multiple images at a time.
Edit	To crop, rotate, or reset an image, click on the image and then click this button.
Delete	Select one or more images and click this button to remove them from the Image Library.

Searching Images in Image Library

To search for specific images, use the filter, search, or both to help refine the search results.

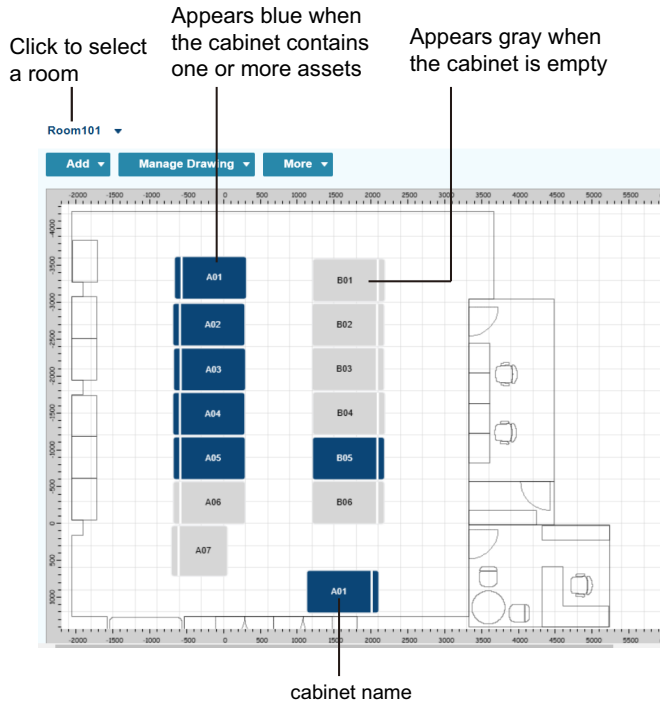
Control	Description
All assets	Click on the filter icon to access the following options: ◆ **Missing image files:** displays items with missing image files. ◆ **Not associated with model library:** displays images that are not used in Model Library.
	Type keywords in the search box and press **Enter** to do a fuzzy search of images based on the file name.

Floor Maps

Understanding Floor Maps

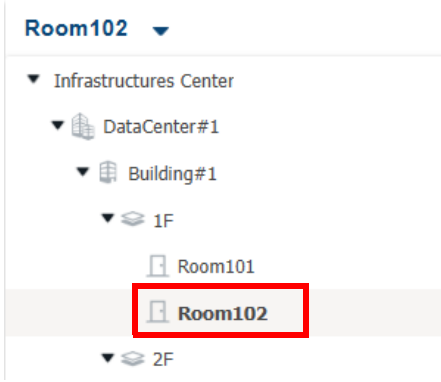
An *asset floor map* is a tool for defining asset deployment to allow remote management through the dashboard floor map. A dashboard floor map uses the configuration made in asset floor map to render 2D and 3D images, showing rail occupancy with asset photos, providing access to assets' property settings, and signalling alerts to prompt for intervention.

A floor map provides access to basic information (such as device photos) and specifications of the assets. Refer to the illustration below for an overview of tools and indications on a 2D floor map.



Creating a Floor Map

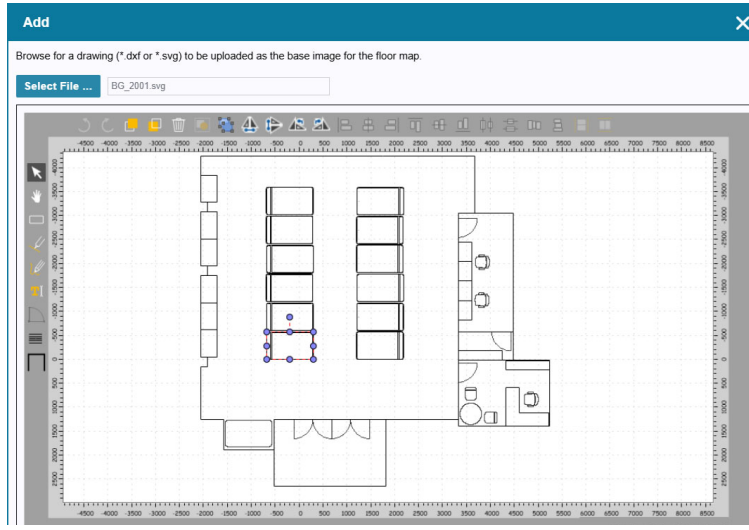
1. In CC2000 browser GUI, go to **Asset Management** > **Floor Maps**.
2. Select your target room from the Room drop-down list. For example:



3. (Optional) To add a base drawing, click **Manage Drawing** and click **Add**.
   a) In the pop-up window, click **Select File** to select and upload a base drawing (.dxf or .svg).

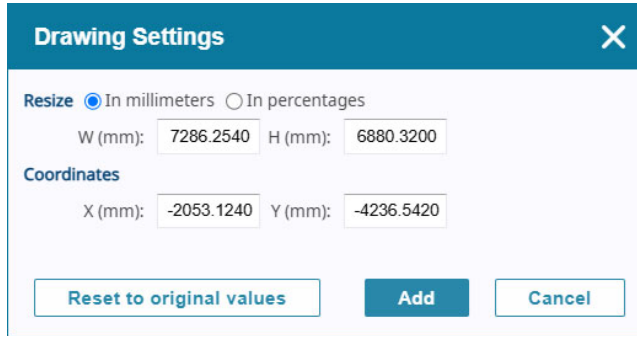
   Note: Make sure to use a .dxf or .svg file of 10 MB or less in file size.

   b) Edit the image as required.



   c) Click **Add**.

d) Adjust the drawing size and coordinates as required.

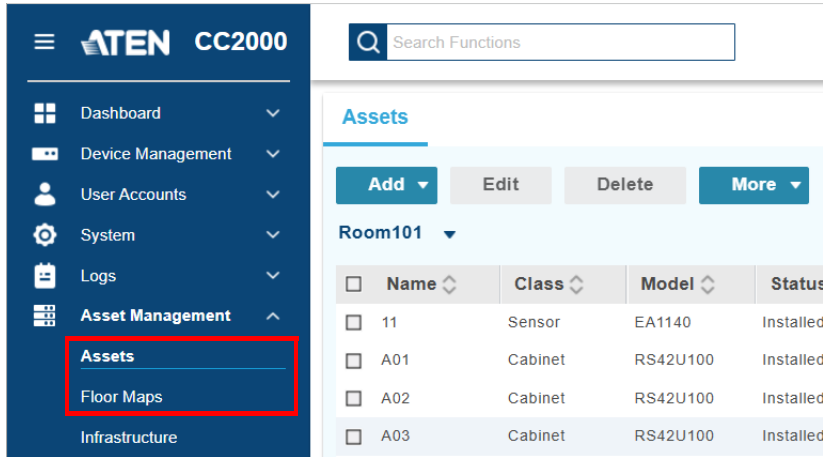


e) Click **Add** to apply the drawing.

4. Allocate the added cabinets, UPS, and/or sensors. For details, see *Allocating Cabinets, UPS, or Sensors on a Floor Map*, page 331.

Adding Cabinets, UPS, or Sensors

You can add cabinets, UPS, or sensors from either the **Assets** page or the **Floor Maps** page. The CC2000 system automatically synchronizes the added assets and their settings to both of these pages.



To add a cabinet, UPS, or sensor:

1. In CC2000 browser GUI, go to **Asset Management** > **Floor Maps**.
2. Select a room from the Room drop-down list to add assets.
3. Click **Add**, and then select an asset.

4. For detailed information on the properties of the added asset, refer to the following topics:
   - *Adding a Cabinet*, page 309
   - *Adding Other Asset Types*, page 312

Note:

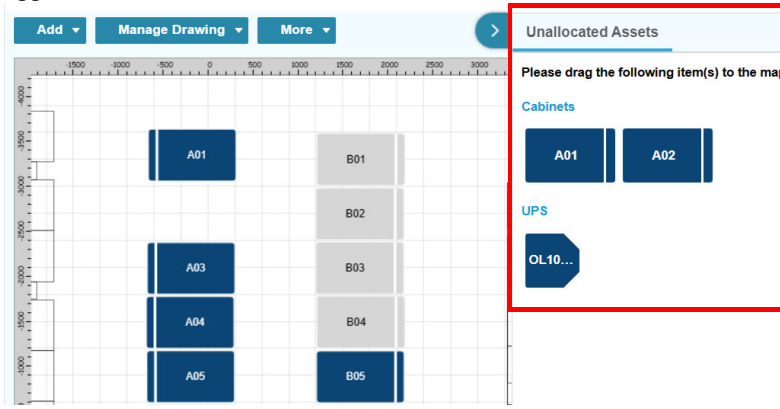
- With setup privileges for asset management, the CC2000 system prompts you to create a monitoring rule for the added sensor if it is bound to an unlocked sensor port and no monitoring rule has been configured for that port.
- For detailed information on monitoring rules, see *Event Monitoring*, page 158.

Allocating Cabinets, UPS, or Sensors on a Floor Map

After adding cabinets, UPS, or sensors to the asset list or floor map of the target room, allocate these assets onto the floor map.

1. In CC2000 browser GUI, go to **Asset Management** > **Floor Maps**.
2. Select your target room from the Room drop-down list.

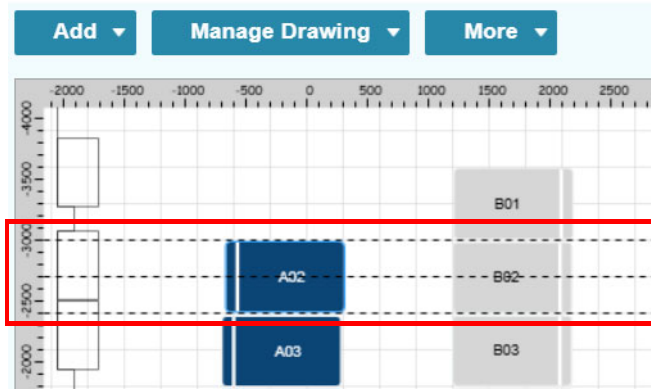
   If the room contains unallocated assets, the Unallocated Assets panel appears.



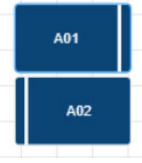
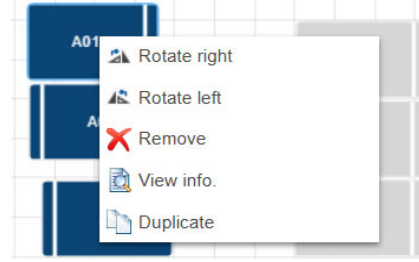
Note: If the Unallocated Assets panel does not appear, click ≡ to open the panel.

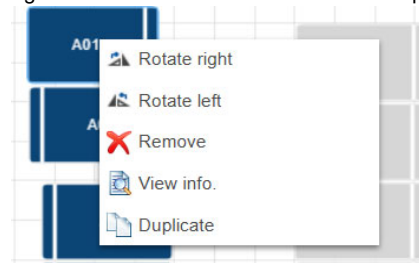
3. From the Unallocated Assets panel, drag-and-drop the asset onto the floor map.

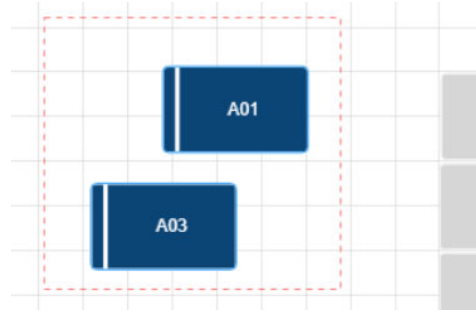
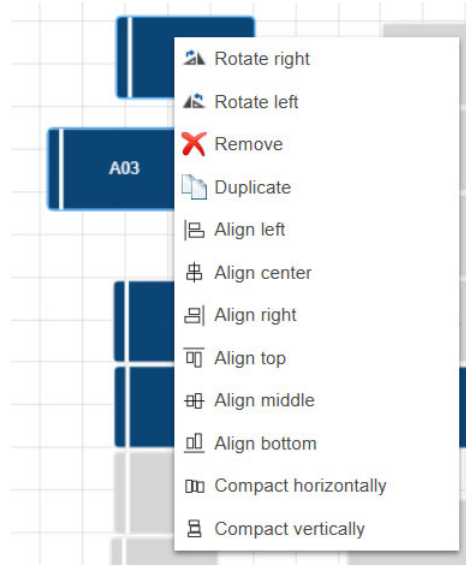
Tip: While dragging an asset on the floor map, drop the asset when alignment lines appear. The asset will be aligned with nearby assets.



4. (Optional) Adjust the orientation, alignment, and/or distribution of the added assets as needed.

Configuration	Control Actions
To change the orientation of an added cabinet, UPS, or sensor	1. Click on a cabinet, UPS, or sensor. A blue outline appears, indicating that the asset is selected.  2. Right-click on the asset. The action menu appears.  3. Select a rotation action.

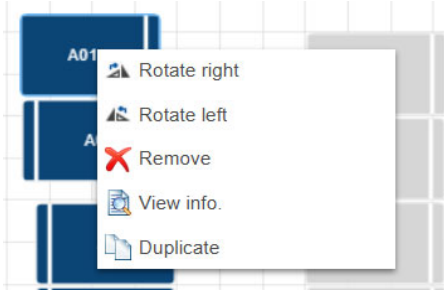
Configuration	Control Actions
To remove a cabinet, UPS, or sensor	1. Click on the cabinet, UPS, or sensor. A blue outline appears, indicating that the asset is selected.  2. Right-click on the asset. The action menu appears.  3. Select **Remove**. The asset now appears in the Unallocated Panel.

Configuration	Control Actions
To adjust alignment or distribution of multiple assets	1. Hold and drag the mouse to select the target assets.  2. Right-click on any of the selected assets. This menu appears.  3. Click an action from the pop-up menu.

Removing a Cabinet, UPS, or Sensor from the Floor Map

1. Click on the cabinet, UPS, or sensor. A blue outline appears, indicating that the asset is selected.

2. Right-click on the asset. The action menu appears.



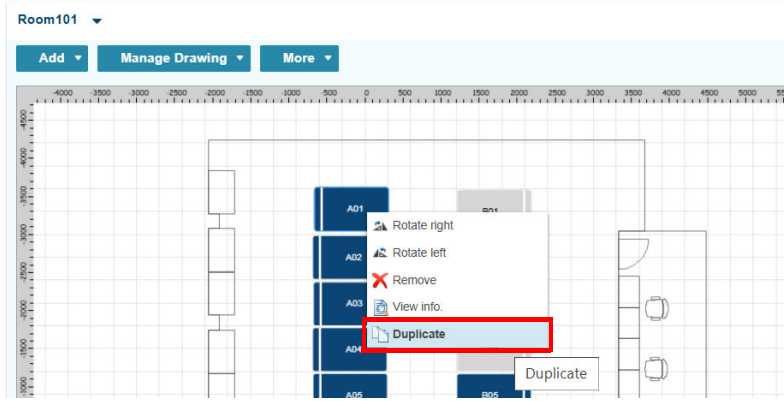
3. Select **Remove**. The asset is removed from the current floor map and appears in the Unallocated Panel.

Note: To completely remove an asset from the CC2000, use the asset page (**Asset Management** > **Assets)** to do so. If the target asset is a cabinet, also make sure all its installed devices (if the target asset is a cabinet) are removed first.

Duplicating a Cabinet, UPS, or Sensor

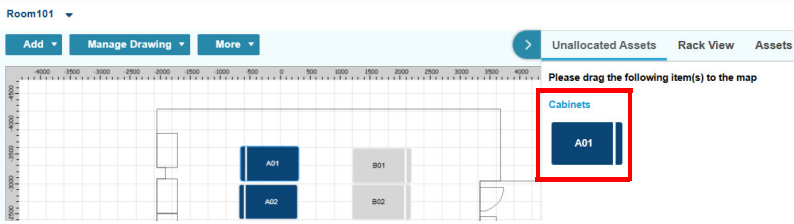
To duplicate a cabinet, along with its installed devices:

1. In a floor map, click on a cabinet first, and the right-click the cabinet.



   To duplicate multiple cabinets, click-and-drag to select cabinets, and then right-click anywhere on the selected cabinets.

2. From the pop-up menu, select **Duplicate**. The cabinet is duplicated to the unallocated panel.



3. Drag-and-drop the cabinet to the floor map.

Editing the Base Drawing

To edit a base drawing:

1. In CC2000 browser GUI, go to **Asset Management** > **Floor Maps**.
2. Select your target room from the Room drop-down list.
3. Click **Manage Drawing**, and then click **Edit**.

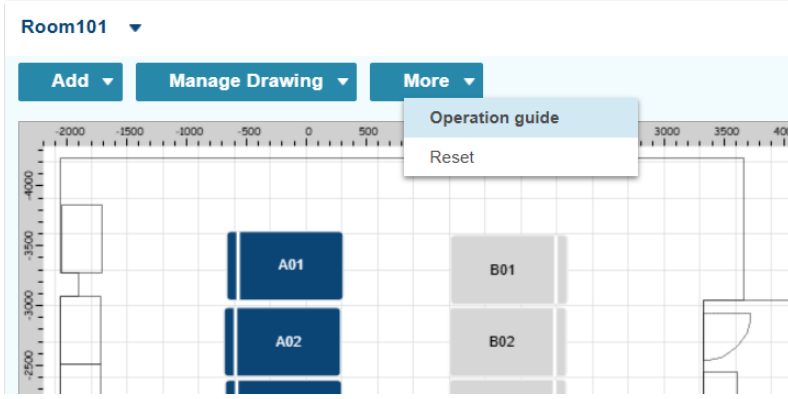
Navigating the Floor Map

Operation Guide

Refer to the table below for mouse/keyboard controls to help you navigate, obtain information, and access control functions on floor maps.

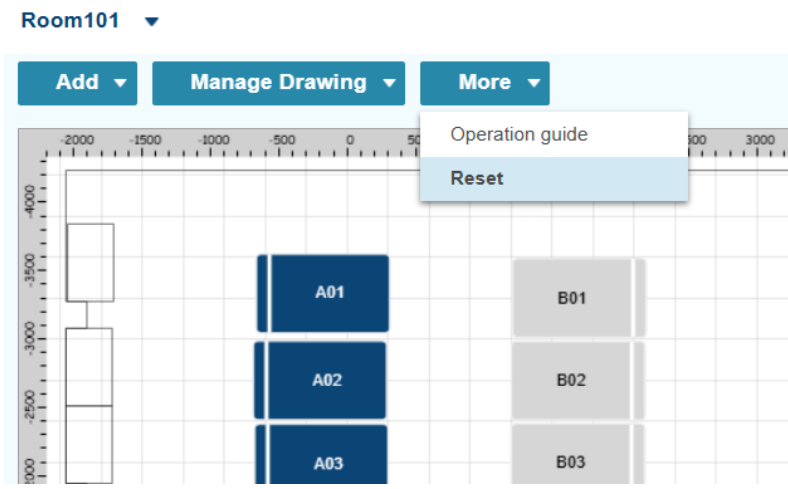
Operation	Mouse & Keyboard Action
Zoom in	Scroll the mouse wheel.
Move the map around	Shift + left mouse click to drag the map around
View details of an asset	Double-click on the asset.
Select two or more assets	Ctrl + left click on assets
Open menu for more control actions	Click on an asset, and then right-click on the asset.

You can also find this operation guide on the CC2000 browser GUI by clicking more and select **Operation guide**.:



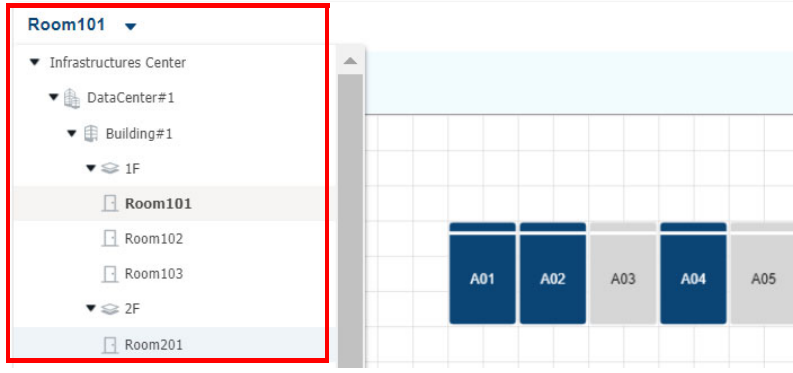
Resetting the Floor Map to Default Viewing Size

Click **More** and then select **Reset**.

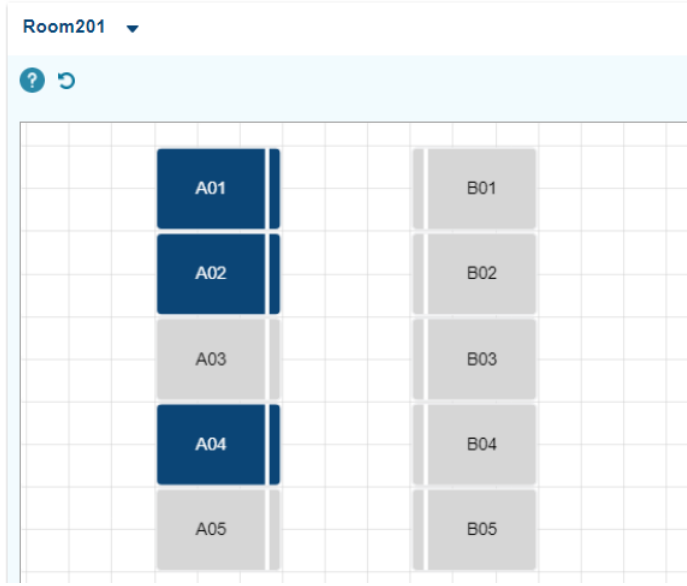


Switching to Floor Map of Another Room

1. Click on the Room drop-down list to open the infrastructure map.

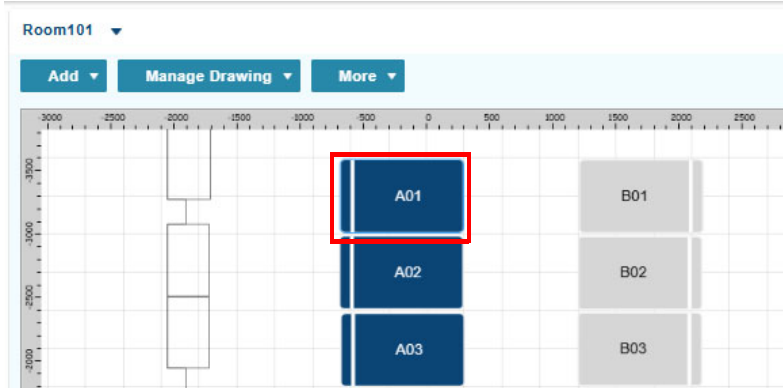


2. Select a room from the infrastructure map. The floor map for the room appears.

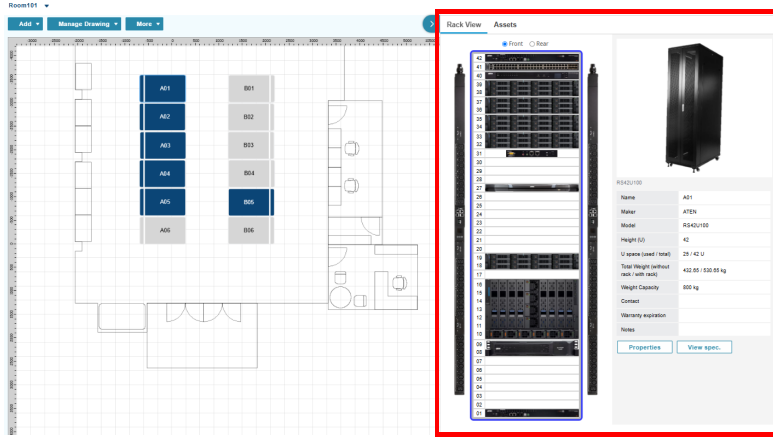


Viewing Asset Properties and Specifications

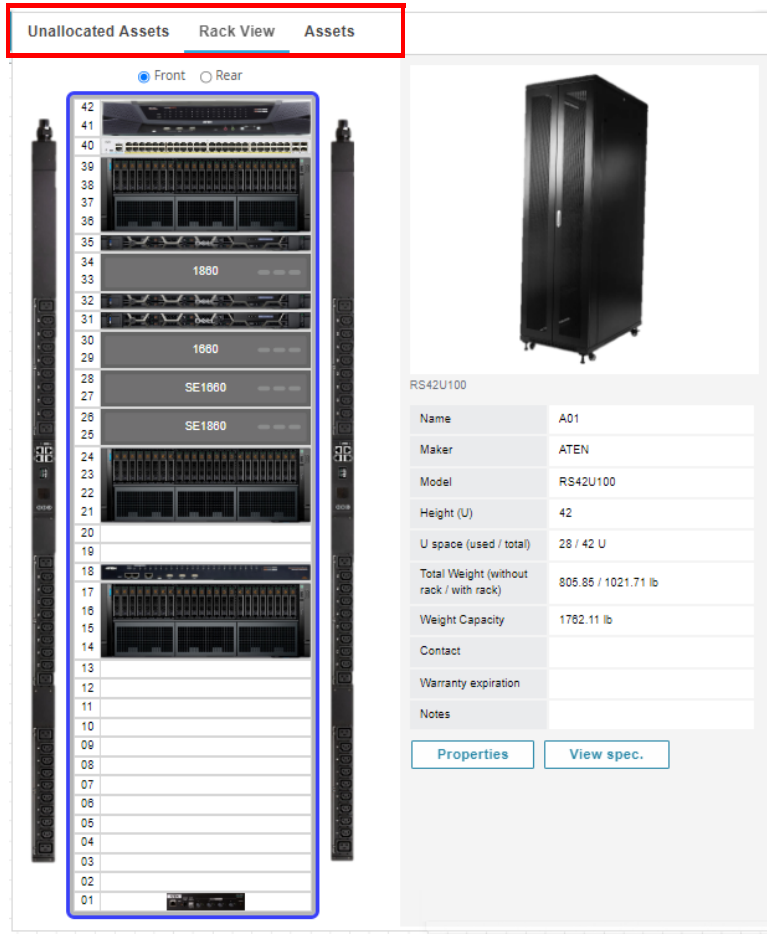
1. From a floor map, double-click on a cabinet.



2. The rack view of the cabinet appears.

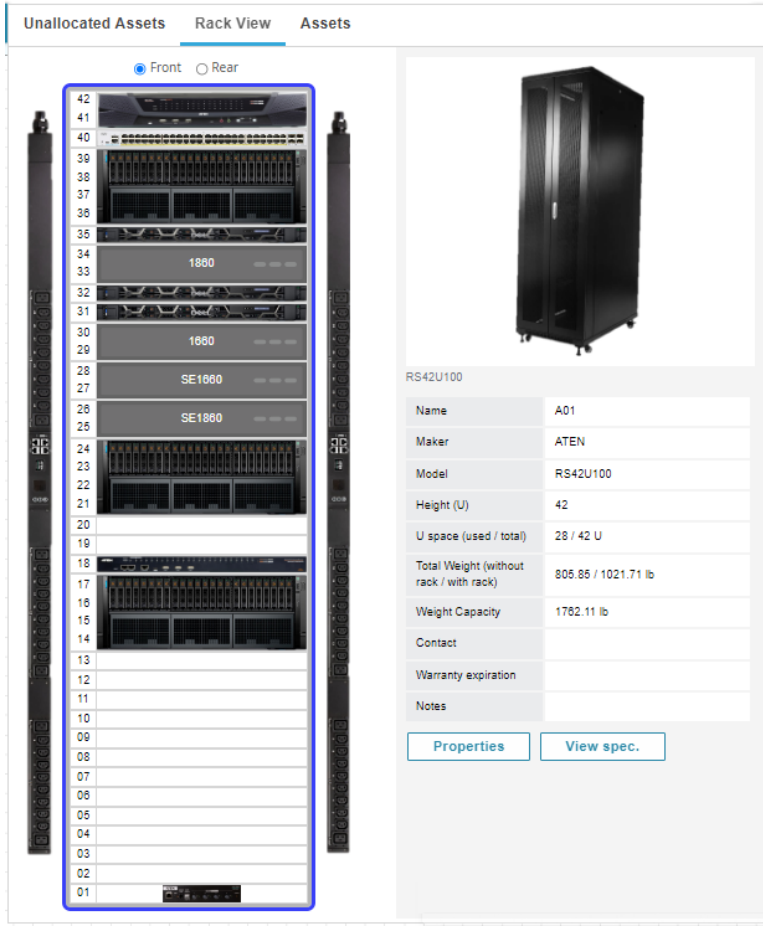


3. Click these tabs to access information.

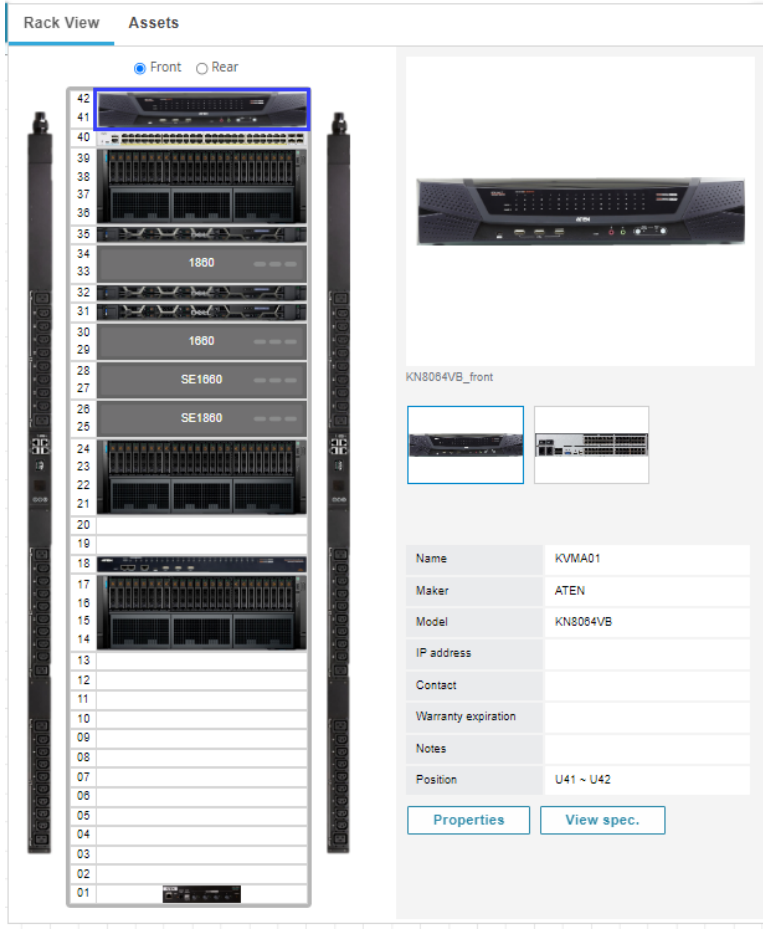


- **Unallocated Assets:** This tab lists assets that have been added to the asset list, but not yet allocated to any floor maps.
- **Rack View:** This tab shows the rack in front and rear views and asset information.
- **Assets:** This tab lists all the assets for the selected cabinet.

Rack View – a cabinet is selected



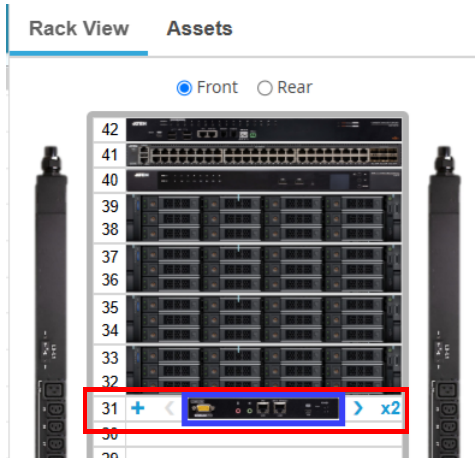
Rack View – an individual device is selected



In the Rack View tab, click on the cabinet or an individual device to access the following:

- To switch the cabinet view between front or rear, click the **Front** or **Rear** radio button.
- To view properties or specifications of the cabinet/an individual device, click **Properties** or **View spec.** button accordingly.

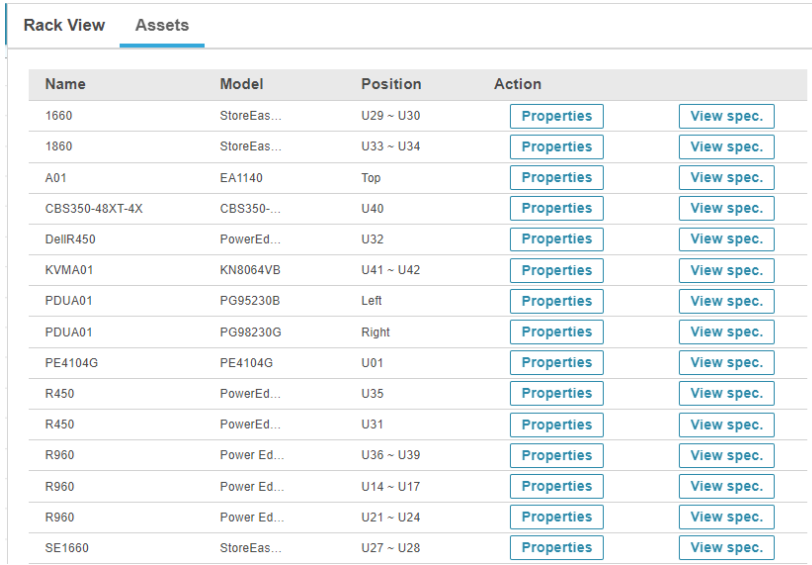
- For a rail that is installed with more than one device, mouse over the rail space and click on the blue arrows to switch views. The blue number indicates the number of devices installed to the rail.



  - Click + to add another device to the rail.

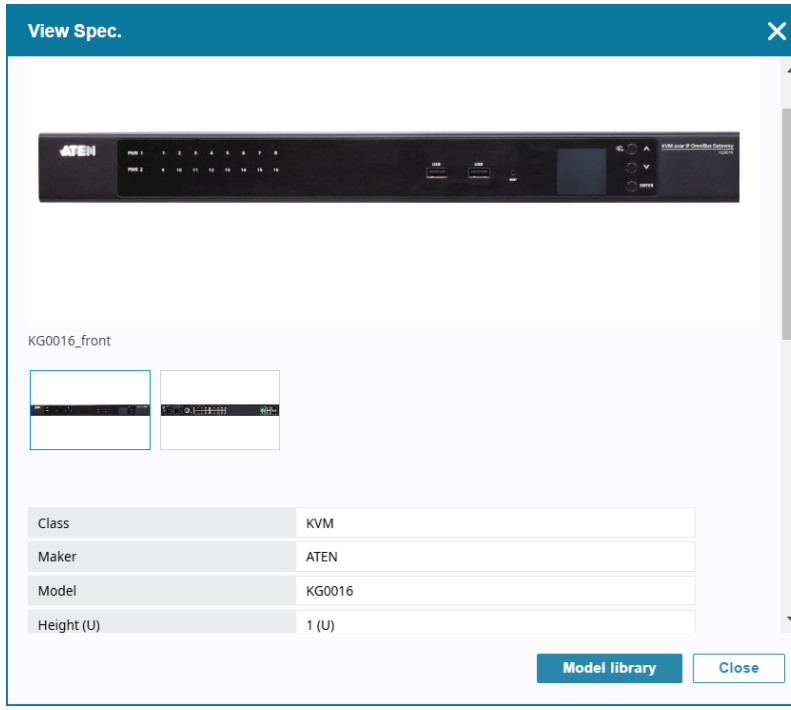
Assets Tab

To show a list of installed assets, click the **Assets** tab. This page appears. Click on **Properties** or **View spec.** to see more information.



View Specs

View full specifications from this window. To revise specs, click the **Model library** button to access the settings.



Exporting the Floor Map with Added Assets

To export the floor map, along with the added cabinets, UPS, and/or sensors icons:

1. In CC2000 browser GUI, go to **Asset Management** > **Floor Maps**.
2. Select your target room from the Room drop-down list.
3. Click **Manage Drawing**, and then click **Export floor map**. The file is exported in .svg.

Exporting the Base Drawing

To export the base drawing (the floor map without the added cabinets, UPS, and/or sensors icons):

1. In CC2000 browser GUI, go to **Asset Management** > **Floor Maps**.
2. Select your target room from the Room drop-down list.
3. Click **Manage Drawing**, and then click **Export drawing**. The file is exported in .svg.

Duplicating the Base Drawing to Another Room

To duplicate the base drawing to another room:

1. In CC2000 browser GUI, go to **Asset Management** > **Floor Maps**.
2. Select your target room from the Room drop-down list.
3. Click **Manage Drawing**, and then click **Copy to**. The drawing is applied immediately.

Appendix A

Technical Information

License Agreement

End User Software License Agreement For CC2000 Series

This END USER SOFTWARE LICENSE AGREEMENT is entered into as of the date of installment of the Licensed Software by you ("Effective Date"), by and between ATEN International Co. Ltd., having its principal place of business at 3F, No. 125, Sec. 2, Da-Tung Rd., Si-Jhih, Taipei, Taiwan 221, R.O.C. ("ATEN") and YOU.

This Agreement is a legal agreement between you (either an individual or a single entity) and ATEN. PLEASE READ THIS AGREEMENT CAREFULLY. BY INSTALLING OR USING THE SOFTWARE THAT ACCOMPANIES THIS AGREEMENT ("Software"), YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE, DO NOT USE THE SOFTWARE. YOU have the rights below:

1. DEFINITIONS:

1.1

"Licensed Software" shall be defined as the object code version of software programs or files in machine readable format provided to YOU by ATEN.

1.2

"Documentation" means all manuals, user documentation, and other related materials pertaining to the Licensed Software that ATEN provides to YOU.

2. GRANT OF RIGHTS:

2.1

ATEN hereby grants to YOU, and YOU hereby accept, subject to the terms and conditions of this Agreement, a non-exclusive, non-transferable, non-sublicense, non-assignable, non-irrecoverable, limited license to install the Licensed Software to the hardware with ONE COPY ONLY, and to use the hardware, incorporated Licensed Software and the related Documentation.

Aforesaid grants are restricted as follows: (a) The Licensed Software hereunder is licensed, not sold, to you by ATEN. YOU acknowledge that all copyrights and intellectual property rights in the Licensed Software in any form provided by ATEN to YOU are the sole property of ATEN and its licensor. YOU shall not have any right, title or interest in or to any of the copyrights and intellectual property rights in the Licensed Software. ATEN reserves all rights not expressly granted. (b) YOU may make a single archival copy of the Licensed Software only, but may not copy, modify, distribute, or resell the Licensed Software. (c) You may not rent, lease, lend or encumber the Licensed Software. (d) You may not decompile, or reverse engineer the Licensed Software. (e) The terms and conditions of this Agreement will apply to any Licensed Software updates, provided to you at ATEN's discretion. (f) the Licensed Software is not designed, licensed or intended for use in the design, construction, operation or maintenance of any nuclear facility. ATEN and its licensors disclaim any express or implied warranty of fitness for such use. (g) No right, title or interest in or to any trademark, service mark, logo or trade name of ATEN or its licensors is granted under this Agreement.

3. LIMITED WARRANTY.

3.1

WITHOUT WARRANTY OF ANY KIND, ATEN solely warrants that the Licensed Software will meet the functions provided by ATEN for a period of thirty (30) days from the date of receipt. If an implied warranty or condition is created by your state/jurisdiction and federal or state/provincial law prohibits disclaimer of it, YOU also have an implied warranty or condition, BUT ONLY AS TO DEFECTS DISCOVERED DURING THE PERIOD OF THIS LIMITED WARRANTY. Otherwise, the Licensed Software is licensed "As-Is". You bear the risk of using it except otherwise expressed above. ATEN gives no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this agreement cannot change. To the extent permitted under your local laws, ATEN excludes the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

3.2

ATEN hereby declares that (a) this Licensed Software may contain Java technology. You shall make a separate agreement for modifications to or use of the Java technology under compatibility requirements available at www.java.net, and (b) this Licensed Software also may contain open source code from the global community of open source developers. With respect to Licensed Software, Documentation and any Updates and modifications thereof

that is embodied in the Java Compatibility (includes, but not limited to JavaMail API, JavaBeans Activation Fremawork (JAF), AXL-RADIUS, AXL-TACACS, JavaServiceWrapper (3.2.3)) and open source, (includes, but not limited to J2SE JRE, Apache Tomcat, Apache Derby database, Apache Struts framework, JSR 80) or other technologies belonging to third parties, patent holders of such technology may contact YOU and request the payment of royalties. YOU ACKNOWLEDGE THAT ATEN IS NOT RESPONSIBLE FOR THE PAYMENT OF SUCH ROYALTIES AND THAT YOU WILL NEGOTIATE IN GOOD FAITH WITH THE RESPECTIVE PATENT HOLDERS TO ADDRESS THEIR CLAIMS AND OBTAIN NECESSARY LICENSES AS REQUIRED. IN NO EVENT SHALL ATEN BE RESPONSILBLE FOR ANY LOSS AND COST AGAINST AFORESAID INFRINGEMENT OR ROYALTY CLAIMS. ATEN FURTHER DISCLAIMS ALL WARRANTIES AGAINST INFRINGEMENT, EXPRESS OR IMPLIED, WITH RESPECT TO OPEN SOURCE OR JAVA TECHNOLOGY THAT IS EMBODIED IN THIS LICENSED SOFTWARE.

4. Limitation of Liability.

IN NO EVENT SHALL ATEN BE LIABLE TO YOU OR ANY END-USERS, FOR ANY LOSS OF PROFIT, INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES ARISING OUT OF OR RELATING TO THE LICENSING OR USE OF THE SOFTWARE, DOCUMENTATION FOR ANY ERROR OR DEFECT. IF, AT ANY TIME, ATEN SHALL HAVE ANY LIABILITY ARISING FROM OR BY VIRTUE OF THIS AGREEMENT, AND WHETHER SUCH LIABILITY IS DUE TO ATEN'S OR ITS AFFILIATE'S NEGLIGENCE, BREACH OF ITS OBLIGATIONS HEREUNDER, OR OTHERWISE, IN NO EVENT WILL THE TOTAL AGGREGATE LIABILITY OF ATEN AND ITS AFFILIATES FOR ANY CLAIMS, LOSSES, OR DAMAGES INCURRED BY YOU EXCEED THE LICENSE FEE HEREUNDER. THIS LIMITATION OF LIABILITY IS COMPLETE AND EXCLUSIVE, SHALL APPLY EVEN IF AMD OR ITS AFFILIATES HAS BEEN ADVISED.

5. Export Regulations.

All Software, documents and any other materials delivered hereunder are subject to the applicable export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with these laws and regulations and acknowledge that you have the responsibility to obtain any licenses to export, re-export, or import as may be required after delivery to you.

6. TERMINATION:

This Agreement shall be effective on the Effective Date and shall continue in effect until terminated by ATEN without any cause upon prior thirty days' written notice to YOU, or upon the prior thirty days' announcement on the ATEN website.

7. MISCELLANEOUS:

7.1

The following provisions of this Agreement shall survive its termination or expiration: Sections 2, 3, 4, 5 and 6.

7.2

The rights and obligations of each party to this Agreement shall not be governed by the provisions of the United Nations Convention on Contracts for the International Sale of Goods, but instead this Agreement will be governed by and construed in accordance with the laws of the Republic of China.

7.3

If any provision of this Agreement shall be held by a court of competent jurisdiction to be illegal, invalid or unenforceable, the remaining provisions shall remain in full force and effect.

7.4

This Agreement may be supplemented, modified, amended, released or discharged by a notice of ATEN in writing, or prior thirty days' announcement on the ATEN website.

7.5

If any action at law or in equity, including an action for declaratory relief or injunctive relief, is brought to enforce or interpret the provisions of this Agreement, the prevailing party shall be entitled to reasonable attorneys' fees in addition to any other relief to which the party may be entitled.

7.6

Any waiver by either party of any default or breach hereunder shall not constitute a waiver of any provision of this Agreement or of any subsequent default or breach of the same or a different kind.

Technical Support

International

- For online technical support – including troubleshooting, documentation, and software updates: **http://eservice.aten.com**
- For telephone support, see *Telephone Support*, page ii.

North America

Email Support		support@aten-usa.com
Online Technical Support	Troubleshooting Documentation Software Updates	http://www.aten-usa.com/support
Telephone Support		1-888-999-ATEN ext 4988 1-949-428-1111

When you contact us, please have the following information ready beforehand:

- 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.
- Any other information you feel may be of help.

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 1.37cm

Supported ATEN KVM Products

For a comprehensive list of supported products, visit the CC20004.0 product page, and scroll to the bottom to find out.

Device ANMS Settings

To enable CC Management of a device from the device's ANMS page, do the following:

1. Log into the device.
2. Refer to the device's User Manual to locate its ANMS page.
3. In the ANMS page, click the checkbox to *enable* CC Management, then key in the IP address and device port number (see *Device port*, page 15), of the CC2000 server that will manage the device.

VPNs

Basically, a VPN (virtual private network) is a private network that uses a public network (usually the Internet) to connect several sites together. It typically includes several WANs. Many companies create their own VPN to provide a secure network connection between two sites. One drawback to VPNs, however, is that while the network is secure, its throughput can be slow.

If a VPN is used to connect several sites in a CC2000 management system, the only CC2000 server that is absolutely necessary to manage that system is a single Primary – rather than the network of primary and secondary CC2000 servers necessary with the standard Internet deployment. We recommend that at least one CC2000 secondary server is deployed, however, in order to provide redundant services to the connected devices.

Another advantage of deploying additional CC2000 Secondaries is that they can provide more efficient operation and management by accelerating network traffic.

Firewalls

When several CC2000 servers are located behind separate firewalls, the following service ports must be specified on the servers, and opened on the firewall.

1. CC Port

Note: Each CC2000 server can have a different setting (8001 on Server 1; 8005 on Server 2, for example). But the port opened on the firewall must correspond to the CC Port setting (8001 on Server 1's firewall; 8005 on Server 2's firewall).

2. The CC2000 primary server's HTTPS port
3. The CC2000 proxy port (see *CC2000 Proxy Function* in the next section).
4. The CC2000 secondary server's HTTPS port (Optional)

Note: 1. CC2000 Client Workstations can open web browser sessions to CC2000 secondary servers within the same firewall. Communication and access with other CC2000 servers on the installation (outside of the firewall) takes place through the CC and Proxy ports – therefore the HTTPS port isn't necessary. There is a drawback to doing this, however, in that you won't be able to perform device configuration on devices outside the firewall.

2. You can open this port if you would like CC2000 Client Workstations outside the firewall to be able to directly open a web browser session to the secondary server inside the firewall.

CC2000 Proxy Function

Activating CC2000 proxy function (proxy server) allows data transmission via a CC2000 server when client PCs are unable to directly communicate with KVM (managed by the CC2000 server) via viewers.
If "Always use proxy" is checked, data is always transmitted via the CC2000 server.
As data is transmitted via the CC2000 server, its bandwidth may vary depending on the number of active viewers – KVM sessions.
For CC2000 Client Workstations (client PC) that are *outside* a firewall to access KVM and serial devices managed by a CC2000 server *inside* the firewall, the CC2000 Proxy function must be enabled on the CC2000 server and two specific ports must be configured (opened) on the firewall:

- TCP Port (default 443) for safe Internet connection (https://) between the CC2000 and the client PC.
- TCP Port (default 8002) for image and Telnet data transmission of viewers.

Note: If you do not wish to use the Proxy function, you must open all of the service ports (HTTPS, Program, Virtual Media, Telnet, SSH, etc.) on the firewall as required by the devices.

Name, Description, and Range Parameters

The following table lists the parameters and defaults for names, descriptions and ranges found in the CC2000 management system:

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

Category		Length / Range	Default
Users	Login name	Up to the equivalent of 32 English alphanumeric characters. The minimum number of characters is based on the account policy settings (see *CC2000's Built-in Authentication Service*, page 204). The following characters may not be used: **/ \ [ ] : ; | = , + * ? < > @ " '**	
	Password	The equivalent of 0–16 English alphanumeric characters. The minimum number of characters is based on the account policy settings (see *CC2000's Built-in Authentication Service*, page 204). 0 means no password authentication needed.	
	Description	Up to 256 Bytes.	
	Session Timeout	1–99 min.	3 min
	Unexpected disconnection timeout	2–10 min.	2 min.
	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 Types	Name	2–32 Bytes. The following characters may not be used: **" '**	
	Description	Up to 256 Bytes.	

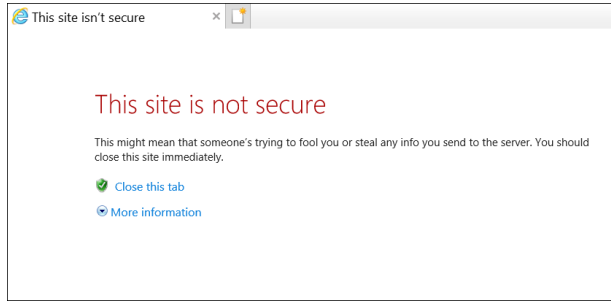
Category		Length / Range	Default
Authentication Server	Server name	2–32 Bytes. The following characters may not be used: **" '**	
	Description	Up to 256 Bytes.	
	Browser Method	Unlimited for Username and Password. **Note:** CC2000 performance may be adversely affected if there are too many characters.	
CC2000 Authentication	Username Minimum	Up to the equivalent of 32 English alphanumeric characters. The minimum number of characters is based on the account policy settings (see *CC2000's Built-in Authentication Service*, page 204). The following characters may not be used: **/ \ [ ] : ; | = , + * ? < > @ " '**	6
	Password Minimum	The equivalent of 0–32 English alphanumeric characters. The minimum number of characters is based on the account policy settings (see *CC2000's Built-in Authentication Service*, page 204). 0 means no password authentication needed.	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	1–32 Bytes.	
	Description	Up to 256 Bytes.	
Departments / Locations	Name	1–32 Bytes.	
	Description	Up to 256 Bytes.	
Tasks	All Tasknames	No limit on the number of Bytes.	
	Primary Database Backup Password	0–32 Bytes. 0 means no password authentication needed.	
	Export Device Log Pattern	No limit on the number of Bytes.	

Category		Length / Range	Default
System Log Options	By Period	30-1096 days	
	By Record	10,000–1,000,000	
	Records per page	100, 300, 500	
Log Notification Settings	Subject	1–128 Bytes.	
	Mail from	Up to 64 Bytes.	
	Send to	Up to 128 Bytes.	

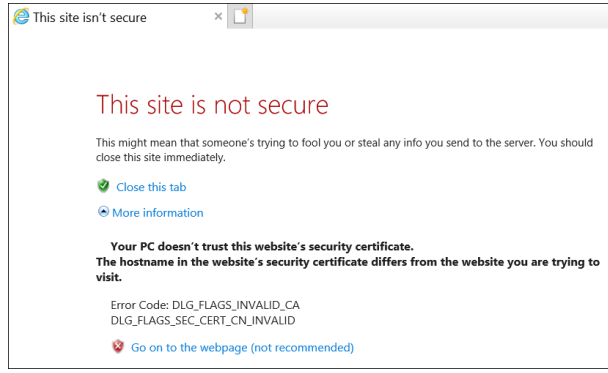
Trusted Certificates

Overview

When you try to log in to the device from a browser, a Security Alert message appears 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, click **More information** and click **Yes** to go on.

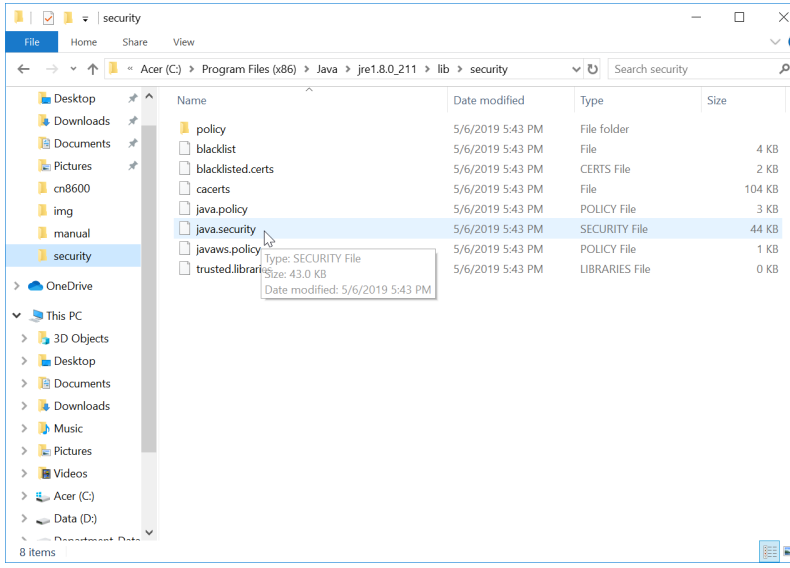
Note: To avoid having to go through the certificate acceptance prompt every time when logging in, you can use a third party certificate authority (CA) to obtain a signed certificate. See *Importing a Signed SSL Server Certificate*, page 241, for details.

Adding ARM-based PE series PDU

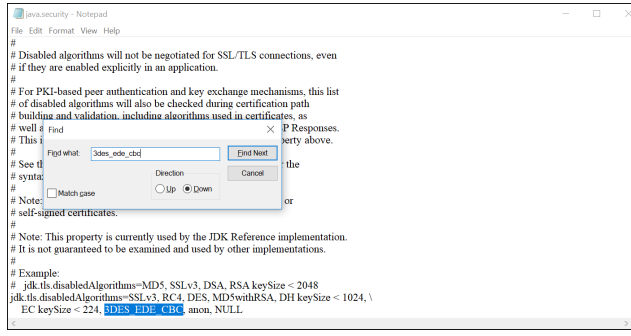
Compatibility settings of Java may prevent you from adding ARM-based PE series PDU.

Follow the steps below to modify the compatibility:

1. Go to your Java folder.
   e.g. C:\Program Files (x86)\Java\jre1.8.0_211\lib\security
2. Locate the file “java.security”.



3. Open it with a text editor (e.g. notepad) and use the **Find** function.
4. In the **Find** window, enter “3DES_EDE_CBC,” as exemplified below:



5. Delete the “3DES_EDE_CBC” part and save the file.

Note: It is recommended to keep this whole line of text in a separate text file should you wish to add it back later on.

6. Restart your computer and add your ARM-based PE series PDU as demonstrated in *Adding an ATEN KVM or Serial Console Device* on page 77.

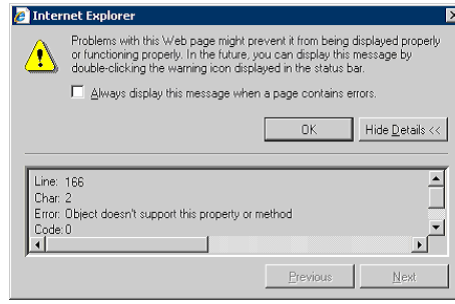
Troubleshooting

Problem	Resolution
A few minutes after installing the CC2000, the following error message appears: *Error 1067*	The error message is generated by the Operating System, it indicates that the CC2000 service is unable to run. To resolve the problem, try the following: 1. Reboot the computer. 2. See if your computer meets the minimum requirements to run the CC2000 (see *Server Requirements*, page 6). 3. If there was a previous version of the CC2000, 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 the CC2000*, page 23). Uninstall, by following the procedures mentioned, and reinstall the CC2000.
I entered the IP address for the CC2000's web interface, but cannot bring up the CC2000 login page.	1. The CC2000 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 set to something else by the administrator, the port number must be entered as part of the URL string. For example, if the CC2000's IP address is 10.10.10.10, and the SSL port has been set to 8443, then the URL string that you enter in the browser should be: `https://10.10.10.10:8443` 2. Other services running on the CC2000 server are occupying the same ports. Use the CC2000 Utility (see page 371) to change the port settings. 3. Make sure that the CC2000 service is running. If you are running Windows, see *Post-installation Check*, page 18; if you are running Linux, see *Post-installation Check*, page 21.
The language of the login dialog box wording is not the language I have set in my CC2000 Preferences.	The language of the login page first corresponds to the language that your browser is set for, and then look at what your OS language is. The CC2000 will display in the language you have set in Preferences once logged in.
I cannot log in to the CC2000.	Make sure your Username and Password are correct.

Problem	Resolution
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.”	Certain browsers (e.g. Mozilla-based browsers) share the same session ID for multiple connections to the same server. The CC2000 will deny any login request when there already is a session opened 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.
When I log in, the browser generates a *CA Root certificate is not trusted* or *Certificate Error* response.	The certificate’s name is not found on Microsoft’s list of Trusted Authorities. The certificate can be trusted, however. See *Trusted Certificates*, page 359, for details.
After I log in to the CC2000, There is no device management page.	You have not been authorized to access any ports. Check with your CC2000 administrator to get authorization for accessing the ports you are responsible for.
After I log in to the CC2000, I cannot bring up the page for the device I want to access.	Check with your CC2000 administrator to find out whether you are authorized to access that device.
When I log in to the CC2000, the only page that comes up is the System Management tab with only two menu entries: *This Server* and *License*.	A license conflict has occurred. See *License Conflict*, page 248, for details on resolving the problem.
I am not receiving email notifications of event trap situations	1. Check that the email server settings have been specified correctly in the CC2000 Manager. 2. Check that the email address specified in the related device’s settings has been set correctly. 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 device management page, nothing happens.	Generic devices are accessed directly via the device’s IP address. If the IP address has changed (because of a DHCP change, for example), then clicking the old IP address will not connect to the device at the new address. Ascertain the device’s new IP address and change its settings accordingly.
The device I want to add cannot be found.	1. Make sure the CC2000 Manager is running and all services have started successfully. 2. Make sure that CC Management has been enabled and specified correctly in the device’s ANMS page.
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 online. See *Adding an ATEN KVM or Serial Console Device*, page 77, for details.

Problem	Resolution
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 the CC2000. Update the device's firmware to the latest version.
Devices connected to my CC2000 secondary servers do not show up in the primary server's Available Devices list.	1. Check to see if the device has already been added. If it has, it will not show up in the list. 2. Click the Auto Discovery button on each of the Secondaries. 3. After trying #2, if the devices don't show up, check if the device's ANMS has been enabled and that the IP and port address of the CC2000 you want the device to be recognized by has been correctly specified. 4. After trying #2, if the devices do show up, there was probably a network problem. Perform the Replicate Database to the Primary function. See *Replicate Database*, page 266, for details.
My ATEN/Altusen device isn't recognized by the CC2000.	1. The device in question may not be supported by the CC2000 management system. See *Supported ATEN KVM Products*, page 352, for a list of supported devices. 2. The device's firmware must be upgraded to the latest version in order to be capable of CC2000 management.
After making a setting change and clicking Save, a **HTTP Status 500 -** error page comes up.	You made a mistake when you entered the setting. This is an Apache Tomcat error message that appears whenever it receives a setting that makes no sense to it. To recover, select any other tab and then come back to make your change – be sure to enter a valid setting.
I set the CC2000 for "No timeout" operation, but it timed out anyway.	The change doesn't take effect until the next time you log in.

Q1: When I open a viewer, the web page does not display or work correctly, and I receive an error message that is similar to the following:



1. Reset the Internet Explorer security settings to enable Active Scripting, ActiveX controls, and Java Web Start.

   By default, Internet Explorer 6 and some versions of Internet Explorer 5.x use High security level for Restricted sites zone, and Microsoft Windows Server 2003 uses High security level for both Restricted sites and Internet zone. You may want to enable Active Scripting, ActiveX controls, and Java Web Start. To enable Active Scripting, ActiveX controls, and Java Web Start, follow these steps:

   a) Start Internet Explorer.

   b) On the Tools menu, click Internet Options.

   c) In the Internet Options dialog box, click Security.

   d) Click Default Level.

   e) Click OK.

2. Verify that Active Scripting, ActiveX, and Java are not blocked

   If some computers work but not others, 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 Web Start.

3. Verify that your anti-virus program is not set to scan the Temporary Internet Files or Downloaded Program Files folders

4. Delete all temporary Internet files

   To remove all temporary Internet files from your computer, follow these steps:

   a) Start Internet Explorer.

   b) On the Tools menu, click Internet Options.

   c) Click the General tab.

   d) Under Temporary Internet files, click Settings.

   e) Click Delete Files.

   f) Click OK.

   g) Click Delete Cookies.

   h) Click OK.

   i) Under History, click Clear History, and then click Yes.

   j) Click OK.

5. Make sure that you have the latest version of Microsoft DirectX installed

   For information about how to install 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

6. Make sure that you have the latest version of OpenJDK 8 or Java JRE 8 installed.

   For information about how to install the latest version of OpenJDK 8 or JRE 8, visit the websites www.azul.com or www.java.com

Installing OpenJDK 8

To install OpenJDK 8, make sure the any pre-existing JRE has been removed.

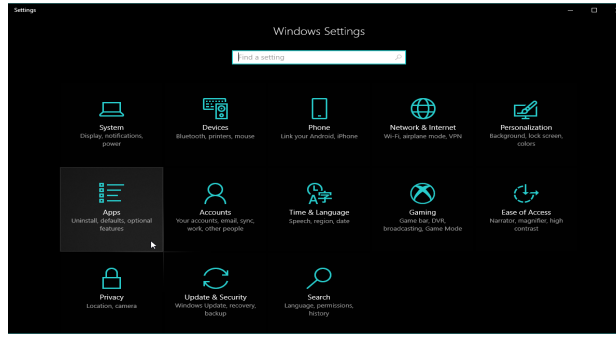
After installing OpenJDK 8, make sure you restart your CC2000 service.

Windows

The operations for most Windows versions are the same. Windows 10 is used in the example procedures demonstrated below.

Uninstalling JRE

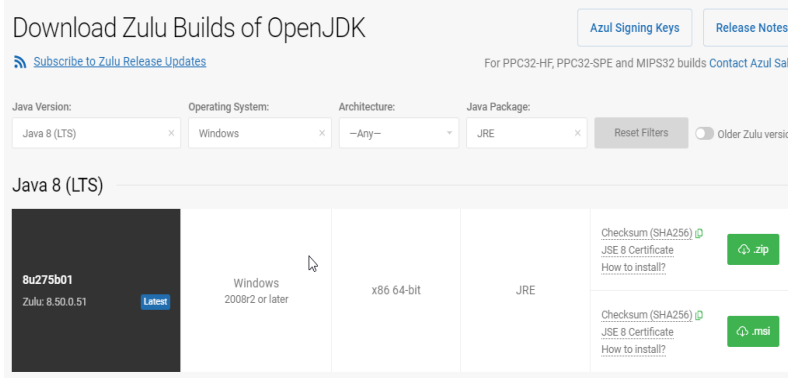
1. Click **Start** > **Settings.**



2. Click **Apps** for the app list, find and click Java.
3. Click **Uninstall** and follow the on-screen instructions.
   If you have multiple Java on the system, uninstall them all.

Downloading and Installing OpenJDK

1. Go to www.azul.com, hover your mouse over “Downloads” and click **Zulu Builds of OpenJDK**.
2. Scroll down the page and find “Download Zulu Builds of OpenJDK”.
3. For the drop-down menus *Java Version*, *Operating System*, and *Java Package*, choose **Java 8 (LTS)**, **Windows**, and **JRE**. For *Architecture*, choose according to your operating system’s architecture. The page should look similar to the example below:



4. Select *.msi* to download the execution file directly and the file will look similar to the diagram below:

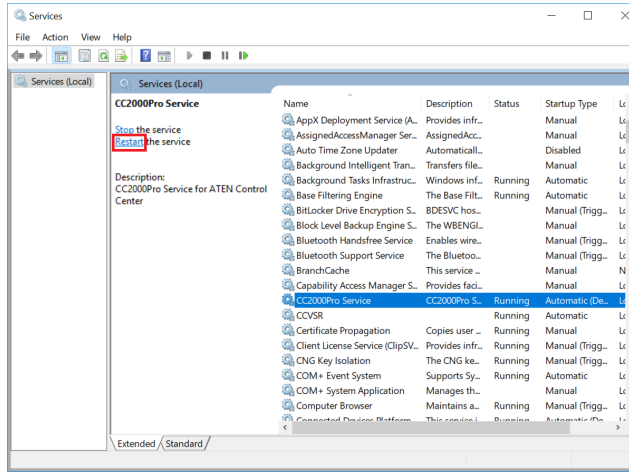
5. Execute the file and follow the on-screen instructions to complete the setup.

Downloading and Installing IcedTea-Web

The process is very similar to the OpenJDK process, except you choose “IcedTea-Web” in the “Download” extended menu instead.

Restarting CC2000

1. On your windows desktop, search for the keyword *Services* and click to start this desktop app.
2. Click to select the CC2000 service.



3. Click *Restart* to restart the service.

Linux

To remove JRE, refer to https://java.com/en/download/help/linux_uninstall.xml.

For downloading and installing OpenJDK, refer to https://openjdk.java.net/install/.

To restart your CC2000 service, refer to *Post-installation Check* on page 21.

Self-Signed Private Certificates

If you wish to create your own self-signed encryption key and certificate, a free utility – openssl.exe – is available for download over the web at **www.openssl.org**. To create your private key and certificate, do the following:

1. Go to the directory where you downloaded and extracted openssl.exe to.
2. Run openssl.exe with the following parameters:

   openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509 -keyout CA.key -out CA.cer -config openssl.cnf

Note: 1. The command should be entered all in one line (i.e. do not press [Enter] until all parameters have been keyed in).
2. If there are spaces in the input, surround the entry in quotes (e.g.,"ATEN International").

To avoid having to input information during key generation, the following additional parameters can be used: **/C /ST /L /O /OU /CN /emailAddress**.

Examples

openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509 -keyout CA.key -out CA.cer -config openssl.cnf -subj / C=yourcountry/ST=yourstateorprovince/L=yourlocationorcity/ O=yourorganiztion/OU=yourorganizationalunit/ CN=yourcommonname/emailAddress=name@yourcompany.com

openssl req -new -newkey rsa:1024 -days 3653 -nodes -x509 -keyout CA.key -out CA.cer -config openssl.cnf -subj /C=CA/ST=BC/ L=Richmond/O="ATEN International"/OU=ATEN /CN=ATEN/ emailAddress=eservice@aten.com.tw

Importing the Files

After the openssl.exe program completes, two files – CA.key (the private key) and CA.cer (the self-signed SSL certificate) – are created in the directory that you ran the program from. These are the files to be uploaded in the *Update CC2000 Server Certificate* panel (see *Import Private Key and Certificate*, page 242).

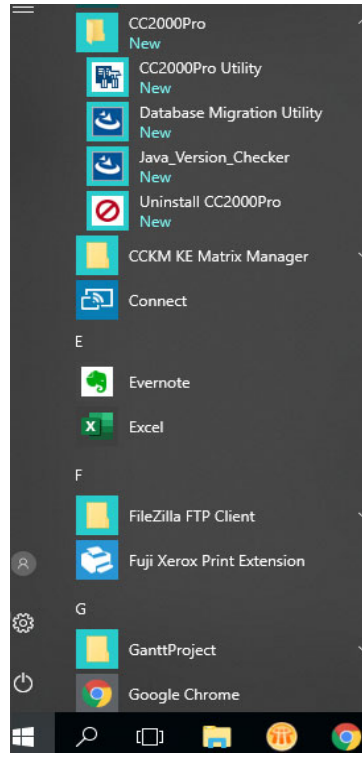
Appendix B

The CC2000 Utility

Overview

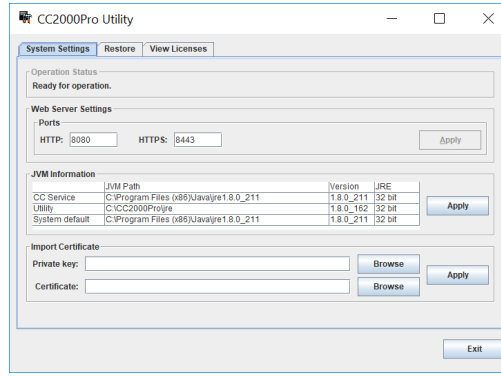
The CC2000Pro Utility is installed as a part of the CC2000 installation. It allows you to configure a number of the CC2000's parameters from the desktop of the computer that the CC2000 runs on, without having to invoke the browser GUI.

In Windows, to run the program, open the *Start* menu, navigate to the CC2000 entry (Programs → CC2000Pro), and select CC2000Pro Utility:



In Linux, as root, go to the **/opt/CC2000Pro/Runable** directory, and run the CC2000Pro_Utility file.

When you run the program, a screen, similar to the one below, appears:



The Utility offers three tabs: *System Settings*, *Restore* and *View Licenses*. Each of the tabs is described in the sections that follow.

System Settings

Apache Tomcat is the program that serves the CC2000's web pages. The CC2000's installation programs ask you to specify the ports that Apache Tomcat communicate through for web requests.

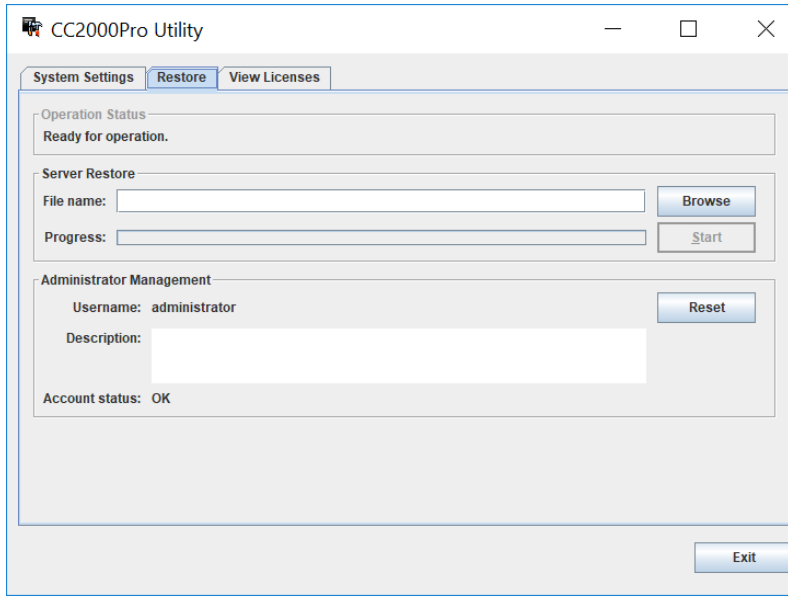
- The *HTTP* port is the regular port that Apache Tomcat communicates through. The default value is 80. If you use a different port, users must specify the port number in the URL of their browsers.
- The *HTTPS* port is the secure port that Apache Tomcat communicates through. The default value is 443. If you use a different port, users must specify the port number in the URL of their browsers.

If a port conflict occurs with the ports that you have set and prevents the web page from opening, you can use this utility to change the port settings.

After making your settings, click **Apply** to save the changes.

Restore

Clicking the Restore tab brings up a dialog box that looks similar to the one below:



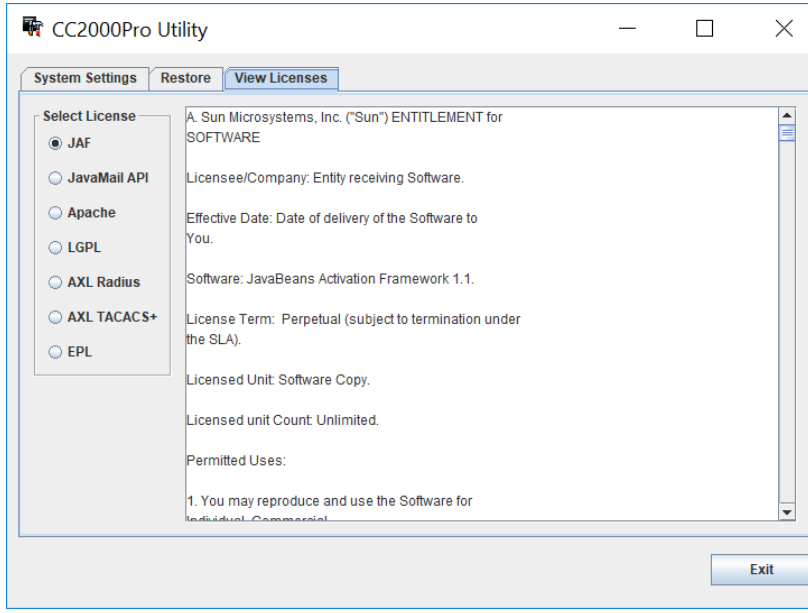
The dialog box is divided into three panels, as described in the table below:

Panel	Description
Operation Status	You can use this to check if the CC2000 service is up and running normally.
CC2000 Restore	Used to restore the CC2000's primary server database to a previously saved version (see *Backup Primary Server Database*, page 252). Click **Browse** to locate the file. After you select the file and return to the dialog box, click **Start** to begin the operation. The progress of the operation is indicated in the *Progress* field.

Panel	Description
Administrator Management	To return the System Administrator's account to the default login credentials (**administrator** / **password**), follow the steps below. 1. Insert the CC2000 USB license key to the primary server for checkup. 2. Click **Reset**. **Note:** ◆ If this account has been Locked (see *Lockout Policy*, page 274), it is automatically Unlocked. ◆ If two-factor authentication has been enabled for this account, re-initialization will be required at the next login.

View License

The View Licenses tab lets you view the licenses that are related to the CC2000 package. To view a license, click its radio button.



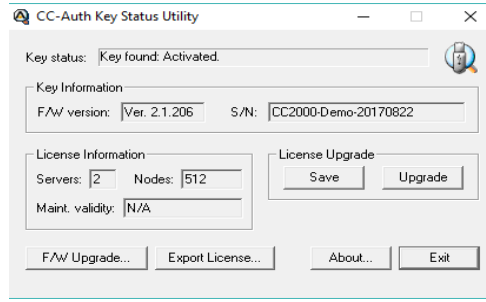
Appendix C

Authentication Key Utility

Overview

The Authentication Key Utility (*CCAuthKeyStatus.exe*), is a Windows-based utility for accessing and updating the information and data contained in the CC2000 Authentication Key. *CCAuthKeyStatus.exe* can be found on the CD that comes with the CC2000 package.

When you run the program, a screen, similar to the one below, appears:



Key Status Information

The layout of 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 servers (Primary and Secondaries), and the number of nodes the key is licensed for.
License Upgrade	These buttons are used for 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

The CC2000 Authentication Key's firmware is upgradable. As new revisions of the firmware are released, upgrade files are posted on our web site. Check the web site regularly to find the latest files and information relating to them.

Starting the Upgrade

To upgrade your firmware, do the following:

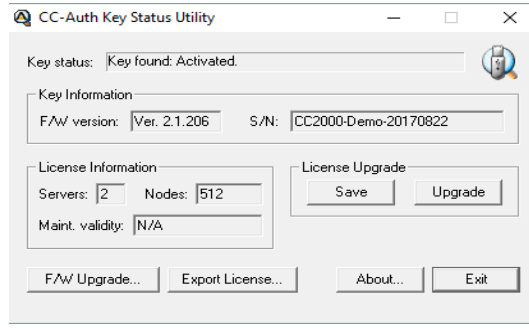
1. Go to our website and download the new firmware file onto your computer.
2. With the authentication key plugged in, run the *Key Status Utility* (CCAuthKeyStatus.exe).

Note: 1. *CCAuthKeyStatus.exe* only runs under Windows.

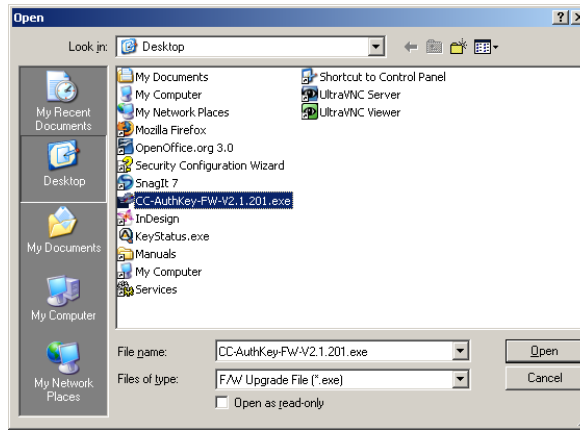
2. Firmware version 2.1.204 or higher is required for CC2000 authentication keys to support the license upgrade function.
3. *KeyStatus.exe* can be found on the CD that comes with the CC2000 package. This file should be copied to a convenient location on your computer.

---

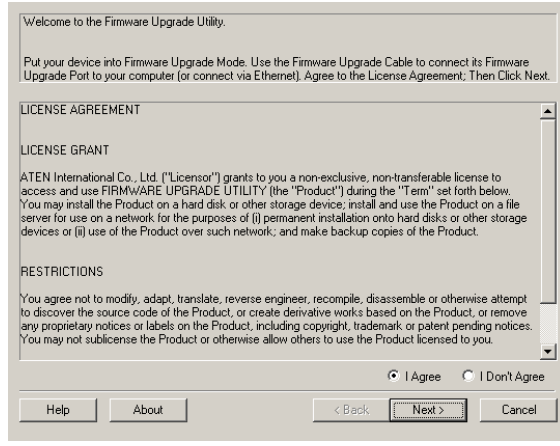
4. In the screen that appears, click **F/W Upgrade...**



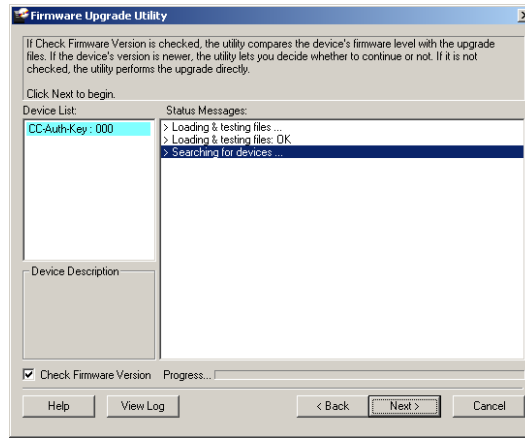
5. In the *File Open* dialog box that appears, select the firmware upgrade file, then click **Open**.



6. Read and *Agree* to the License Agreement (check the *I Agree* radio button).



7. The utility searches for your installation. When it finds your device, it lists it in the *Device List* panel.



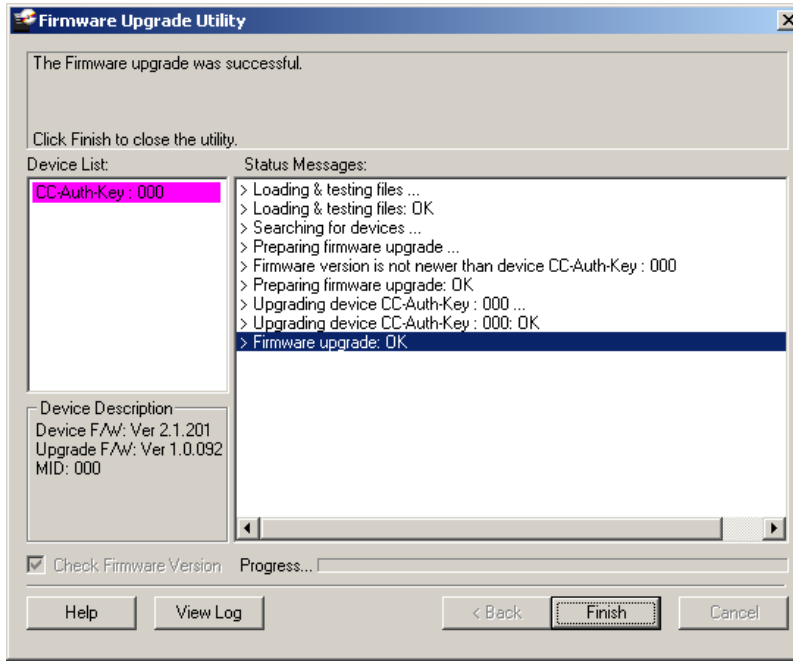
Note: If you enable *Check Firmware Version*, the Utility compares the device's firmware level with that of the upgrade files. If it finds that the device's version is higher than the upgrade version, it brings up a dialog box informing you of the situation and gives you the option to Continue or Cancel.

If you don't enable *Check Firmware Version*, the Utility installs the upgrade files without checking if there are any higher levels.

Click **Next** to continue.

Upgrade Succeeded

After the upgrade has completed, a screen appears to inform you that the procedure was successful:



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

Key License Upgrade

Overview

The CC series has a feature that allows end users (clients) to update their authentication keys to reflect an increase to their number of licenses. The key license upgrade can be performed either by the clients or by the dealers/distributors, and can take place either in a browser session over the Internet (an online upgrade), or via a standalone utility program (an offline upgrade).

Clients first inform their dealers/distributors of the number of licenses to be upgraded by. The dealers/distributors then place an order with an ATEN sales representative, specifying the number of licenses to be added. After processing the order, ATEN then sends a confirmation and authorization e-mail to the dealer/distributor with the necessary details for performing the upgrade.

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

There are two ways to upgrade the key:

- **Online:** To perform the upgrade, insert the key into the computer's USB port and open a browser session to directly upgrade the key. If the client performs the upgrade, the dealer/distributor provides him with the e-mail authorization details; if the dealer/distributor performs the upgrade, the client provides him with the Authentication Key.

- **Offline:** A Windows-based *Key Status Utility* is used to extract the key's information and saved as 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.
  - If the client is the one who updates the CC license database, the dealer/distributor provides him with the e-mail authorization details – allowing the client to generate his key license upgrade file. The client then uses the Key Status Utility and the key license upgrade file to upgrade the Authentication Key's license information.
  - If the dealer/distributor is the one who updates the CC license database, the client provides him with the key information data file (extracted with the Key Status Utility) to be used to generate the client's key license upgrade file. The dealer/distributor then returns the key license upgrade file to the client for upgrading the Authentication Key's license information using the Key Status Utility.

Online Upgrade

Clients contact their dealers/distributors to place their upgrade order(s). A separate order must be processed for each key. After the dealers/distributors place the upgrade orders with an ATEN sales representative, they receive a confirmation and authorization e-mail, similar to the example below:

Your order is ready to be processed. Please go to http://xxx.xxx.x.xxx to upgrade your key's license.

Login Information:

- Username: myname2
- Password: mypassword5678

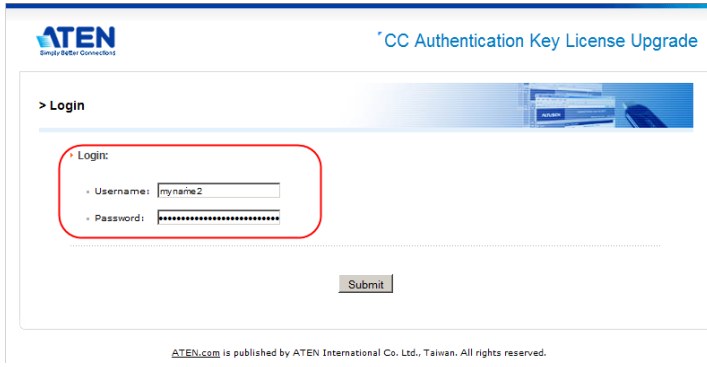
Order Information:

- Order ID: 1017000700 (authorized number: 2068919892). This order requests CCMA512 (1YR SUP FOR 512 NODES)

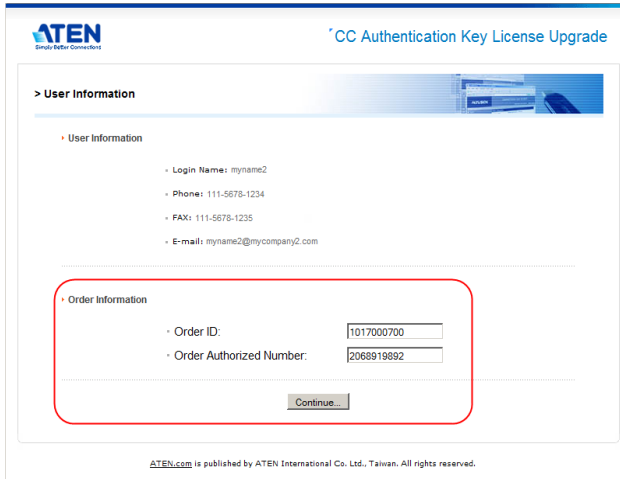
Either the client or the dealers/distributors can perform the upgrade. If the dealer does it, the client provides the dealer with his license key; if the client does it, the dealer forwards the confirmation e-mail to him.

Follow the steps below to perform an online upgrade.

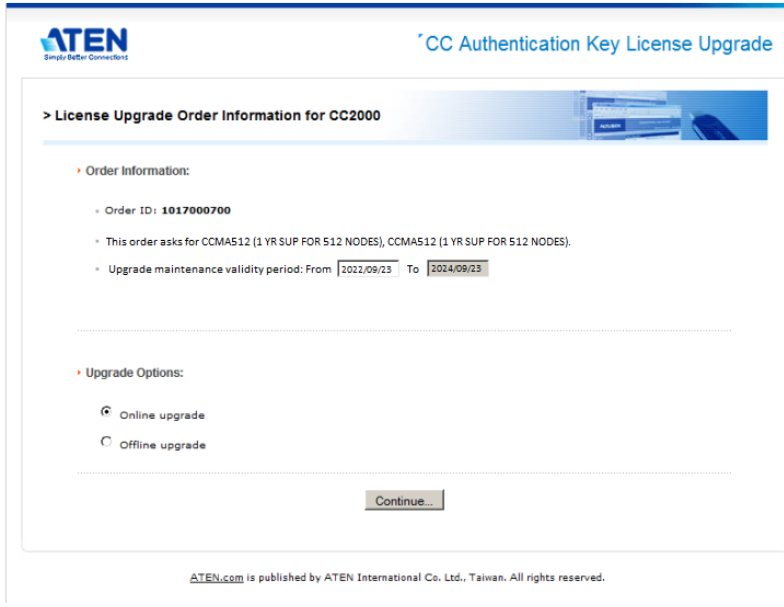
1. Plug the authentication key into a USB port on your computer.
2. Open a browser, go to the CC Authentication Key License Upgrade page: https://cc.aten.com:10443/
3. When the upgrade Login screen comes up, log in with the Username and Password provided in the authorization e-mail.



4. In the screen that comes up, key in the Order ID number and Order Authorization number that applies to the upgrade, then click **Continue**.



5. In the License Upgrade Order Information screen, key in the current number of licenses in the From fields (the To fields are automatically filled in), and select **Online upgrade**.

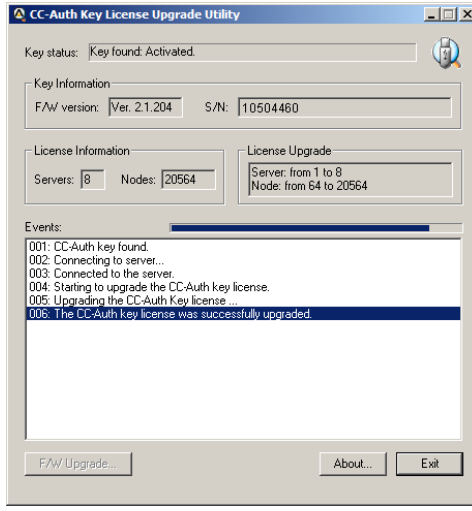


Note: You can use the Key Status Utility (CCAuthKeyStatus.exe) to see the current number of licenses.

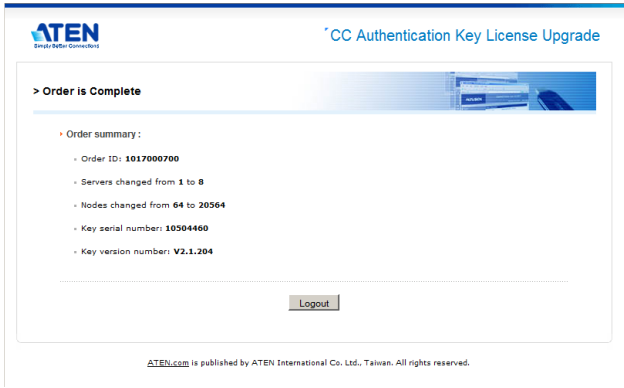
6. Click **Continue**.
7. When the CC Authentication Key License Upgrade by Distributor screen comes up, click **Download**.
8. When the browser asks what to do with the file (KeyUpgrade.exe), select *Save to disk*.
9. Leave the browser open as is; go to where you downloaded the file and execute it.

Note: This step must be done in the same web session that you downloaded the KeyUpgrade.exe file in. Otherwise the upgrade will not succeed.

The upgrade utility comes up and starts the upgrade. The actions it performs are reported in the main panel:

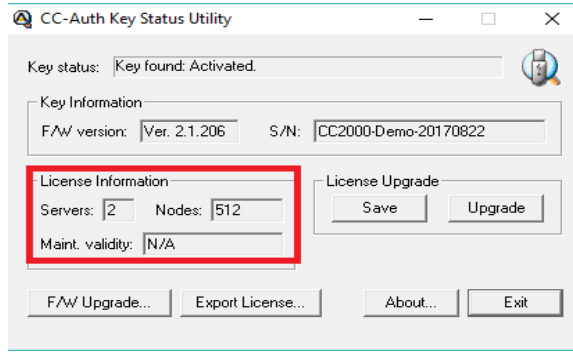


10. When the upgrade is finished, a window pops up to inform you that the upgrade was successful. Click **OK** to close the popup.The browser screen provides a summary of the upgrade:



11. Click **Logout** to exit.

You can use the Key Status Utility (CCAuthKeyStatus.exe) to double-check that the number of licenses on the key has been successfully upgraded:



Upgrade Succeeded

After the upgrade has succeeded, the dealer/distributor receives an e-mail from ATEN informing him that the upgrade has been completed online. For example:

> Your order (Order ID: 1017000700) has been completed successfully by the online utility.
> The key (PSN: 10504460) server number has been upgraded from 1 to 8, and node number from 64 to 20564.

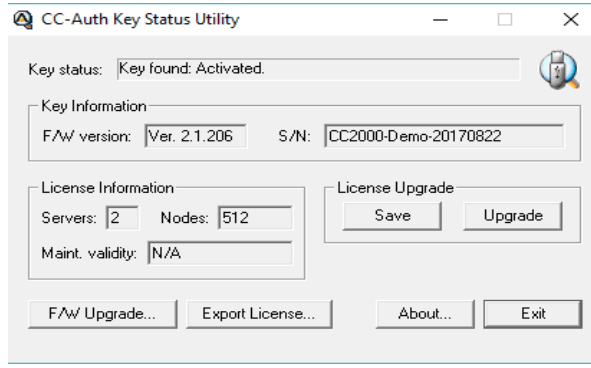
Offline Upgrade

An Offline upgrade can be performed either by the dealer/distributor, or the end user client. The advantage of this type of upgrade is that the client doesn't give up the use of his key. All he needs to do is e-mail the key information data file to the dealer/distributor and receive a key upgrade file in return.

Preliminary Steps

To perform the upgrade, the first step that the client must perform is to create a *Key Information Data File*, as follows:

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



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

After the Key Information Data File is created, the client sends it to the dealer/distributor.

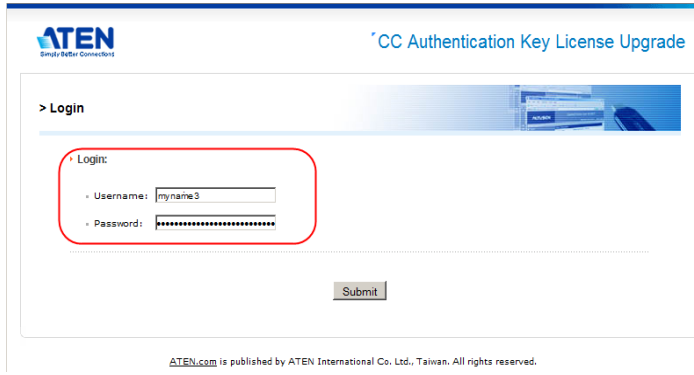
Performing the Upgrade

After the dealers/distributors place the upgrade orders with an ATEN sales representative, they receive a confirmation and authorization e-mail from ALTUSEN, for example:

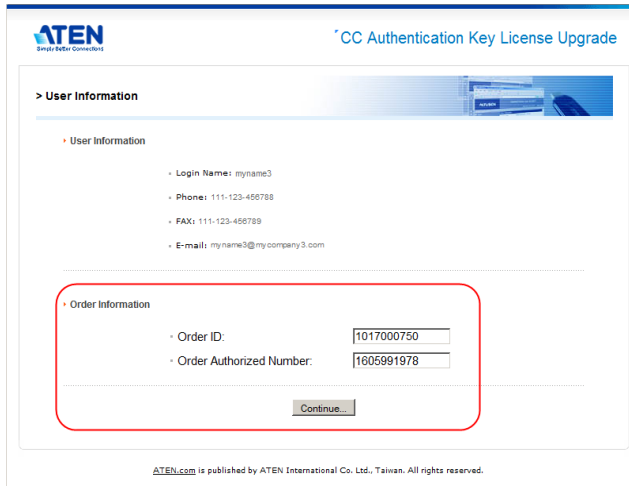
> Your order is ready to be processed. Please go to http://xxx.xxx.x.xxx to upgrade your key's license.
>
> Login Information:
>
> - Username: myname3
> - Password: mypassword3
>
> Order Information:
>
> - Order ID: 1017000750 (authorized number: 1605991978). This order requests 1 more server(s) and 448 more node(s)

To perform the upgrade, do the following:

1. Follow steps 1 – 3 given in Online Upgrade (see page 383).
2. When the upgrade Login screen comes up, log in with the Username and Password provided in the authorization e-mail.



3. In the screen that comes up, key in the Order ID number and Order Authorization number that applies to the upgrade, then click **Continue**.

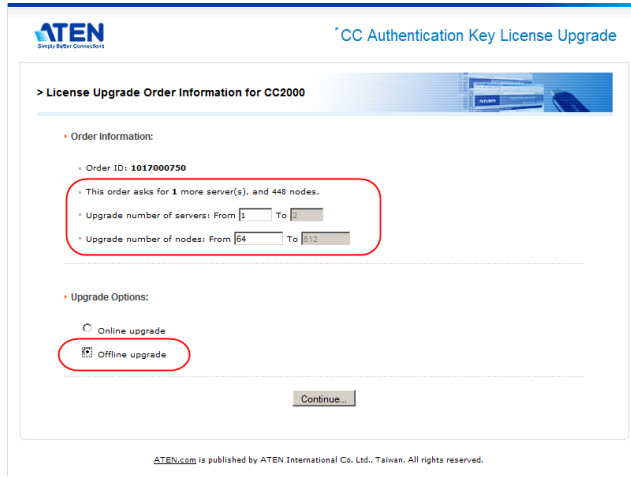


4. When the License Upgrade Order Information screen comes up, key in the number of current licenses in the *From* fields. The *To* fields are automatically filled in.

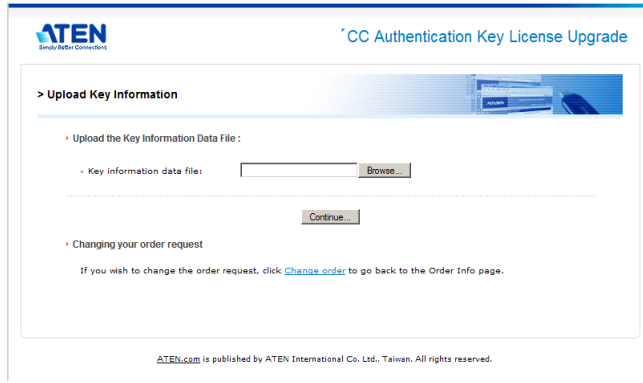
Note: If necessary, you can use the Key Status Utility (CCAuthKeyStatus.exe) to see the number of current licenses.

---

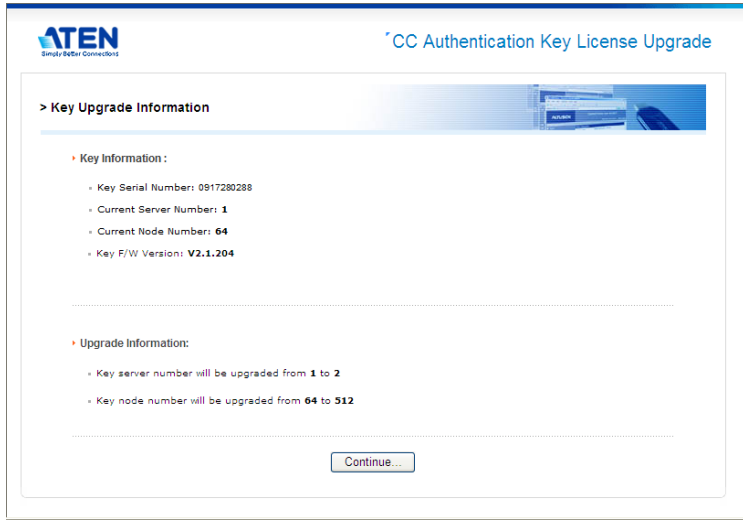
5. Select that this is an Offline upgrade, then click **Continue**.



6. When the Upload Key Information screen comes up, click **Browse**; load the **KeyUpload.dat** file that was generated in the *Preliminary Steps* section; then click **Continue**.

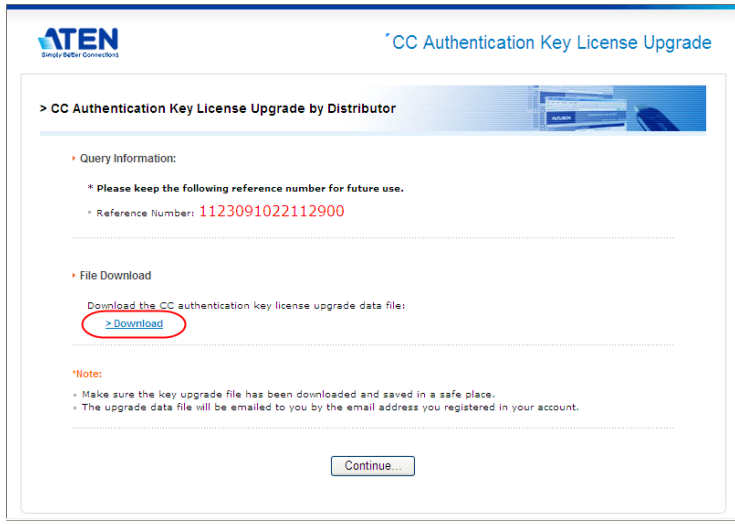


7. The next screen that comes up summarizes the transaction up to this point.



Click **Continue** to move on.

8. In the screen that appears next, click **Download** to download the key license upgrade data file (KeyUpgrade.dat).



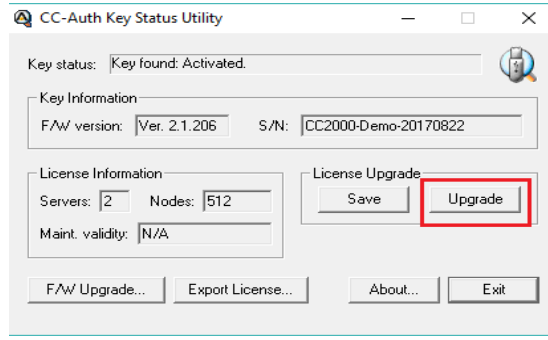
9. When the browser asks what to do with the key upgrade file, select *Save to disk*. After the file is saved to disk, click **Continue** to go on.
10. In the confirmation popup that appears, click **Yes**. A summary page confirming the order appears.
11. Click **Logout** to exit.

Note: 1. If you are upgrading more than one key, you can rename the KeyUpgrade.dat files to separately recognizable names (keeping the *dat* extension).

2. If the client is performing the upgrade, the dealer/distributor provides the KeyUpgrade.dat file to the client.

12. Run the *Key Status Utility* again.

13. In the License Upgrade panel, click **Upgrade**.



14. In the dialog box that comes up, navigate to the upgrade file (KeyUpgrade.dat) and select it.
    - Once you click **Open**, a window pops up stating that the upgrade was successful.
    - The figure for the number of licenses in the License Information panel changes to reflect the upgrade.

Offline Upgrade Failure

If the offline upgrade fails, it may be due to the key upgrade file (KeyUpgrade.dat) having become corrupted during the file transfer process. There are two ways to resolve this:

- When the key upgrade file is downloaded, an e-mail is sent to the dealer/distributor containing the particulars, along with a copy of the upgrade file in case there was a problem with the original file transfer – as shown in the example, below:

```
Offline upgrade email response:

Your CC-Authentication key's upgrade data file is
attached. Please upgrade your CC-Auth key with the
attached file.

Key Info:

* F/W Version: 2.1.204

* Serial number: 0917280288

License Upgrade Info:

* From 1 to 2 concurrent servers

* From 64 to 512 concurrent nodes

Confirmation Info:

* Username: newname

* Password: 1123091022112900

If you have any problem with upgrading your CC-
Authentication key's license, please confirm it online
at http://xxx.xxx.x.xxx using the username and
password above.
```

  You can repeat steps 11 (Run the Key Status Utility) and 12 (Click Upgrade) – this time using the copy of the key upgrade file (KeyUpgrade.dat) that was attached in the dealer/distributor e-mail.

- If the above fails to resolve the problem, information contained in the *Offline email upgrade response* can be used to try an online upgrade. Either the dealer/distributor can provide the end user with the authorization details, or the end user can give his key to the dealer/distributor.

Order Expiration

Once ATEN sends the dealer/distributor the confirmation/authorization e-mail informing him that the order is ready to be processed, he has a total of two weeks to process the order. If the order is not processed within that time period, two more e-mails reminding him that order has not been processed are sent:

1. Your order will expire in one week...
2. Your order will expire in one day...

If, the order still has not been processed by the end of the deadline, a final e-mail is sent, informing the dealer/distributor that the order has expired, as follows:

Your order has expired and has been canceled...
If you still wish to add licenses, you must place a new order.

Appendix D

External Authentication Services

Overview

In addition to the built-in *Username / Password* authentication procedure, the CC2000 supports authentication from external, third party authentication services. If a third party service has been used to specify a user, the CC2000 receives the login information for authentication using an encrypted HTTPS (SSL) connection. This section provides suggestions on configuring third-party authentication services.

The following services have been tested and approved for use with CC2000. Refer to the corresponding section in this appendix for setup suggestions.

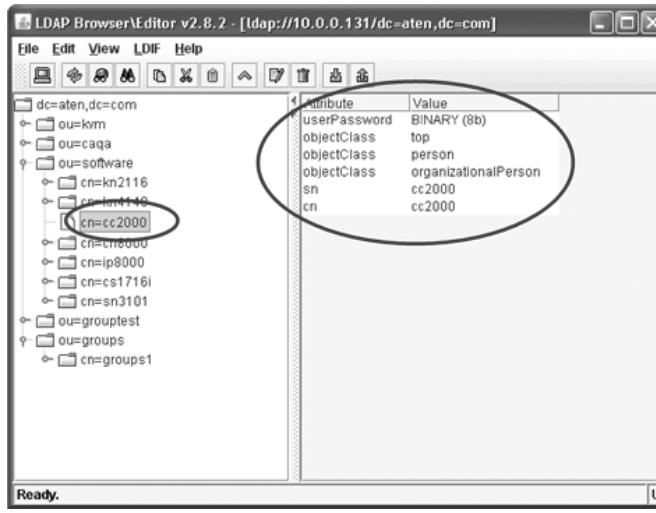
- LDAP: Microsoft Windows Server 2003; OpenLDAP
- AD Server: Microsoft Windows Server 2003
- RADIUS: Microsoft IAS for Windows Server 2003; FreeRADIUS
- TACACS+: Microsoft Windows Server 2003 (ClearBox)
- Microsoft Windows NT Domain
- MOTP: Mobile One-Time Password
- Microsoft Entra ID

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 *cc2000ldap.ldif* in the OpenLDAP directory containing the following information:

```
dn: cn=cc2000,ou=software,dc=aten,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: cc2000
sn: cc2000
userPassword: password
```

The LDAP administrator can check the LDAP definition with LDAP Browser. He should see a screen that looks like the one below:



The CC2000 Administrator gets this information to be used in the *Adding an External Authentication Server* procedure (see *LDAP*, page 195). In this example, the fields would be filled in as follows:

IP: 192.168.10.100

Port: 389

BaseDN: dc=aten,dc=com

UserRDN: ou=software

Key attribute: cn

Object class: person

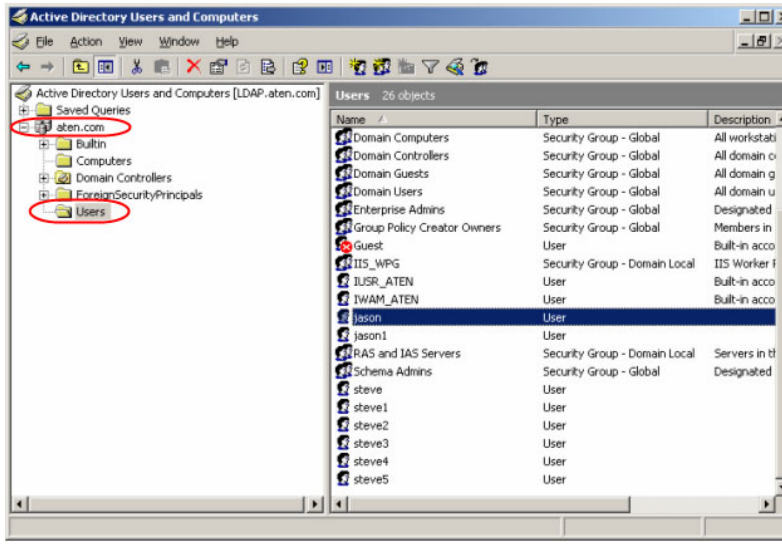
Full name attribute: sn

After the LDAP/LDAPS Authentication server has been added, the CC2000 Administrator can use the Browse button to browse for all user names in the *software* directory.

Active Directory Settings Example

In this example, the external server used is Active Directory on a 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 (aten.com in our example) → Users. A window, similar to the one below, appears:



The CC2000 Administrator gets this information to be used in the *Adding an External Authentication Server* procedure (see *Active Directory*, page 194). In this example, the fields would be filled in as follows:

IP: 192.168.10.100

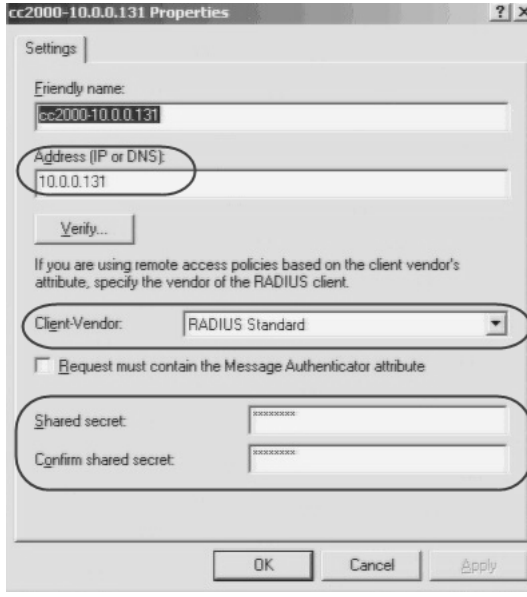
UserRDN: cn=users

After the Active Directory Authentication server has been added, the CC2000 Administrator can use the Browse button to browse for all the user names in the *Users* directory.

RADIUS Settings Example

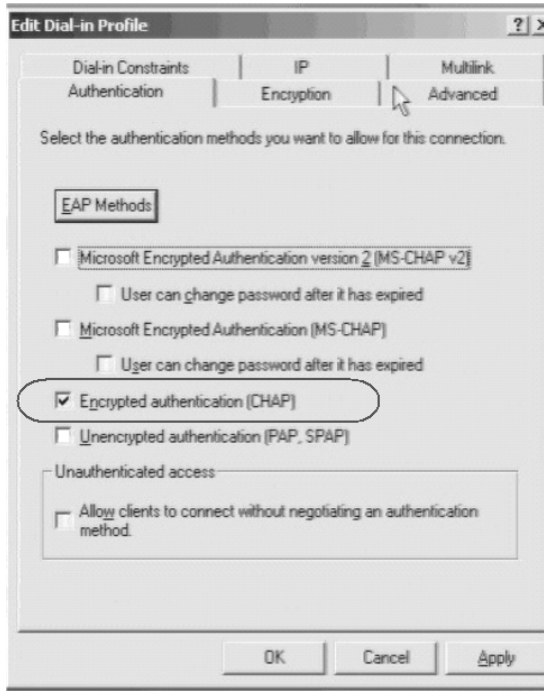
In this example, the external server used is RADIUS: Microsoft IAS for Windows Server 2003; its IP address is 10.0.0.100. Configure RADIUS as follows:

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 comes up, key in the *Friendly name*. For example: cc2000-10.0.0.131, then click **Next**. A screen, similar to the one below, appears:



5. In this example, the CC2000'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**; select *Properties.*

7. In the screen that comes up, click the **Edit Profile** button, then select the **Authorization** tab. A screen similar to the one below appears:



8. In this example, we use CHAP for encrypted authorization

The CC2000 Administrator gets this information to be used in the *Adding an External Authentication Server* procedure (see *MOTP (Mobile One-Time Password)**, page 197). In this example, the fields would be filled in as follows:

IP: 10.0.0.100

Authentication type: CHAP

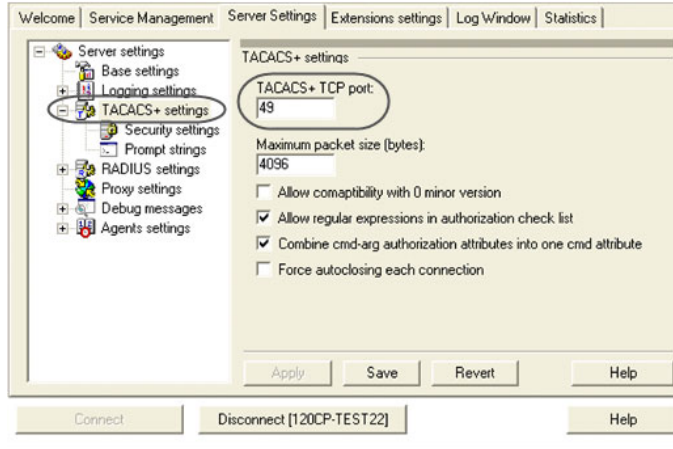
Shared secret: password

After the RADIUS Authentication server has been added, when the CC2000 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 as its Login names.

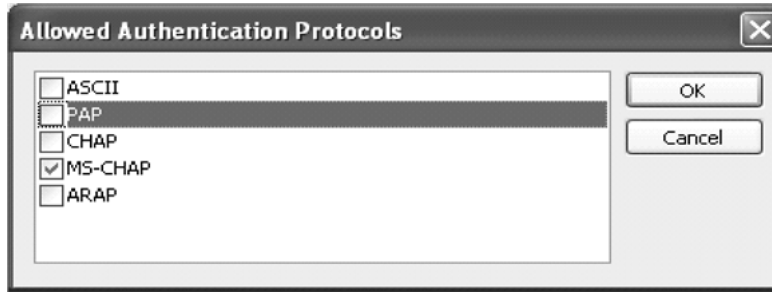
TACACS+ Settings Example

In this example, the external server used 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. Key in the password that you set when you installed the ClearBox RADIUS TACACS+ Server.
4. In the *ClearBox Server Configurator* screen that comes up, select the **Server Settings** tab. A screen, similar to the one below, appears:



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 comes up in the left panel, select Realms → def; then select the **Authentication** tab.
8. Click the **Allowed Protocols...** button. A screen similar to the one below appears:



9. In this example, we use MS-CHAP for the allowed authentication protocol.
10. Back on the *ClearBox Server Configurator* screen, select Data Sources → users in the left panel.
11. In the main panel of the screen that comes up, there is an MS Access entry field with a path locating the *general.mdb* file. The accounts contained in this file are generated through MS Access.

The CC2000 Administrator gets this information to be used in the *Adding an External Authentication Server* procedure (see *MOTP (Mobile One-Time Password)**, page 197). 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 CC2000 Administrator adds user accounts, he must use the names that were configured in the TACACS+ server's *general.mdb* file.

NT Domain Settings Example

In this example, the external server used 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. A screen, similar to the one below, appears:

The CC2000 Administrator gets this information to be used in the *Adding an External Authentication Server* procedure (see *Windows NT Domain*, page 200). In this example, the fields would be filled in as follows:

Server IP: QA_NT_SERVER

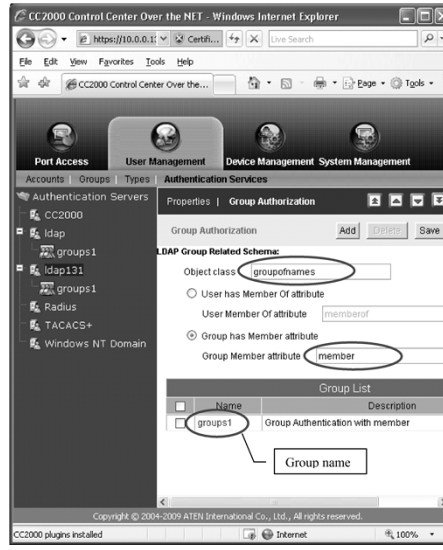
After the NT Domain server has been added, when the CC2000 Administrator adds user accounts, he must use the names that were configured under *User Manager for Domains*.

LDAP Group Authorization Setting Examples

Example 1

In this example, the external server used is OpenLDAP on Windows Server 2003, as shown in the LDAP/LDAPS Settings Example on page 395.

1. Under the CC2000 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, the **groups1** group is added. The screen should look similar to the one below:



The OpenLDAP administrator uses this name (*groups1* in our example) to create a group under OpenLDAP with the same name as the one just created on the CC2000 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 *cc2000ldap.ldif* file to add a definition for groups1 and have cc2000 user accounts fall under groups1, as follows:

   dn: cn=***groups1***,ou=groups,dc=aten,dc=com

   objectclass: ***groupofnames***

   member: cn=***cc2000***,ou=software,dc=aten,dc=com

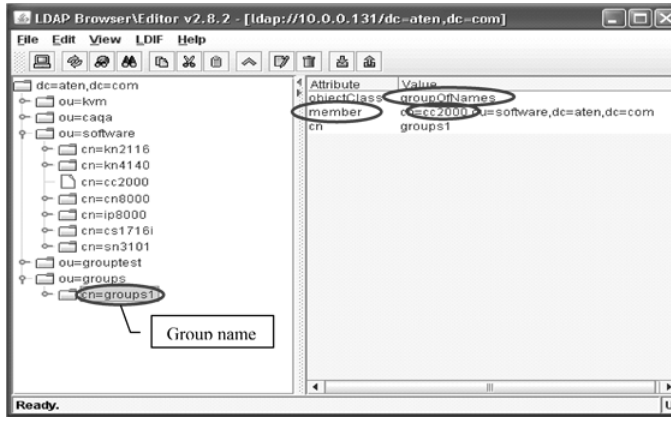
   cn: ***groups1***

Note:

- The entry after dn: cn= should be the name of an actual group created under Group Authorization on the CC2000 server.
- The entry after objectclass: should be consistent with the name that was entered for the Object class when the group was created on the CC2000 server. Change the default entry in this file to match.
- The entry after *member: cn=* should be an actual user login name.

---

3. You can check the group definition with LDAP Browser. You should see a screen similar to the one below:



4. The above example has added a member – cc2000 – to the groups1 group. To add additional members to the group, edit the file to include them. For example:

   member: cn=***cc2000-1***,ou=software,dc=aten,dc=com

   member: cn=***cc2000-2***,ou=software,dc=aten,dc=com

Once these procedures are completed, CC2000 users who are authenticated through the LDAP/LDAPS server, are authorized according to the permissions assigned to the group.

Example 2

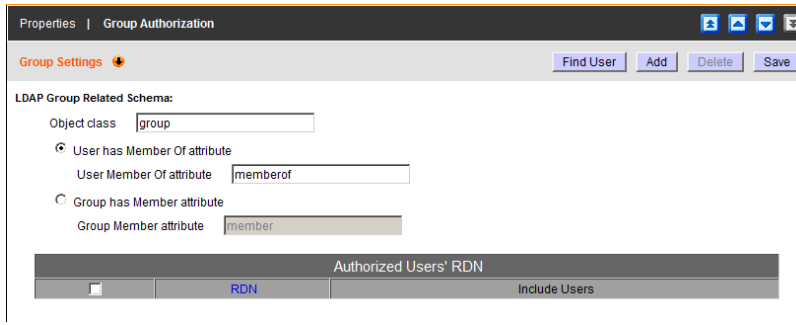
By default, OpenLDAP only supports the *Group has Member attribute* setting for the group related schema – this was the setting used in Example 1.

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 Settings Example on page 395.

1. Under the CC2000 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, the **groups1** group is added. The screen should look similar to the one below:



The OpenLDAP administrator uses this name (*groups1* in our example) to create a group under OpenLDAP with the same name as the one just created on the CC2000 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 *cc2000ldap.ldif* file to add a user account to the *groups1* group, as follows:

   dn: cn=***cc2000test***,ou=software,dc=aten,dc=com

   objectclass: top

   objectclass: ***person***

   objectclass: organizationalPerson

   cn: cc2000test

sn: cc2000test

memberof: cn=***groups1***,ou=groups,dc=aten,dc=com

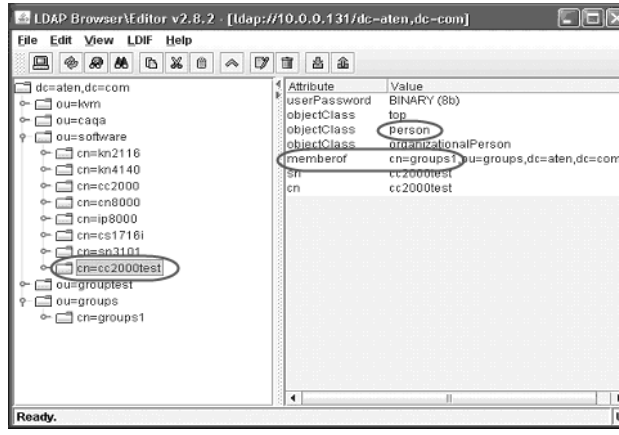
userPassword: password

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 on the CC2000 server.

3. You can check the group definition with LDAP Browser. You should see a screen similar to the one below:



4. Repeat step 2 for each user account that you want to add to the group.

Once these procedures are completed, CC2000 users are authenticated through the LDAP/LDAPS server, and authorized according to the permissions assigned to the group.

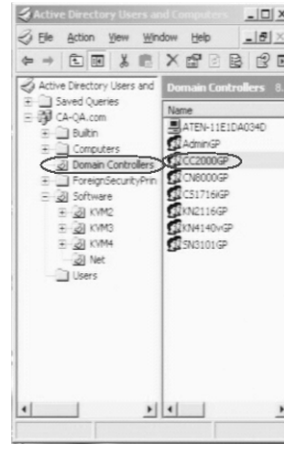
Active Directory Group Authorization Setting Example

In this example, the external server used is Active Directory on Windows Server 2003, as shown in the Active Directory Settings Example on page 397.

1. Under the CC2000 User Manager tab, select Authentication Services → Authentication Servers.
2. Select the Active Directory server; then click **Group Authorization**.
3. In this example, the **CC2000GP** group is added.

The Active Directory administrator uses this name (CC2000GP in our example) to create a group under Active Directory with the same name as the one just created on the CC2000 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 that comes up, key in the name of the group (CC2000GP in our example). A window, similar to the one below, appears:



4. In the right panel, right click **CC2000GP**; select **Properties**; select **Members**. A window, similar to the one below, appears:

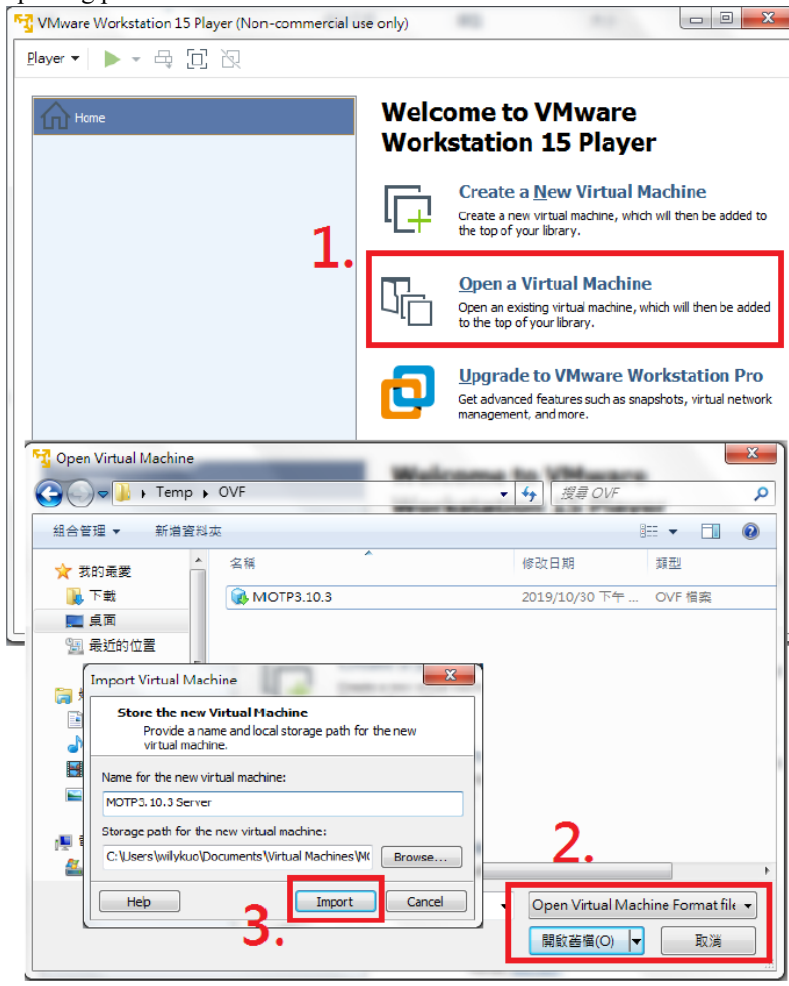
5. Click **Add**.

The dialog that comes up 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).

MOTP Settings

MOTP VM Server Setup

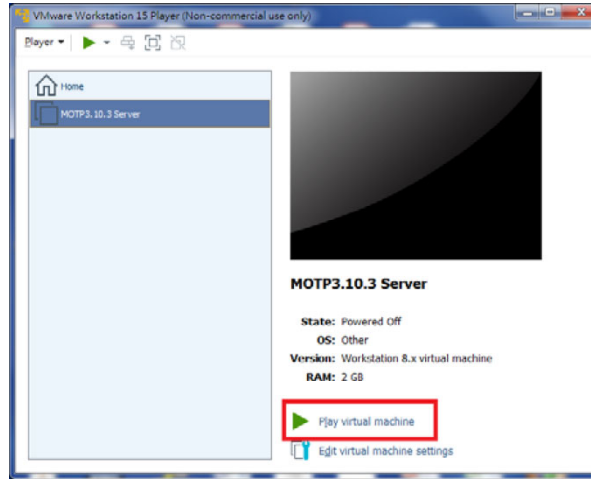
By using VMware Workstation or VMware Player, click “Open a Virtual Machine” to open the ovf/ova file in the MOTP server to start the system importing process.



Setup using system built-in “opuser”

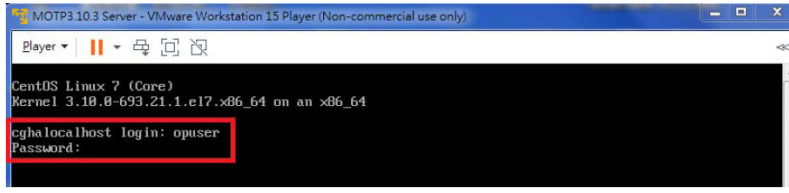
“opuser” is a built-in administrator account in the system. During initial installation, you can use “opuser” to set up the IP address and connect to the MOTP VM system through a web browser.

Setup IP Address



Open MOTP VM. The welcome page will show a login hint.

Enter the account name (”opuser”) and password (“op123pass”) to login.



1. Find the IP of the MOTP server with dynamic IP:

By default, the MOTP server obtains an IP automatically through a DHCP server. To find the obtained IP, enter *ifconfig*.

2. Set the MOTP server IP with Static IP

   Confirm in advance:

   - The address we will be using (e.g. 192.168.1.200) is available for the first VM network card.
   - The computer the admin is using for this setup is also capable of connecting to this IP address.

   Assuming we are setting MOTP welcome page of the first network card IP address to 192.168.1.200:

   1. Enter

   ```
   sudo /sbin/ifconfig ens0 192.168.1.200 netmask
   255.255.255.0
   ```

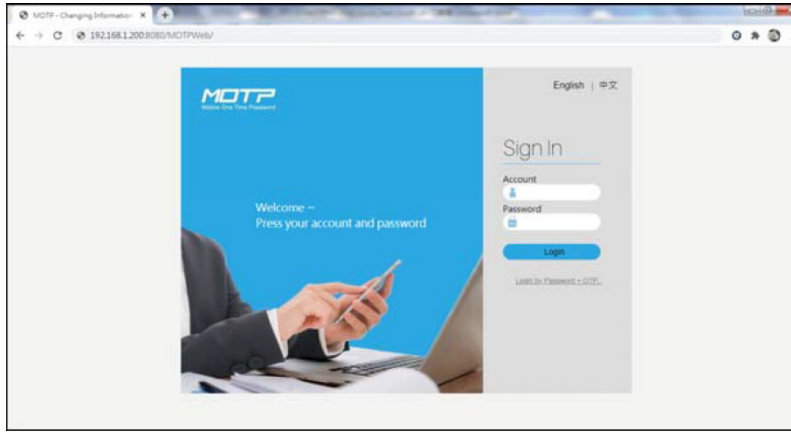
   2. Enter the password of the opuser (“op123pass”)

> You can check the network card name by using the *ifconfig* command.

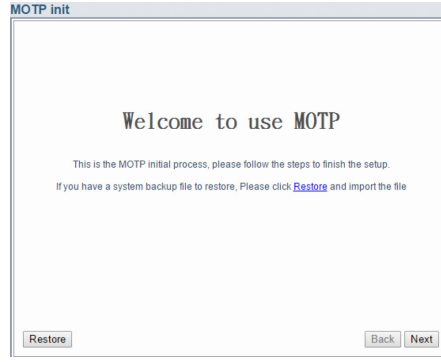
MOTP Server Initialization

After setting the IP address, open the IP address in a browser in the format below for MOTP server initialization:

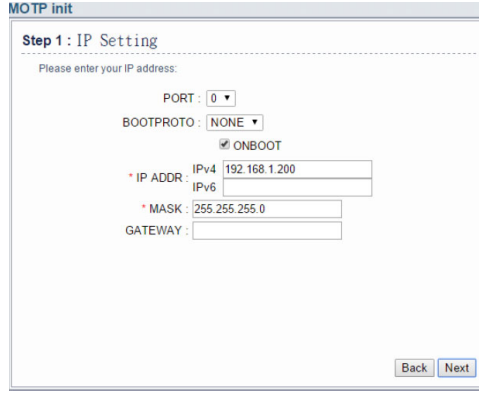
```
http://192.168.1.200:8080/MOTPWeb
```



Enter the account name (admin) and password (admin).



Step 1: IP Setting



Configure the information below:

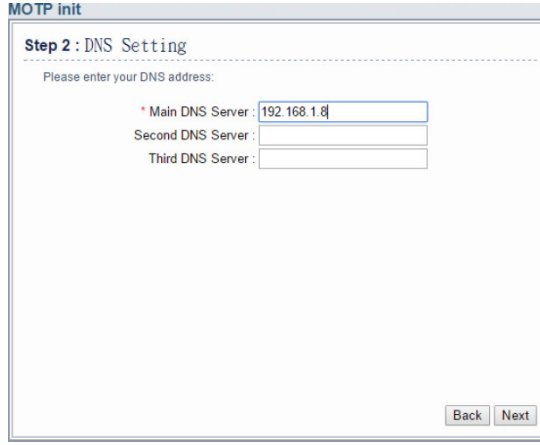
Bootproto: NONE

IPV4: 192.168.1.200

Mask: 255.255.255.0

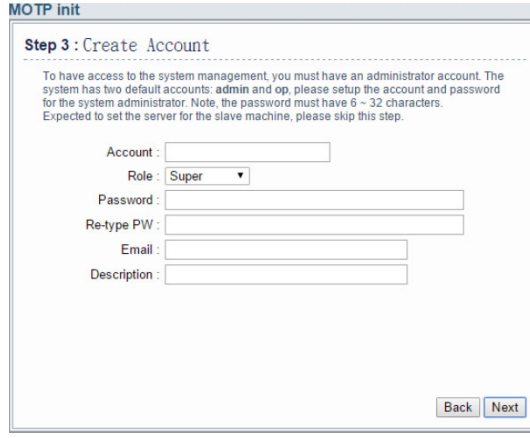
The fields with a red asterisk are must-filled fields.

Step 2: DNS Setting



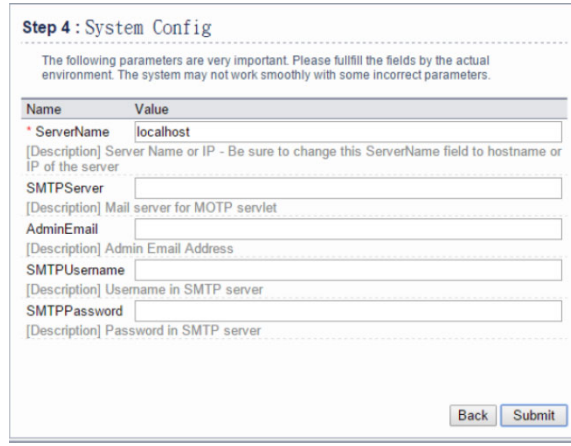
Configure your main DNS server IP.

Step 3: Create Account



Note: You can skip this step and come back later.

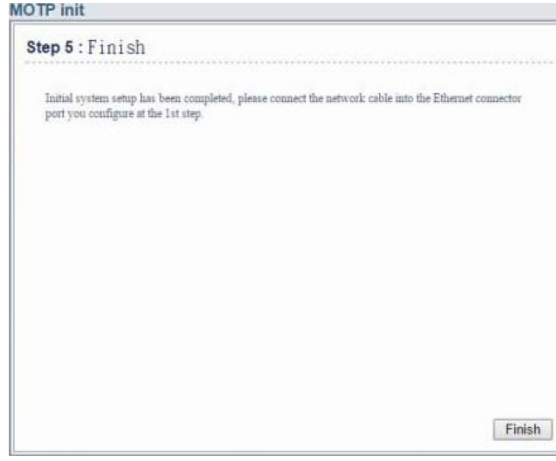
Step 4: System Config



Note: You can skip this step and come back later.

Step 5: Finish

The initialization is complete.



MOTP Server Setting

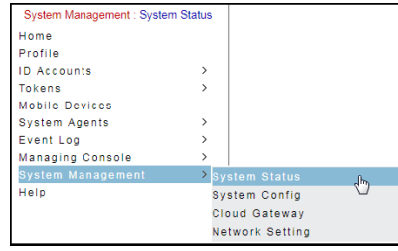
Go to the MOTP server (e.g. http://192.168.1.200:8080/MOTPWeb) and log in with the account name “admin” and password “admin”.

The Management page of the server appears, as exemplified below:

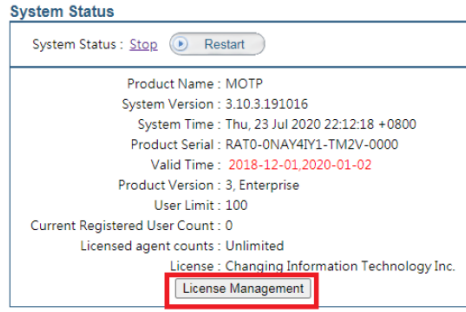
Import License

To activate the MOTP server service, you will need to purchase a license (*.pem) and tokens (*.csv) from CHANGING Information Technology Inc. (https://www.changingtec.com/EN/). When you have the details of the License and Tokens, import them by following the steps below:

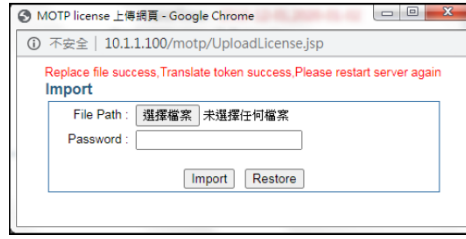
1. Go to [System Management] → [System Status]:



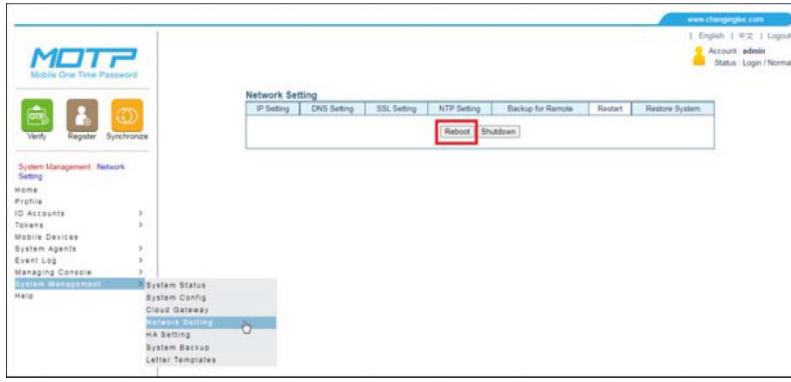
2. In System Status, click “License Management” to start importing the purchased license.



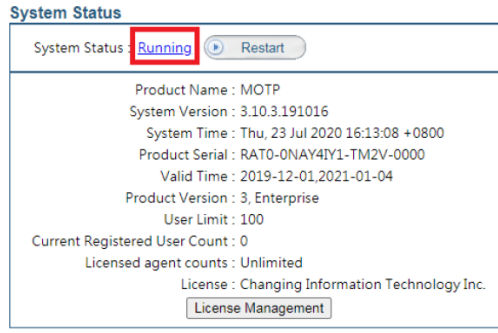
3. Click “Browse” to select the license file (*.pem), then enter the password given by CHANGING and click “Import” to update the license.



4. Go to [System Management] → [Network Setting] → [Restart] and click “Reboot” to restart the MOTP server.



5. After the restart, log in and check System Status to make sure that the license is valid and the service is running.



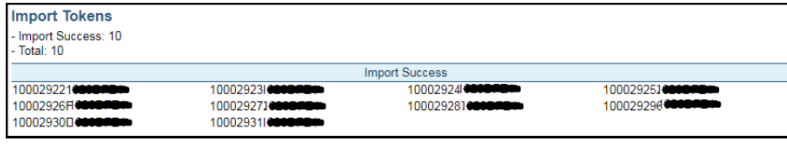
Import Tokens

A token license (*.csv/ *.dat) allows a MOTP client to receive a one-time pass code every time you want to sign in to an application server. To import token license, follow the steps below:

1. Go to [Tokens] → [Import Tokens]

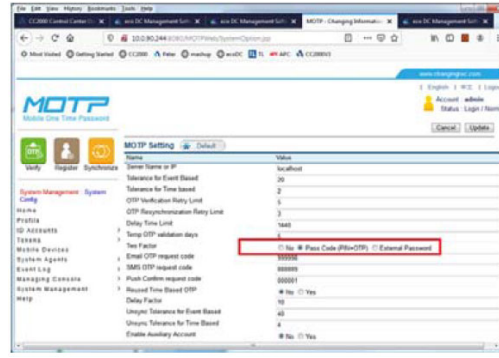
2. Click “Browse” to select the token license and click “Submit” to import.

3. You will see a list of imported tokens after the import.

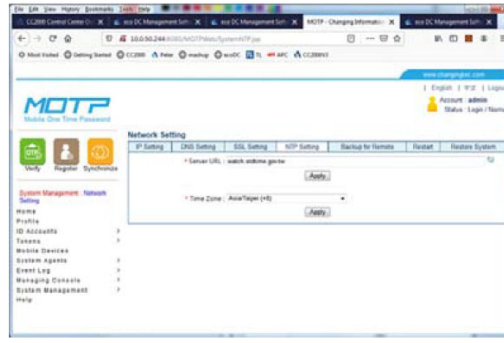


Note:

- After the MOTP VM server setup, make sure the MOTP server setting for “Two Factor” is set to “Pass Code (PIN+OTP)” (“No” is selected by default). Go to [System Management] → [System Config]. An example is shown below:

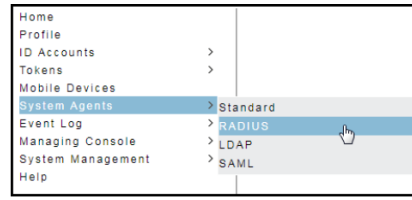


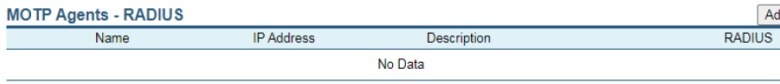
- For verification purposes, a MOTP server needs to be synchronized to an NTP server. Go to [System Management] → [Network Setting] → [NTP Setting] to configure the NTP settings, as shown below:



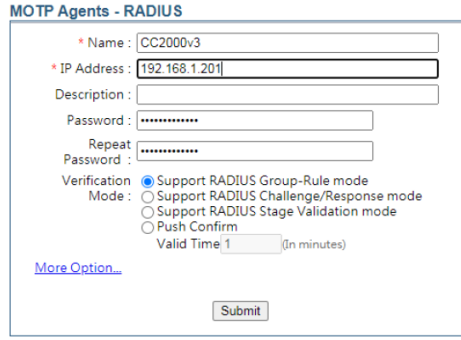
RADIUS Setup

1. Go to [System Agents] → [RADIUS]:



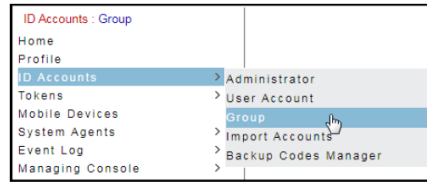


2. Click “Add” to create a CC2000 server entry.
3. Enter the information of the CC2000 server (MOTP agent) and set up a password for CC2000 to access the MOTP server. Make sure that the password is the same as the shared secret in CC2000.

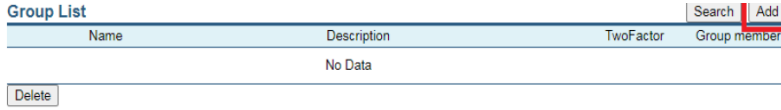


Create Trust Group

1. Go to [ID Accounts] → [Group]:



2. Click “Add” on the top right corner to create a group.

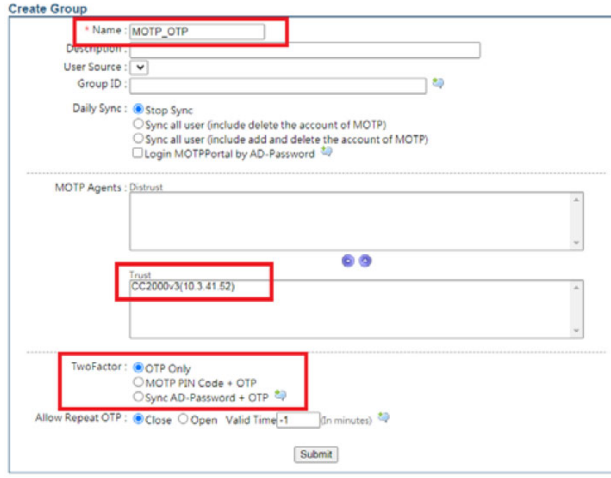


3. Fill in the group name. In MOTP Agents, move CC2000 from Distrust to Trust. In TwoFactor, select “OTP Only” (only username and OTP will be used for CC2000 login).

   “MOTP PIN Code + OTP” means username, OTP, and a PIN (default = 000000) are needed when logging in to CC2000.

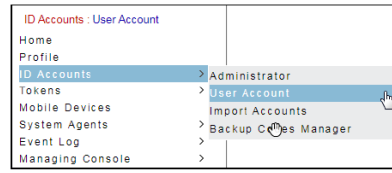
Note: To change the PIN, go to the MOTP’s user portal (e.g. http://192.168.1.200/MOTPPortal) and change it in Profile category.

“Sync AD-Password + OTP” means AD username, OTP, and AD password are needed when logging in to CC2000.

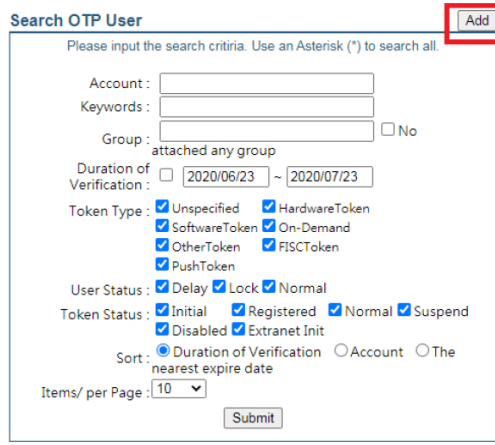


Create Account Manually

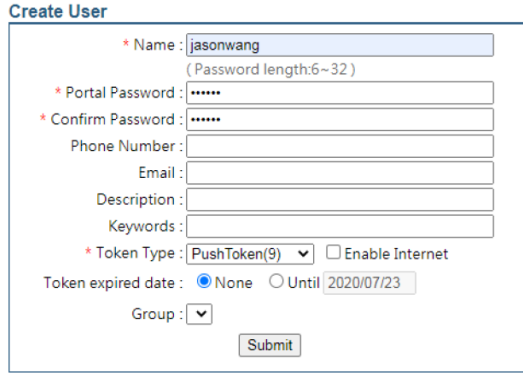
1. Go to [ID Accounts] → [User Account]:



2. Click “Add” on the top right corner to create a user account.



3. Create an account by entering the information of each field (for signing into the MOTP Client Portal later) and select the token type that you have previously imported.

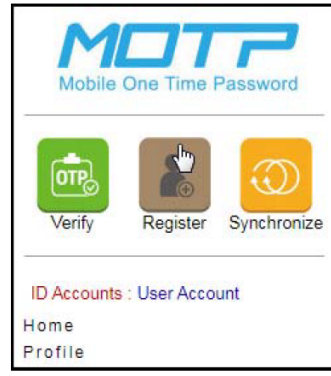


You will see the following information after registering successfully.

Register Software Token

1. Search for “MOTP Client” in your mobile device’s application store, download it and open the application.

2. Click “Register” on the MOTP management page (on the computer).

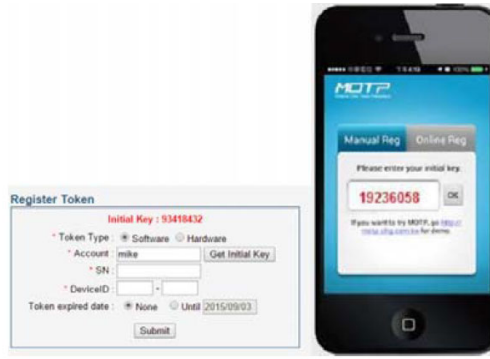


3. Registering Token:

   Choose software token as Token Type.

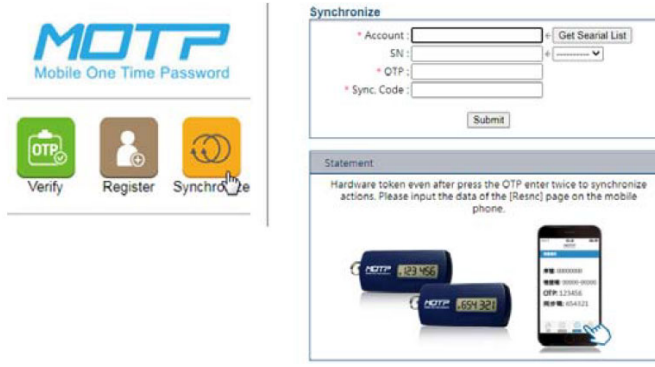
   Enter the user account for the Account and click “Get Initial Key” to display the initial key generated (center top).

   On the mobile device, open the MOTP Client mobile app, and enter the initial key in the available field.



4. A serial number (SN) and Device ID are generated on the MOTP Client mobile app. Enter them into the MOTP server and click “Submit” to finish the registration.

5. You need to be OTP-verified and then synchronized after registering. Click “Synchronize” on the left of the MOTP management page.



6. On the server page, enter the user account you have created and click “Get Serial List”. The SN field will be filled in automatically.
7. Enter the OTP and Sync Code fields obtained from the MOTP Client to synchronize.

   You will receive a message upon successful synchronization.

8. If you have already been OTP-verified and synchronized previously, click “Verify” on the MOTP management page.

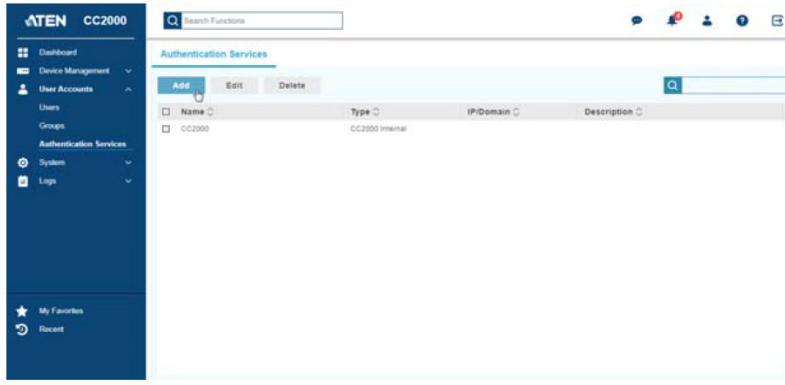
MOTP Authentication Services on CC2000

The content below is an example of how to set up MOTP authentication services on CC2000, thereby creating a user that is MOTP-authenticated, as well as an example of how that user logs into CC2000 using MOTP authentication.

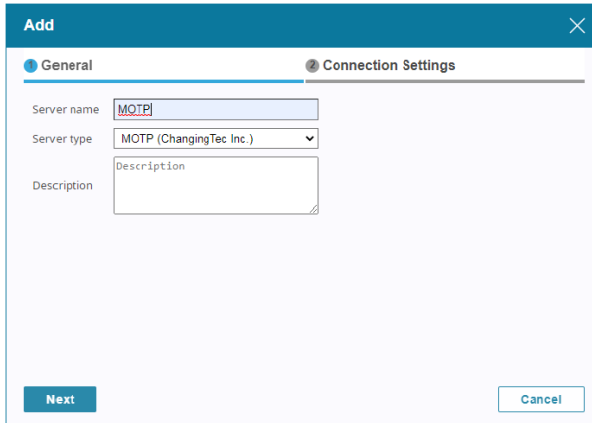
Setting up MOTP Authentication Service

Make sure you are logged into CC2000 as an administrator.

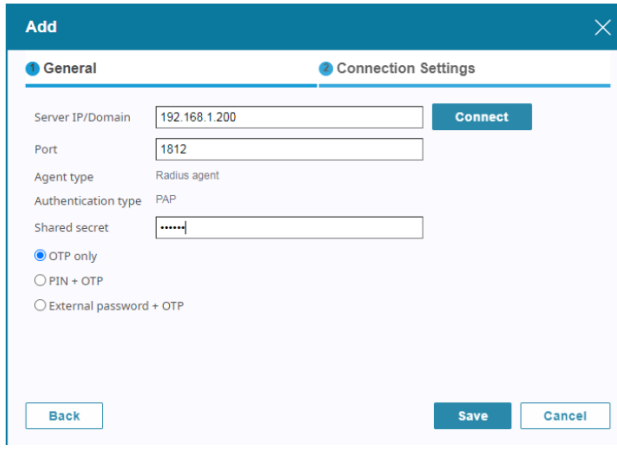
1. On the Sidebar Menu, go to **User Accounts** → **Authentication Services**.



2. Click **Add** for the following dialog box.



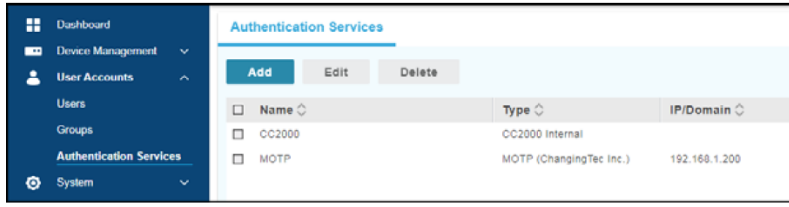
3. Enter the Server name and select “MOTP (ChangingTec Inc)” for Server type and click **Next**.
4. Enter the IP address of the MOTP server and the shared secret you entered in the RADIUS agents of the MOTP server.



Note: If “Dual Authentication” in server type is selected, CC2000 will ask you for both a login credential and an OTP authentication.

Use the **Connect** button after the “Server IP/Domain” field to test the connection before saving.

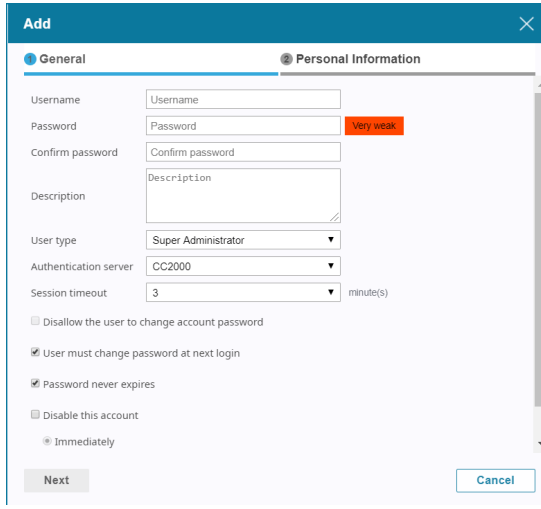
5. Click **Save** to save the authentication service and it will be listed in the service list, as exemplified below:



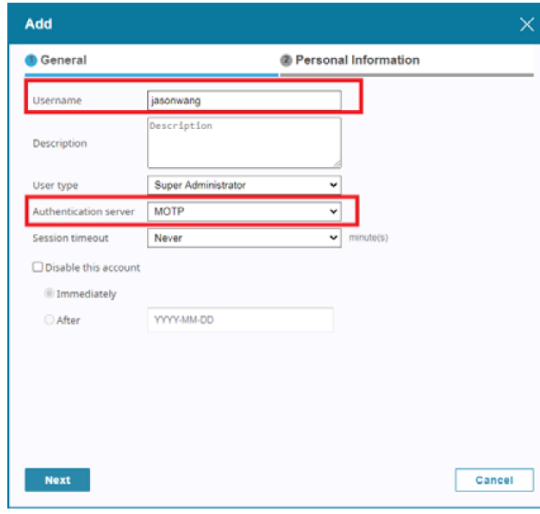
Creating User Account(s) for MOTP Authentication Service

Make sure you are logged into CC2000 as an administrator.

1. Go to **User Accounts** → **Users** and click **Add**.



2. Select MOTP as the authentication server, as shown below. Enter the same username as the one you created in the MOTP server (e.g. jasonwang). Click **Next** to continue.

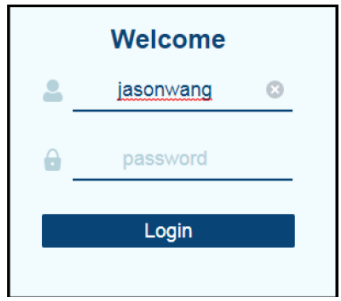


3. Enter the available fields in the Personal Information tab and click **Save**. For more details about the Personal information tab, refer to *Adding a User Account*, page 173.

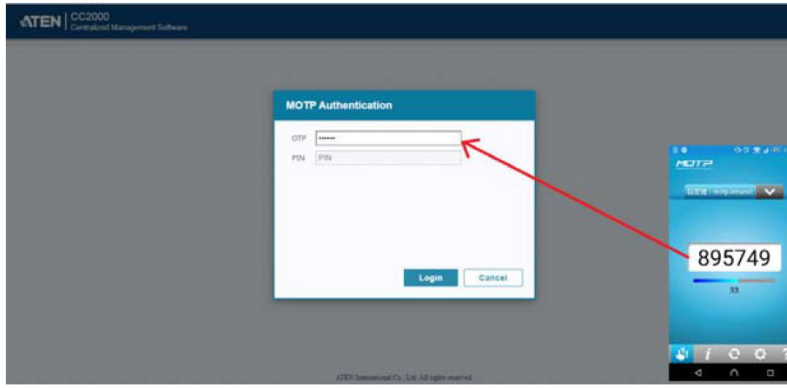
4. The user will be listed in the user list.

Logging into CC2000

1. Go to the CC2000 login page and enter the username of the MOTP-authenticated user (e.g. jasonwang) and click **Login**.



2. A MOTP Authentication window appears. Fill in the OTP generated from the mobile app (on your mobile device) MOTP client to log into CC2000.

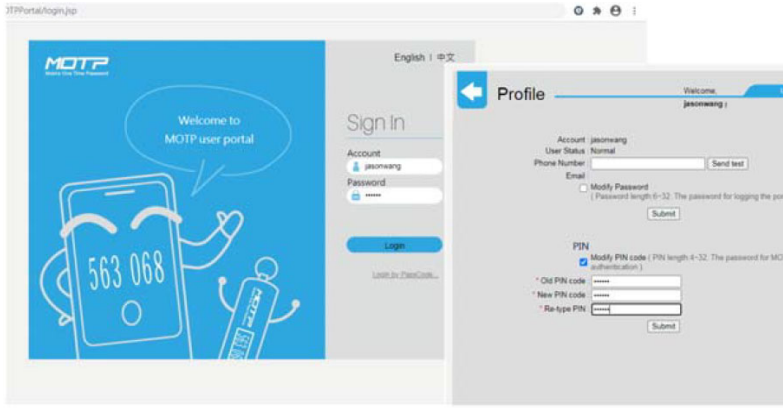


Note: 1. OTP changes every 60 seconds.

2. If “Dual Authentication” in server type is selected, CC2000 will ask you for both a login credential and an OTP authentication.

If TwoFactor configuration in MOTP server is OTP + PIN, enter OTP and the PIN (default: 000000) to log into CC2000.

To change the PIN, log into the user portal of the MOTP server (e.g. http://192.168.1.200/MOTPPortal) and change it in Profile category.



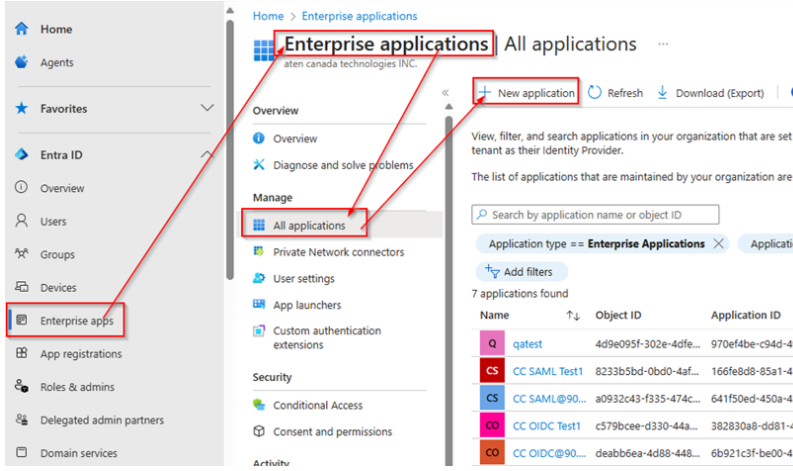
Single Sign-On

This section covers the suggested configuration of Microsoft Entra ID for setting up single sign-on (SSO). For full information of SSO setup, see *Single Sign-On Using Microsoft Entra ID*, page 202.

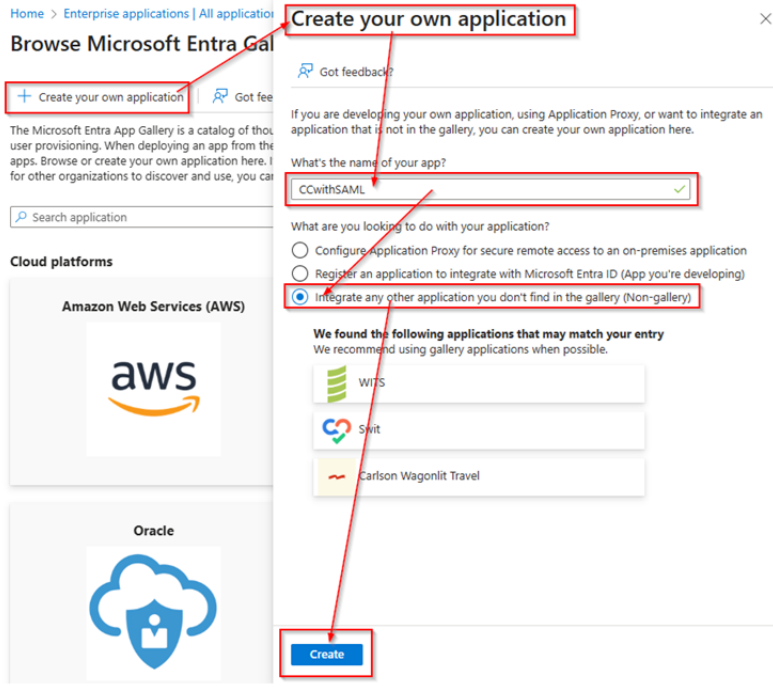
Note: The user interface of Microsoft Entra admin center may be updated at any time. Please consult the Microsoft Entra online help for detailed or current practice.

Registering Applications in Microsoft Entra ID

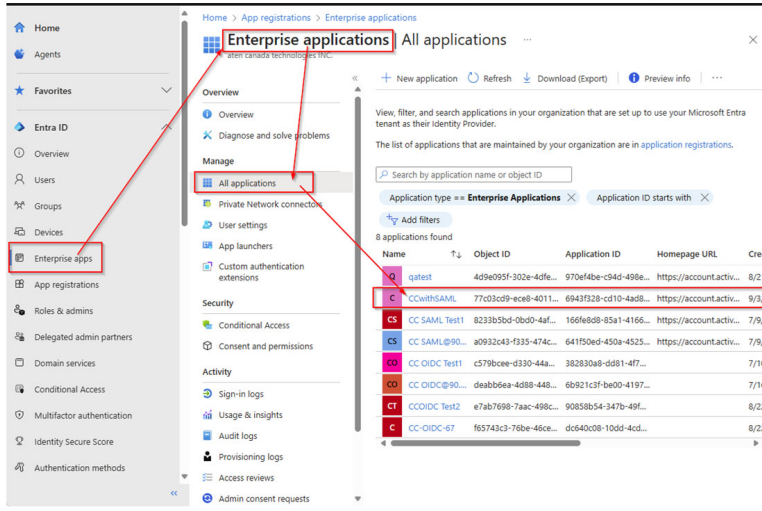
1. In Microsoft Entra admin center, add the target application.
2. Go to **Enterprise apps** > **All applications**, and click **New application**.



3. Click **Create your own application**, select **CCwithSAML** for the app name, select **Integrate any other application you don't find in the gallery (Non-gallery)**, and click **Create**.

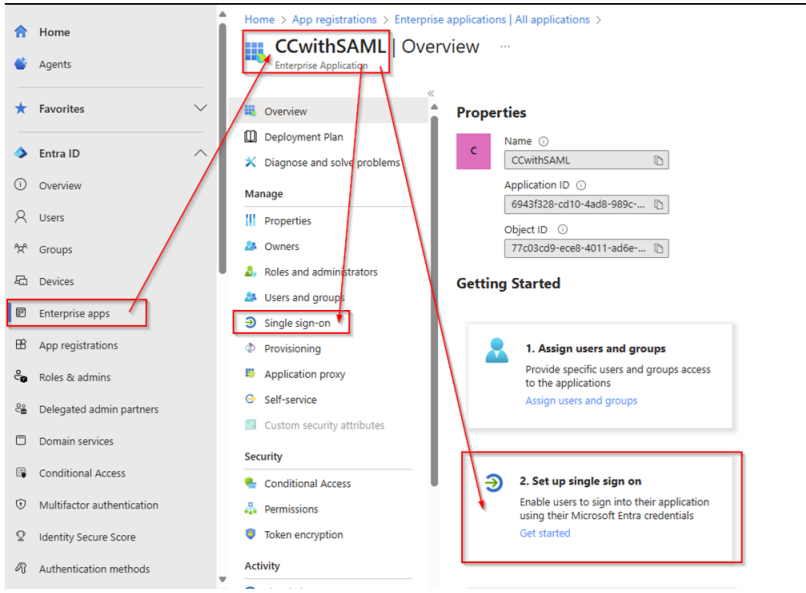


The application is added to the list of enterprise apps.

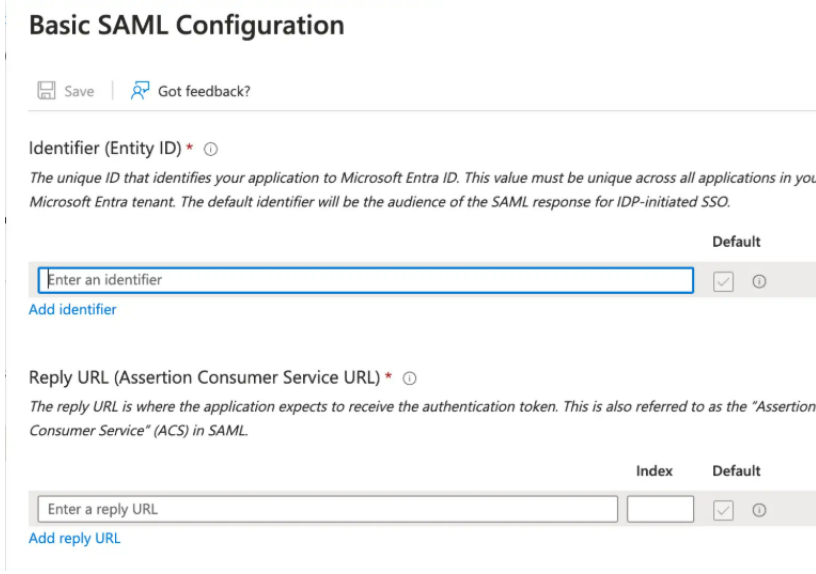


4. Configure the authentication type.

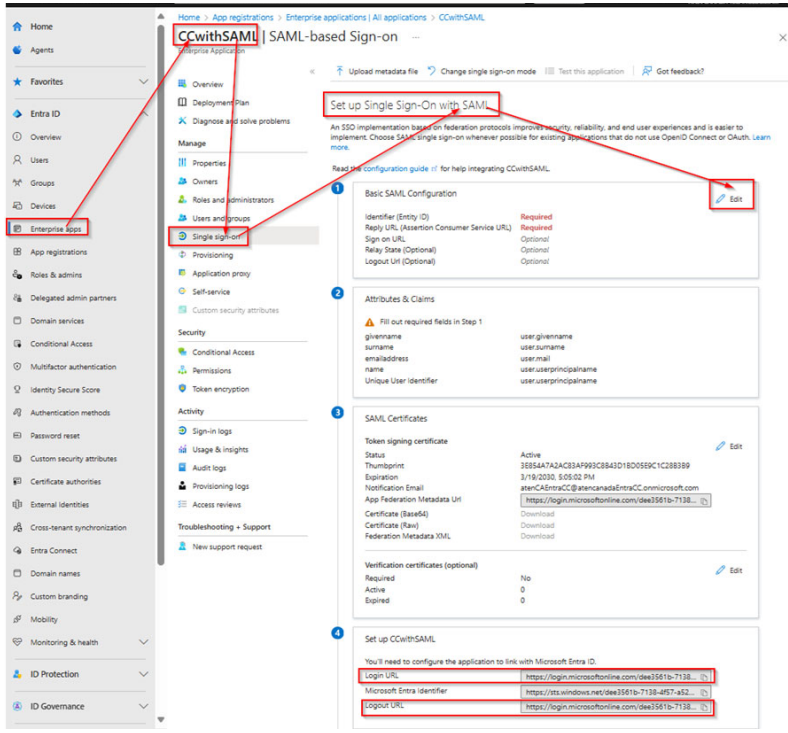
   a) Go to **Enterprise apps > Single sign-on > 2. Set up single sign on**.



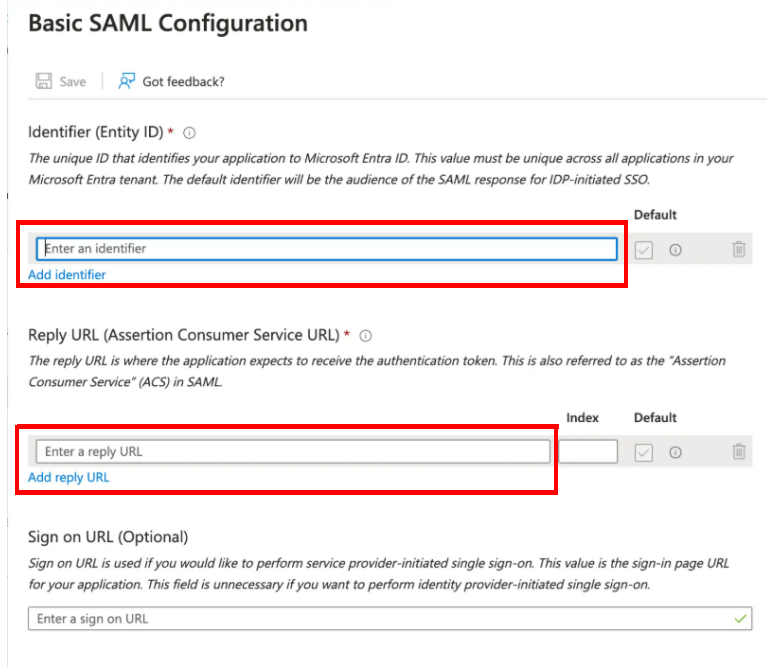
   b) Select **SAML**.



c) Save the Login URL and Logout URL to a notepad for later CC2000 configuration, and then click **Edit** to configure SAML.



d) In the Basic SAML Configuration window, make sure to add configure the following settings.

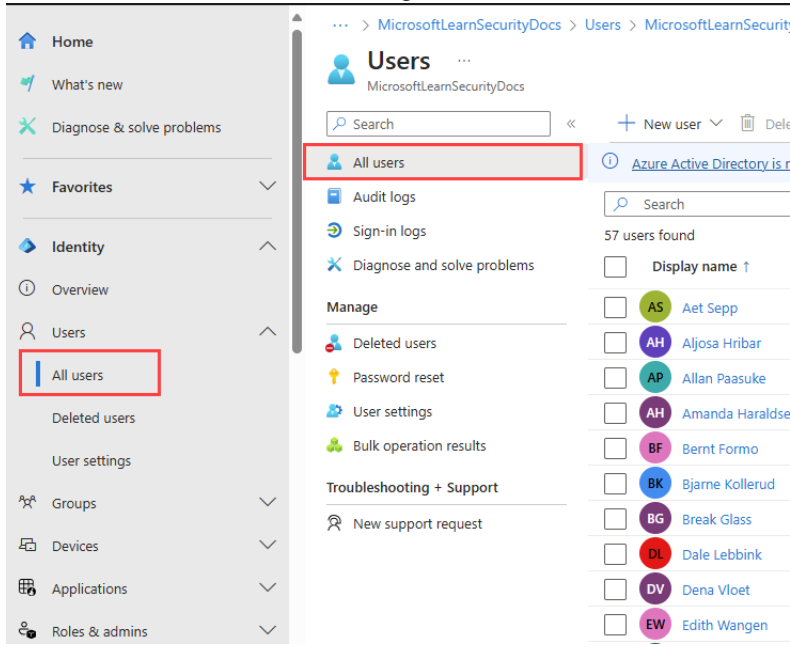


- **Entity ID:** This is a unique identifier of the added application. Make sure that CC2000 uses the same entity ID to specify this application.
- **Reply URL:** This is the predefined address where the IdP redirects users after authentication. Use the IP address and port designated for the CC2000 intranet access to set up the reply URL.

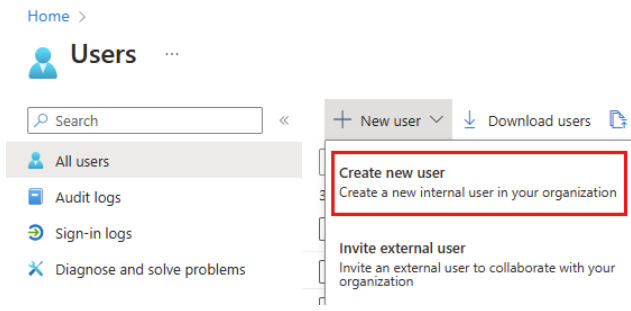
e) Save the entity ID and reply URL to a notepad for later CC2000 configuration.

Creating Users on Microsoft Entra ID

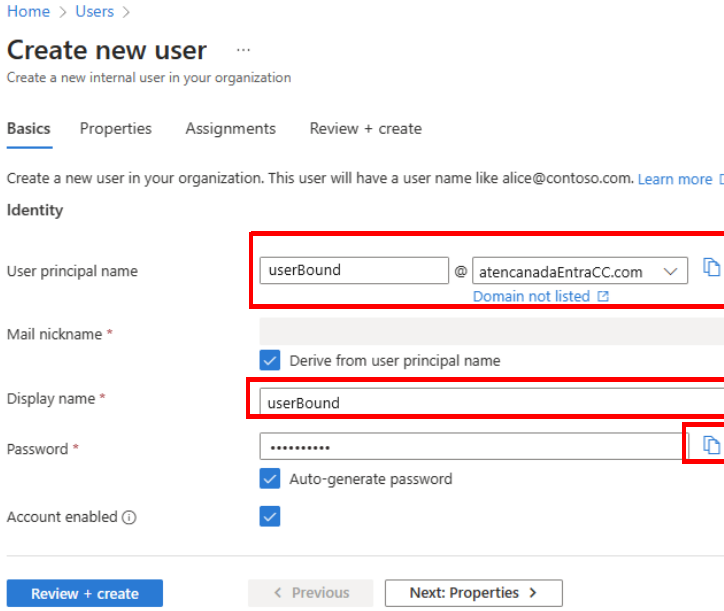
1. In Microsoft Entra ID admin center, go to **Users** > **Add users**.



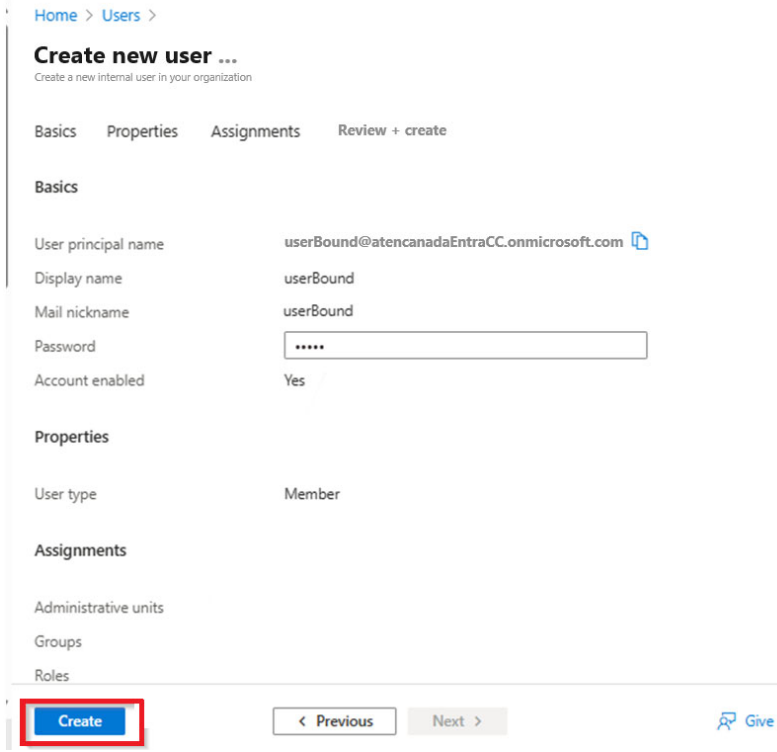
2. Click **+New user** and select **Create new user** from the drop-down menu.



3. Enter the user principal name, display name, copy the randomly generated password, and then click **Review + create**.

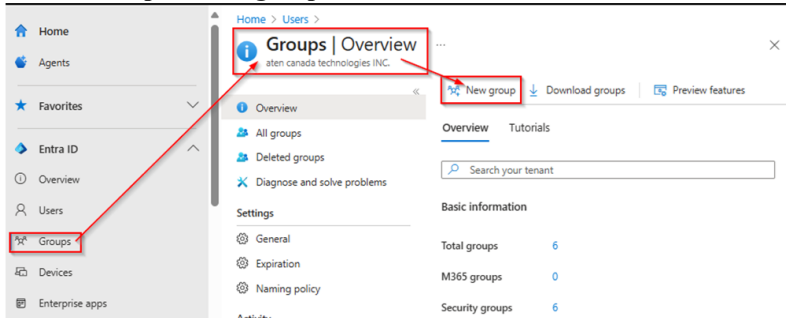


4. Verify the entered information. To edit information, click **Previous**.To proceed, click **Create**.

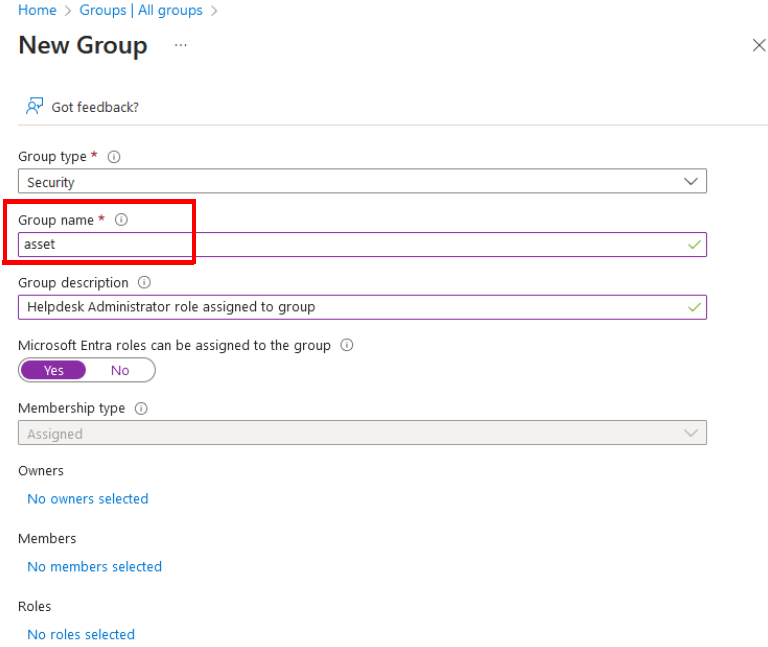


Creating Groups on Microsoft Entra ID

1. Create users to be added to the group.
   For a detailed procedure, see *Creating Users on Microsoft Entra ID*.
2. Go to **Groups** > **New group**.



3. In the New Group page, enter a group name.

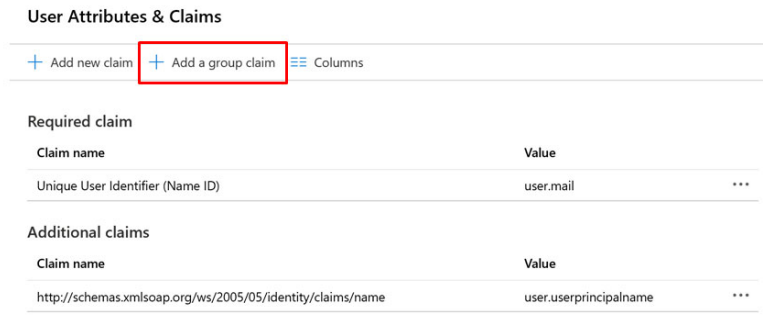


4. Click **No members selected** to add members to the group.
5. Click **Create** to apply the settings.

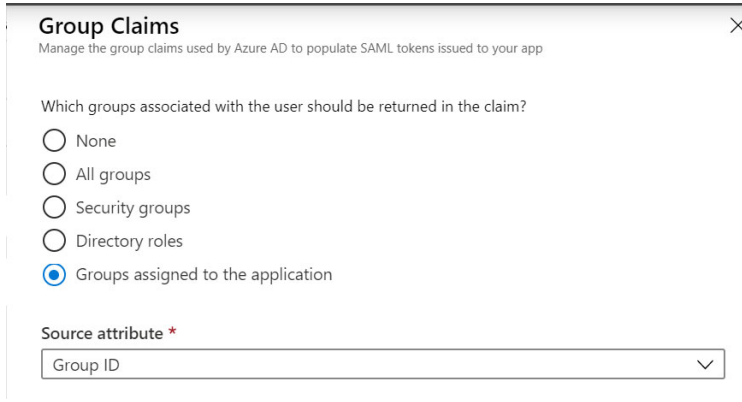
Adding Group Claims to Tokens

To allow the authentication token to contain a list of IDs of the groups that a user belongs to, configure the Group Claims as follows.

1. In Microsoft Entra admin center, go to **Enterprise Apps**, select the application in the list, select **Single Sign On configuration**, and then select **User Attributes & Claims**.



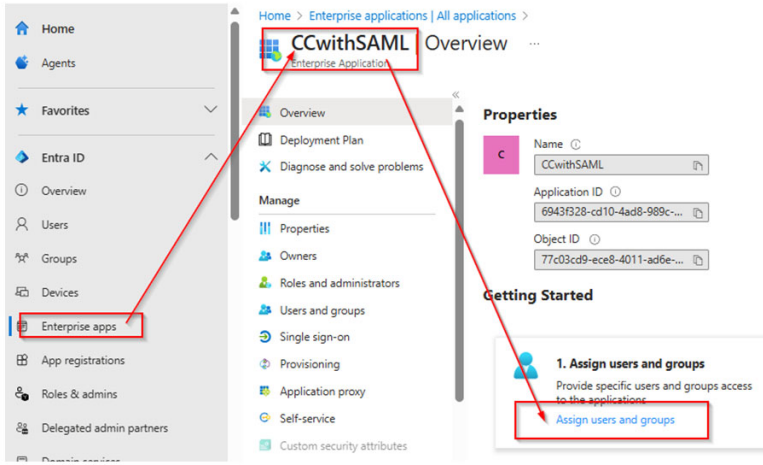
2. In the pop-up window, select **Groups assigned to the application**, and specify the source attribute. For example:



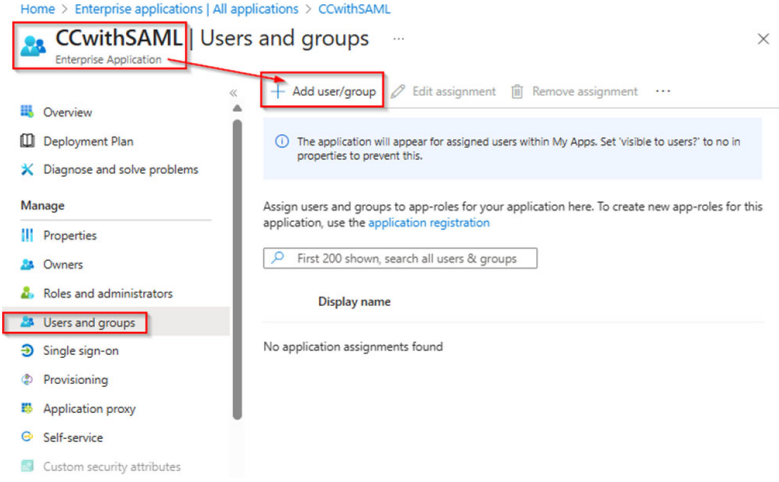
3. Click **Save** to save the settings.

Granting Access Privilege to Users and Groups

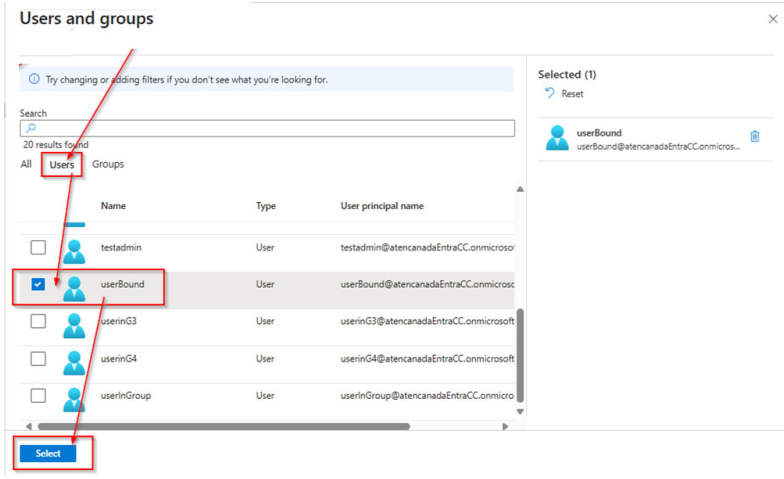
1. In Microsoft Entra admin center, go to **Enterprise Apps**, select the application in the list, and then select **Assign users and groups**.



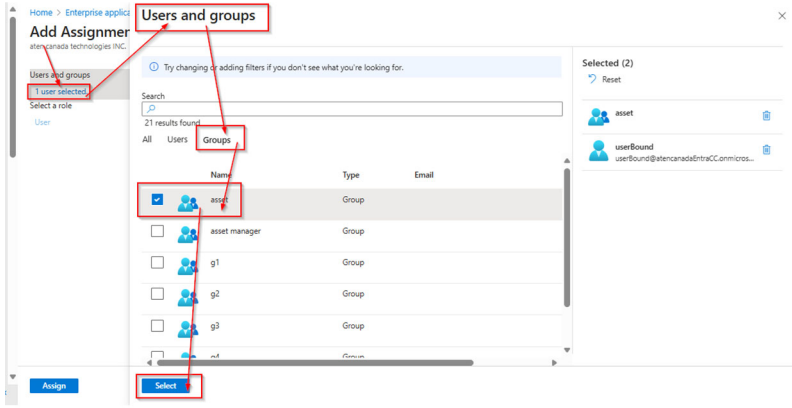
2. From the Users and groups page, click + **Add user/group**.



3. In the Users tab, click to select users to grant access privilege, and then click **Select**.



4. To add a group, go to the Groups tab, click to select groups to grant access privilege, and then click **Select**.



Appendix E

SSO HTML Sample Codes

Overview

If *Single Sign On* is enabled, it will allow users from another web application to log in CC2000 automatically through a form-based authentication. An example of HTML sample codes are demonstrated in the next section.

SSO HTML Sample Codes

```
<html>
<head><title>Sample page for CC2000 SSO (Single Sign On) Sample</
title></head>
<script language="JavaScript">
<!--
function doLogin()
{
    form1.submit();
}
-->
</script>
<body>
    <table>
  <div align="center">
      <form id="form1" name="form1"  method="post" action="https://
10.3.166.65:443/ccadmin/singlesignon.do">
    <!-- Server_IP_port: CC2000 server IP/port (default port could be omitted)
-->
      <tr>
```

```
        <td>
      <font size=5>Test page for CC2000 SSO (Single Sign On)</font>
  
        </td>
      </tr>
      <tr>
        <td>
          CC Username: <input class="sw4" type="text"
name="MySSO_Username" value="administrator" size="15"> <br><br>
          <!-- signonusername: Username field in CC2000 SSO setting page -->
      </td>
    </tr>
      <tr>
        <td>
          CC Password: <input class="sw4" type="password"
name="MySSO_Password" value="password" size="15"> <br><br>
          <!-- signonpassword: Password field in CC2000 SSO setting page -->
      </td>
    </tr>
      <tr>
        <td>
          <!--
          CC Username: <input class="sw4" type="text" name="loginname"
value="administrator" size="15">       CC
Password: <input class="sw4" type="password" name="loginpass"
value="password" size="15"> <br><br>
          -->
          <input class="bw" type="button" value="SSO to CC2000"
name="login" onClick="doLogin();">
      </td>
    </tr>
```

```
        </form>
    </div>
</body>
</html>
```

Appendix F

CC2000 MIB Reference

Overview

This section provides information about the MIBs supported in CC2000.It provides detailed information required for integration with network management systems, automated monitoring, and event handling.

The section includes the following information:

- A list of supported MIB objects, including OIDs, access types, data formats, and descriptions
- Definitions of SNMP traps, including trap OIDs, trigger conditions (descriptions), and associated parameters
- Subtree structure and organization for object grouping and navigation

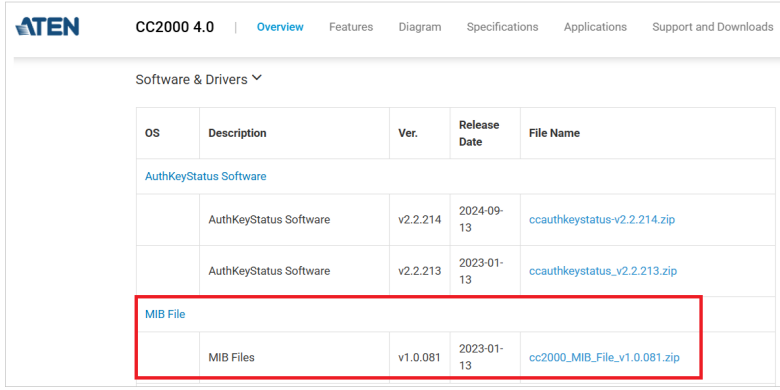
MIB Tree Structure

- **atenProducts** `(.1.3.6.1.4.1.21317.1)`
  This is the root node for all ATEN products.
- **software** `(.1.3.6.1.4.1.21317.1.2)`
  This is a subtree for ATEN software products.
  - **CC2000** `(.1.3.6.1.4.1.21317.1.2.1)`
    Defines the MIB objects and traps for ATEN CC2000.

Downloading MIB Files

To download the latest MIB files:

1. Click this link to visit the CC2000 v4.0 product page.
2. Scroll down to locate the **MIB File** section.



3. Click to download the MIB file.

Note: To use MIB v1.1.101, make sure to update CC2000 to v4.2 or later.

OID Format

In this document, all object identifiers (OIDs) are presented in their numeric form without a leading period.

For example, the OID may be displayed by some SNMP tools as:

```
.1.3.6.1.4.1.21317.1.2.1.1.1.1.0
```

In this document, it is written as:

```
1.3.6.1.4.1.21317.1.2.1.1.1.1.0
```

Both notations are equivalent. The leading period is omitted for consistency and readability.

Object Types and Indexing

SNMP objects can be scalar or table-based. When sending GET requests, ensure to distinguish between scalar objects and instance objects, and their correct OID usage.

- **Scalar Objects**

  A scalar object is an object that contains a discrete piece of data. Since scalar objects are always defined as having one instance, and to distinguish this type of object from instance objects, append **".0"** to the OID when referencing scalar objects in GET requests.

  For example:

  If the `DeviceName` object is defined as:

Object Name	OID
DeviceName	1.3.6.1.4.1.21317.1.3.3.3.7.1

  Using SNMP version 2c, with community string 'public', to retrieve the value of the scalar object `DeviceName.0` from the SNMP agent at IP 192.168.1.10, the GET request will be:

```
snmpget -v2c -c public 192.168.1.10 DeviceName.0
or
snmpget -v2c -c public 192.168.1.10 1.3.6.1.4.1.21317.1.3.3.3.7.1.0
```

  Result:

```
SNMPv2-MIB::DeviceName.0 = STRING: ServerA
```

Note: When ".0" is omitted, SNMP agents will not be able to find the instance and returns an error or invalid message.

- **Instance Objects**

  As opposed to scalar objects, some objects may contain multiple instances, e.g. network interfaces for a device. An instance object is one of the multiple pieces of data that exist in an SNMP table. To refer to these pieces of data correctly in a GET request, use the OIDs that are appended with index numbers.

  For example:

  If the MIB defines the column OID of interface card as `1.3.6.1.2.1.2.2.1.2`

and the device has two interfaces:

Interface Index	Description
1	Ethernet 0
2	Ethernet 1

Using SNMP version 2c, with community string ‘public’, to retrieve the value of the instance 2, from the SNMP agent at IP 192.168.1.10, the SNMP command would be:

```
snmpget -v2c -c public 192.168.1.10 1.3.6.1.2.1.2.2.1.2.2
```

ATEN-CC2K-CFG MIB

System Settings Objects

This section defines objects used for identifying, classifying, and configuring servers and their network communication settings, including server name, server description, server role, HTTP port, HTTPS port, proxy port, viewer port, device port, proxy enablement, and proxy enforcement.

- `serverName`

OID	`1.3.6.1.4.1.21317.1.2.1.1.1.1.0`
Syntax	DisplayString (SIZE (0..32))
Max-Access	read-write
Status	current
Description	A textual string containing name of the server.

- `serverDescription`

OID	`1.3.6.1.4.1.21317.1.2.1.1.1.2.0`
Syntax	DisplayString (SIZE (0..256))
Max-Access	read-write
Status	current
Description	A textual string containing description of the server.

- `serverRole`

OID	`1.3.6.1.4.1.21317.1.2.1.1.1.3.0`
Syntax	DisplayString (SIZE (0..32))
Max-Access	read-only
Status	current
Description	A textual string containing role of the server.

- `httpPort`

OID	`1.3.6.1.4.1.21317.1.2.1.1.1.4.0`
Syntax	Integer32 (1..65535)
Max-Access	read-only
Status	current
Description	The port number of http server listening in CC2000.

- `httpsPort`

OID	`1.3.6.1.4.1.21317.1.2.1.1.1.5.0`
Syntax	Integer32 (1..65535)
Max-Access	read-only
Status	current
Description	The port number of https server listening in CC2000.

- `ccPort`

OID	`1.3.6.1.4.1.21317.1.2.1.1.1.6.0`
Syntax	Integer32 (1..65535)
Max-Access	read-only
Status	current
Description	The port number of cc server manager listening in CC2000.

- `devicePort`

OID	`1.3.6.1.4.1.21317.1.2.1.1.1.7.0`
Syntax	Integer32 (1..65535)
Max-Access	read-only
Status	current
Description	The port number of ATEN device manager listening in CC2000.

- viewerPort

OID	1.3.6.1.4.1.21317.1.2.1.1.1.8.0
Syntax	Integer32 (1..65535)
Max-Access	read-only
Status	current
Description	The port number of cc viewer manager listening in CC2000.

- proxyPort

OID	1.3.6.1.4.1.21317.1.2.1.1.1.9.0
Syntax	Integer32 (1..65535)
Max-Access	read-only
Status	current
Description	The port number of cc porxy listening in CC2000.

- proxyEnable

OID	1.3.6.1.4.1.21317.1.2.1.1.1.10.0
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The proxy enable flag of CC2000, 1: enabled; 0: disabled.

- proxyForce

OID	1.3.6.1.4.1.21317.1.2.1.1.1.11.0
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The proxy force flag of CC2000, 1: force to use proxy; 0: auto-detect to use proxy or not

Server Objects

This section defines objects used for listing, identifying, monitoring, and managing multiple CC servers within a network via SNMP. These objects include number of servers, server status, server name, server type, and IP address.

- `serverNumber`

OID	`1.3.6.1.4.1.21317.1.2.1.1.2.1.0`
Syntax	Integer32
Max-Access	read-only
Status	current
Description	The number of cc servers in CC2000 system management.

- `serverTable`

OID	`1.3.6.1.4.1.21317.1.2.1.1.2.2`
Syntax	SEQUENCE OF ServerEntry
Max-Access	not-accessible
Status	current
Indexes	`servindex`
Description	A list of cc servers. The number of cc servers is given by the value of serverNumber.

- `serverEntry`

Each server entry describes a server property, such as the name, type, IP address, role, or status.

OID	`1.3.6.1.4.1.21317.1.2.1.1.2.2.1`
Syntax	ServerEntry
Max-Access	not-accessible
Status	current
Indexes	`servindex`
Description	Status and parameter values for a cc2000 cc server.

- servIndex

OID	1.3.6.1.4.1.21317.1.2.1.1.2.2.1.1
Syntax	Integer32 (1..2147483647)
Max-Access	read-only
Status	current
Indexes	servindex
Description	The value of index for the cc servers.

- servName

OID	1.3.6.1.4.1.21317.1.2.1.1.2.2.1.2
Syntax	DisplayString (SIZE (0..32))
Max-Access	read-only
Status	current
Indexes	servindex
Description	A textual string containing name of the cc server.

- servType

OID	1.3.6.1.4.1.21317.1.2.1.1.2.2.1.3
Syntax	DisplayString (SIZE (0..32))
Max-Access	read-only
Status	current
Indexes	servindex
Description	A textual string containing type of the cc server.

- servIP

OID	1.3.6.1.4.1.21317.1.2.1.1.2.2.1.4
Syntax	DisplayString (SIZE (0..32))
Max-Access	read-only
Status	current
Indexes	servindex
Description	A textual string containing IP address of the cc server.

- servRole

OID	1.3.6.1.4.1.21317.1.2.1.1.2.2.1.5
Syntax	DisplayString (SIZE (0..32))
Max-Access	read-only
Status	current
Indexes	servindex
Description	A textual string containing role of the cc server.

- servStatus

OID	1.3.6.1.4.1.21317.1.2.1.1.2.2.1.6
Syntax	DisplayString (SIZE (0..32))
Max-Access	read-only
Status	current
Indexes	servindex
Description	A textual string containing status of the cc server.

Trap Objects

This section provides detailed information about the SNMP traps defined in the ATEN-CC2K-CFG MIB. The following entries describe the trap types, their meanings, and the expected parameters to assist with monitoring, alerting, and troubleshooting within SNMP-enabled network environments.

- `serviceStart`

OID	`1.3.6.1.4.1.21317.1.2.1.10.130000`
Status	current
Description	INFORMATIONAL: The management server (IP: xxx.xxx.xxx.xxx) started successfully.

- `serviceStop`

OID	`1.3.6.1.4.1.21317.1.2.1.10.130001`
Status	current
Description	INFORMATIONAL: The management server (IP: `xxx.xxx.xxx.xxx`) stopped successfully.

- `softwareUpgrade`

OID	`1.3.6.1.4.1.21317.1.2.1.10.130002`
Status	current
Description	INFORMATIONAL: CC2000 is upgraded from Old Version to New Version successfully.

- `softwareUpdate`

OID	`1.3.6.1.4.1.21317.1.2.1.10.130003`
Status	current
Description	INFORMATIONAL: CC2000 update (Update) is installed successfully.

- deviceOnline

OID	1.3.6.1.4.1.21317.1.2.1.10.130020
Status	current
Description	INFORMATIONAL: Device (Type: Model Name, MAC: Device MAC, IP: Device IP) was online.

- deviceOffline

OID	1.3.6.1.4.1.21317.1.2.1.10.130021
Status	current
Description	INFORMATIONAL: Device (Type: Model Name, MAC: Device MAC, IP: Device IP) was offline.

- firmwareAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.130030
Status	current
Description	INFORMATIONAL: New device F/W (File Name) has been added.

- firmwareDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.130031
Status	current
Description	INFORMATIONAL: Device F/W (File Name) has been deleted.

- configRestore

OID	1.3.6.1.4.1.21317.1.2.1.10.130040
Status	current
Description	INFORMATIONAL: Device configuration (File Name) has been restored to the device.

- configureDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.130041
Status	current
Description	INFORMATIONAL: Device configuration (File Name) has been deleted.

- configBackup

OID	1.3.6.1.4.1.21317.1.2.1.10.130042
Status	current
Description	INFORMATIONAL: Device configuration (File Name) has been backed up to the repository.

- networkChange

OID	1.3.6.1.4.1.21317.1.2.1.10.130091
Status	current
Description	INFORMATIONAL: The system settings (System > Redundant Servers > Advanced) have been changed.

- serverChange

OID	1.3.6.1.4.1.21317.1.2.1.10.131100
Status	current
Description	INFORMATIONAL:The system settings (System > System Info > General) have been changed.

- effectiveIPChange

OID	1.3.6.1.4.1.21317.1.2.1.10.131101
Status	current
Description	INFORMATIONAL:The effective server IPs (System > System Info > Server IPs) have been changed.

- smtpChange

OID	1.3.6.1.4.1.21317.1.2.1.10.130091
Status	current
Description	INFORMATIONAL:The system settings (System > Redundant Servers > Advanced) have been changed.

- securityChange

OID	1.3.6.1.4.1.21317.1.2.1.10.131102
Status	current
Description	INFORMATIONAL: The system settings (System > Security > Access Protection) have been changed.

- ntpChange

OID	1.3.6.1.4.1.21317.1.2.1.10.130103
Status	current
Description	INFORMATIONAL:The NTP settings have been changed.

- syslogChange

OID	1.3.6.1.4.1.21317.1.2.1.10.130104
Status	current
Description	INFORMATIONAL:The Syslog settings have been changed.

- snmpChange

OID	1.3.6.1.4.1.21317.1.2.1.10.130106
Status	current
Description	INFORMATIONAL:The SNMP settings (Type:Setting Type) have been changed.

- disclaimerChange

OID	1.3.6.1.4.1.21317.1.2.1.10.130107
Status	current
Description	INFORMATIONAL: The Disclaimer settings have been changed.

- certificateUpdate

OID	1.3.6.1.4.1.21317.1.2.1.10.130110
Status	current
Description	INFORMATIONAL: The server certificate has been updated.

- csrIssue

OID	1.3.6.1.4.1.21317.1.2.1.10.130111
Status	current
Description	INFORMATIONAL: A CSR (Certificate Signing Request) has been issued.

- certificateImport

OID	1.3.6.1.4.1.21317.1.2.1.10.130112
Status	current
Description	INFORMATIONAL: A customer certificate has been imported.

- serverRegister

OID	1.3.6.1.4.1.21317.1.2.1.10.130120
Status	current
Description	INFORMATIONAL: The server (Name: Slave Server Name, IP: Server IP) has been registered successfully.

- serverRolePromote

OID	1.3.6.1.4.1.21317.1.2.1.10.130121
Status	current
Description	INFORMATIONAL: The server (Name: Server Name, IP: Server IP) has been promoted to Master server.

- serverRoleChange

OID	1.3.6.1.4.1.21317.1.2.1.10.130122
Status	current
Description	INFORMATIONAL: The server (Name: Server Name) server role has been changed.

- serverSlaveDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.130123
Status	current
Description	INFORMATIONAL: The server (Name: Server Name) has been deleted.

- logOptionModify

OID	1.3.6.1.4.1.21317.1.2.1.10.130130
Status	current
Description	INFORMATIONAL: System log options have been modified.

- logDeviceOptionModify

OID	1.3.6.1.4.1.21317.1.2.1.10.130131
Status	current
Description	INFORMATIONAL: Device log options have been modified.

- logSessionOptionModify

OID	1.3.6.1.4.1.21317.1.2.1.10.130132
Status	current
Description	INFORMATIONAL: Serial console history options have been modified.

- trapOptionModify

OID	1.3.6.1.4.1.21317.1.2.1.10.130133
Status	current
Description	INFORMATIONAL: SNMP trap options in Logs have been modified.

- reportOptionModify

OID	1.3.6.1.4.1.21317.1.2.1.10.130134
Status	current
Description	INFORMATIONAL: Report options have been modified.

- notificationAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.130143
Status	current
Description	INFORMATIONAL: Email notification (Subject: Notification_Subject) has been added.

- notificationDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.130144
Status	current
Description	INFORMATIONAL: Email notification (Subject: Notification_Subject) has been deleted.

- notificationModify

OID	1.3.6.1.4.1.21317.1.2.1.10.130145
Status	current
Description	INFORMATIONAL: Email notification (Subject: Notification_Subject) has been modified.

- logExport

OID	1.3.6.1.4.1.21317.1.2.1.10.130150
Status	current
Description	INFORMATIONAL: Logs have been exported successfully (Name: File Name).

- logExportFail

OID	1.3.6.1.4.1.21317.1.2.1.10.130151
Status	current
Description	INFORMATIONAL: Failed to export logs.

- devLogExport

OID	1.3.6.1.4.1.21317.1.2.1.10.130152
Status	current
Description	INFORMATIONAL: Device logs have been exported successfully (Name: File Name).

- devLogExportFail

OID	1.3.6.1.4.1.21317.1.2.1.10.130153
Status	current
Description	INFORMATIONAL: Failed to export device logs.

- historyExport

OID	1.3.6.1.4.1.21317.1.2.1.10.130154
Status	current
Description	INFORMATIONAL: Serial console history has been exported successfully (Name: File Name).

- historyExportFail

OID	1.3.6.1.4.1.21317.1.2.1.10.130155
Status	current
Description	INFORMATIONAL: Failed to export serial console history.

- trapExport

OID	1.3.6.1.4.1.21317.1.2.1.10.130156
Status	current
Description	INFORMATIONAL: SNMP traps have been exported successfully (Name: File Name).

- trapExportFail

OID	1.3.6.1.4.1.21317.1.2.1.10.130157
Status	current
Description	INFORMATIONAL: Failed to export SNMP traps.

- emailFailTimeout

OID	1.3.6.1.4.1.21317.1.2.1.10.120161
Status	current
Description	WARNING:Failed to send email (timeout). Send to Send To List. Message:Email Message.

- emailFailOthers

OID	1.3.6.1.4.1.21317.1.2.1.10.120162
Status	current
Description	WARNING:Failed to send email (other reason). Send to Send To List. Message:Email Message.

- vmrcUpload

OID	1.3.6.1.4.1.21317.1.2.1.10.130172
Status	current
Description	INFORMATIONAL: VMware Remote Console (VMRC) has been uploaded successfully (File: Upload_File).

- vmrcUploadFail

OID	1.3.6.1.4.1.21317.1.2.1.10.120173
Status	current
Description	WARNING:Uploaded VMware Remote Console (VMRC) file (Upload_File) is invalid.

- sendMessage

OID	1.3.6.1.4.1.21317.1.2.1.10.130182
Status	current
Description	INFORMATIONAL: Message (Subject: Notification subject) has been sent by UN from Message Box.

- deleteMessage

OID	1.3.6.1.4.1.21317.1.2.1.10.130183
Status	current
Description	WARNING: Message (Subject: Notification subject) has been deleted by UN from Message Box.

- slaveLicenseViolation

OID	1.3.6.1.4.1.21317.1.2.1.10.119010
Status	current
Description	CRITICAL:A license violation has been detected on the slave server.

- masterLicenseViolation

OID	1.3.6.1.4.1.21317.1.2.1.10.119011
Status	current
Description	CRITICAL:A master server license violation has been detected. The conflicting server's IP is:Remote server IP.

- serverConnectionLost

OID	1.3.6.1.4.1.21317.1.2.1.10.119020
Status	current
Description	CRITICAL:Lost connection with the server (Name:Server Name, IP:Server IP).

- serverConnection

OID	1.3.6.1.4.1.21317.1.2.1.10.139021
Status	current
Description	CRITICAL: Connected with the server (Name: Server Name, IP: Server IP).

- serverConnectionReject

OID	1.3.6.1.4.1.21317.1.2.1.10.119040
Status	current
Description	CRITICAL: Rejected the server (Name: Slave server Name, IP: Server IP) connection due to server compatibility.

- servicePortConflict

OID	1.3.6.1.4.1.21317.1.2.1.10.119050
Status	current
Description	CRITICAL:A service port conflict (Port:Port Number) has been detected.

- ipFilterDeneied

OID	1.3.6.1.4.1.21317.1.2.1.10.129060
Status	current
Description	CRITICAL:Access denied by IP filter. Denied IP:IP Address.

- macFilterDenied

OID	1.3.6.1.4.1.21317.1.2.1.10.129061
Status	current
Description	CRITICAL:Access denied by MAC filter. Denied MAC:MAC Address.

- userLogin

OID	1.3.6.1.4.1.21317.1.2.1.10.230000
Status	current
Description	INFORMATIONAL: User (Username: UN, IP: CI) logged in successfully.

- userLoginFail

OID	1.3.6.1.4.1.21317.1.2.1.10.230001
Status	current
Description	INFORMATIONAL: User (Username: UN, IP: CI) login failed.

- `userLogout`

OID	`1.3.6.1.4.1.21317.1.2.1.10.230002`
Status	current
Description	INFORMATIONAL: User (Username: UN, IP: CI) logged out.

- `sessionTimeout`

OID	`1.3.6.1.4.1.21317.1.2.1.10.230003`
Status	current
Description	INFORMATIONAL: Session (Username: UN, IP: CI) timed out.

- `sessionTimeoutUnexpect`

OID	`1.3.6.1.4.1.21317.1.2.1.10.230004`
Status	current
Description	INFORMATIONAL: Session (Username: UN, IP: CI) timed out because of unexpected disconnection.

- `userLockout`

OID	`1.3.6.1.4.1.21317.1.2.1.10.210005`
Status	current
Description	CRITICAL: User (Username: UN, IP: CI) has been locked out due to the system lockout policy.

- `sessionEnded`

OID	`1.3.6.1.4.1.21317.1.2.1.10.230010`
Status	current
Description	INFORMATIONAL: Session (Username: User Name, IP: User IP) has been ended by the administrator (Username: UN, IP: CI).

- sessionEndedSystem

OID	1.3.6.1.4.1.21317.1.2.1.10.220011
Status	current
Description	WARNING: User session (Username: User Name, IP: User IP) has been ended by SYSTEM.

- userAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.330000
Status	current
Description	INFORMATIONAL: User (Username: User Name) was added.

- userDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.330001
Status	current
Description	INFORMATIONAL: User (Username: User Name) was deleted.

- userModify

OID	1.3.6.1.4.1.21317.1.2.1.10.330002
Status	current
Description	INFORMATIONAL: User (Username: User Name) account was modified.

- userRightsModify

OID	1.3.6.1.4.1.21317.1.2.1.10.330003
Status	current
Description	INFORMATIONAL: User (Username: User Name) access rights were modified.

- `userTypeChange`

OID	`1.3.6.1.4.1.21317.1.2.1.10.320004`
Status	current
Description	WARNING: User type for User Name has been changed from Old Use Type to New User Type.

- `groupAdd`

OID	`1.3.6.1.4.1.21317.1.2.1.10.330020`
Status	current
Description	INFORMATIONAL: Group (Group name: Group Name) was added.

- `groupDelete`

OID	`1.3.6.1.4.1.21317.1.2.1.10.330021`
Status	current
Description	INFORMATIONAL: Group (Group name: Group Name) was deleted.

- `groupModify`

OID	`1.3.6.1.4.1.21317.1.2.1.10.330022`
Status	current
Description	INFORMATIONAL: Group (Group name: Group Name) information was modified.

- `groupRightsModify`

OID	`1.3.6.1.4.1.21317.1.2.1.10.330023`
Status	current
Description	INFORMATIONAL: Group (Group name: Group Name) access rights were modified.

- groupMemberAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.330025
Status	current
Description	INFORMATIONAL: Group (Name: Group Name) member (User List) was added.

- groupMemberDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.330026
Status	current
Description	INFORMATIONAL: Group (Name: Group Name) member (User List) was deleted.

- userTypeAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.330040
Status	current
Description	INFORMATIONAL: User defined type (Name: User Type Name) has been added.

- userTypeDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.330041
Status	current
Description	INFORMATIONAL: User defined type (Name: User Type Name) has been deleted.

- userTypeModify

OID	1.3.6.1.4.1.21317.1.2.1.10.330042
Status	current
Description	INFORMATIONAL: User defined type (Name: User Type Name) has been modified.

- internalAuthServerModify

OID	1.3.6.1.4.1.21317.1.2.1.10.330060
Status	current
Description	INFORMATIONAL: CC2000 internal authentication service (Name: Server Name, IP: Server IP) has been modified.

- authServerAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.330070
Status	current
Description	INFORMATIONAL: Third party authentication server (Name: Server Name, IP: Server IP) has been added.

- authServerDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.330071
Status	current
Description	INFORMATIONAL: Third party authentication server (Name: Server Name, IP: Server IP) has been deleted.

- authServerModify

OID	1.3.6.1.4.1.21317.1.2.1.10.330072
Status	current
Description	INFORMATIONAL: Third party authentication server (Name: Server Name, IP: Server IP) has been modified.

- authGroupAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.330090
Status	current
Description	INFORMATIONAL: domain group for third party authentication service (Group: Group Name, Name: Server Name, IP: Server IP) has been added.

- authGroupDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.330091
Status	current
Description	INFORMATIONAL: domain group for third party authentication service (Group: Group Name, Server Name: Server Name, IP: Server IP) has been deleted.

- authGroupModify

OID	1.3.6.1.4.1.21317.1.2.1.10.330092
Status	current
Description	INFORMATIONAL: domain group for third party authentication service (Group: Group Name, Server Name: Server Name, IP: Server IP) has been modified.

- deviceAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.430000
Status	current
Description	INFORMATIONAL: Device (Type: Model Name, MAC: Device MAC) was added.

- deviceDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.430001
Status	current
Description	INFORMATIONAL: Device (Type: Model Name, MAC: Device MAC, Folder: Folder Name) was deleted.

- transferDevSettings

OID	1.3.6.1.4.1.21317.1.2.1.10.430011
Status	current
Description	INFORMATIONAL: Device (Type: Model Name, MAC: Device MAC-1) settings were transferred to another device (MAC: Device MAC-2).

- devicePropertisModify

OID	1.3.6.1.4.1.21317.1.2.1.10.430020
Status	current
Description	INFORMATIONAL: Device (Name: Device Name, ID: DI) properties were modified.

- deviceRightsModify

OID	1.3.6.1.4.1.21317.1.2.1.10.430021
Status	current
Description	INFORMATIONAL: Device (Name: Device Name, ID: DI) access rights were modified.

- portPropertisModify

OID	1.3.6.1.4.1.21317.1.2.1.10.430040
Status	current
Description	INFORMATIONAL: Port (Name: Port Name, ID: DI) properties were modified.

- portRightsModify

OID	1.3.6.1.4.1.21317.1.2.1.10.430041
Status	current
Description	INFORMATIONAL: Port (Name: Port Name, ID: DI) access right was modified.

- genericDeviceAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.430060
Status	current
Description	INFORMATIONAL: Generic device (Name: Generic Device Name) was added.

- genericDeviceDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.430061
Status	current
Description	INFORMATIONAL: Generic device (Name: Generic Device Name, Folder: Folder Name) was deleted.

- genericDevicePropertiesModify

OID	1.3.6.1.4.1.21317.1.2.1.10.430062
Status	current
Description	INFORMATIONAL: Generic device (Name: Generic Device Name) properties were modified.

- genericDeviceRightsModify

OID	1.3.6.1.4.1.21317.1.2.1.10.430063
Status	current
Description	INFORMATIONAL: Generic device (Name: Generic Device Name) access right were modified.

- groupDeviceAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.430090
Status	current
Description	INFORMATIONAL: Group device (Name: Grouped Device Name) was added.

- groupDeviceDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.430091
Status	current
Description	INFORMATIONAL: Group device (Name: Grouped Device Name, Folder: Folder Name) was deleted.

- groupDevicePropertiesModify

OID	1.3.6.1.4.1.21317.1.2.1.10.430092
Status	current
Description	INFORMATIONAL: Group device (Name: Grouped Device Name) properties were modified.

- groupDevicePortAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.430094
Status	current
Description	INFORMATIONAL: Port (Name: Port Name, ID: DI) was added to group device (Name: Grouped Device Name).

- groupDevicePortDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.430095
Status	current
Description	INFORMATIONAL: Port (Name: Port Name, ID: DI) was deleted from group device (Name: Grouped Device Name).

- aggregateDeviceAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.430100
Status	current
Description	INFORMATIONAL: Aggregate device (Name: Aggregate Device Name) was added.

- aggregateDeviceDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.430101
Status	current
Description	INFORMATIONAL: Aggregate device (Name: Aggregate Device Name, Folder: Folder Name) was deleted.

- aggregateDevicePropertiesModify

OID	1.3.6.1.4.1.21317.1.2.1.10.430102
Status	current
Description	INFORMATIONAL: Aggregate device (Name: Aggregate Device Name) properties were modified.

- aggregateDeviceRightsModify

OID	1.3.6.1.4.1.21317.1.2.1.10.430103
Status	current
Description	INFORMATIONAL: Aggregate device (Name: Aggregate Device Name) access rights were modified.

- aggregateDevicePortAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.430104
Status	current
Description	INFORMATIONAL: Port (Name: Port Name, ID: DI) was added to aggregate device (Name: Aggregate Device Name).

- aggregateDevicePortDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.430105
Status	current
Description	INFORMATIONAL: Port (Name: Port Name, ID: DI) was deleted from aggregate device (Name: Aggregate Device Name).

- bladeChassisAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.430130
Status	current
Description	INFORMATIONAL: Blade chassis (Name: Blade Chassis Name, ID: DI) was added.

- bladeChassisDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.430131
Status	current
Description	INFORMATIONAL: Blade chassis (Name: Blade Chassis Name, ID: DI, Folder: Folder Name) was deleted.

- bladeChassisPropertiesModify

OID	1.3.6.1.4.1.21317.1.2.1.10.430132
Status	current
Description	INFORMATIONAL: Blade chassis (Name: Blade Chassis Name, ID: DI) properties were modified.

- bladeChassisRightsModify

OID	1.3.6.1.4.1.21317.1.2.1.10.430133
Status	current
Description	INFORMATIONAL: Blade chassis (Name: Blade Chassis Name, ID: DI) access rights were modified.

- bladeChassisPortAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.430134
Status	current
Description	INFORMATIONAL: Port (Name: Port Name, ID: DI) was added to blade chassis (Name: Blade Chassis Name).

- bladeChassisPortDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.430135
Status	current
Description	INFORMATIONAL: Port (Name: Port Name, ID: DI) was deleted from blade chassis (Name: Blade Chassis Name).

- bladeAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.430150
Status	current
Description	INFORMATIONAL: Blade (Name: Blade Name, ID: DI) was added.

- bladeDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.430151
Status	current
Description	INFORMATIONAL: Blade (Name: Blade Name, ID: DI) was deleted.

- bladePropertiesModify

OID	1.3.6.1.4.1.21317.1.2.1.10.430152
Status	current
Description	INFORMATIONAL: Blade (Name: Blade Name, ID: DI) properties were modified.

- bladeRightsModify

OID	1.3.6.1.4.1.21317.1.2.1.10.430153
Status	current
Description	INFORMATIONAL: Blade (Name: Blade Name, ID: DI) access rights were modified.

- bladePortAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.430154
Status	current
Description	INFORMATIONAL: Port (Name: Port Name, ID: DI) was added to blade (Name: Blade Name).

- bladePortDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.430155
Status	current
Description	INFORMATIONAL: Port (Name: Port Name, ID: DI) was deleted from blade (Name: Blade Name).

- bladeSlotChange

OID	1.3.6.1.4.1.21317.1.2.1.10.430156
Status	current
Description	INFORMATIONAL: Blade (Name: Blade Name, ID: DI) slot was changed from Old Slot No to New Slot No.

- virtualServerAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.430170
Status	current
Description	INFORMATIONAL: Virtual host (Name: Server Name, ID: DI) was added.

- virtualServerDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.430171
Status	current
Description	INFORMATIONAL: Virtual host (Name: Server Name, ID: DI, Folder: Folder Name) was deleted.

- virtualServerPropertiesModify

OID	1.3.6.1.4.1.21317.1.2.1.10.430172
Status	current
Description	INFORMATIONAL: Virtual host (Name: Server Name, ID: DI) properties were modified.

- virtualServerRightsModify

OID	1.3.6.1.4.1.21317.1.2.1.10.430173
Status	current
Description	INFORMATIONAL: Virtual host (Name: Server Name, ID: DI) access rights were modified.

- virtualServerPortAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.430174
Status	current
Description	INFORMATIONAL: Port (Name: Port Name, ID: DI) was added to virtual host (Name: Server Name).

- virtualServerPortDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.430175
Status	current
Description	INFORMATIONAL: Port (Name: Port Name, ID: DI) was deleted from virtual host (Name: Server Name).

- virtualMachinePropertiesModify

OID	1.3.6.1.4.1.21317.1.2.1.10.430192
Status	current
Description	INFORMATIONAL: Virtual machine (Name: VM Name, ID: VM ID) properties were modified.

- virtualMachineRightsModify

OID	1.3.6.1.4.1.21317.1.2.1.10.430193
Status	current
Description	INFORMATIONAL: Virtual machine (Name: VM Name, ID: VM ID) access rights were modified.

- taskAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.530010
Status	current
Description	INFORMATIONAL: Task Type task (Name: Task Name) has been added.

- taskDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.530011
Status	current
Description	INFORMATIONAL: Task Type task (Name: Task Name) has been deleted.

- taskModify

OID	1.3.6.1.4.1.21317.1.2.1.10.530012
Status	current
Description	INFORMATIONAL: Task Type task (Name: Task Name) has been modified.

- taskStart

OID	1.3.6.1.4.1.21317.1.2.1.10.530020
Status	current
Description	INFORMATIONAL: Task (Name: Task Name) has been started successfully.

- taskStartFail

OID	1.3.6.1.4.1.21317.1.2.1.10.520021
Status	current
Description	WARNING: Failed to start task (Name: Task Name).

- taskMiss

OID	1.3.6.1.4.1.21317.1.2.1.10.520022
Status	current
Description	WARNING: Scheduled task is missed due to stopped service. (Name: Task Name, Scheduled time: Task Time).

- taskComplete

OID	1.3.6.1.4.1.21317.1.2.1.10.530030
Status	current
Description	INFORMATIONAL: Task (Name: Task Name) has completed successfully.

- taskCompleteFail

OID	1.3.6.1.4.1.21317.1.2.1.10.520031
Status	current
Description	WARNING: Failed to complete task (Name: Task Name).

- taskCompletePartially

OID	1.3.6.1.4.1.21317.1.2.1.10.520032
Status	current
Description	WARNING: Task (Name: Task Name) has been partially completed.

- taskFWUpgradeFail

OID	1.3.6.1.4.1.21317.1.2.1.10.520040
Status	current
Description	WARNING: Failed to upgrade F/W (Task: Task Name, File: File Name) to device (Name: Device Name, ID: DID).

- taskFWUpgrade

OID	1.3.6.1.4.1.21317.1.2.1.10.530041
Status	current
Description	INFORMATIONAL: Firmware upgrade (Task: Task Name, File: File Name) of device (Name: Device Name, ID: DID) succeeded.

- taskBackupConfigFail

OID	1.3.6.1.4.1.21317.1.2.1.10.520050
Status	current
Description	WARNING: Failed to backup device configuration (Task: Task Name) from device (Name: Device Name, ID: DID).

- taskPowerControlFail

OID	1.3.6.1.4.1.21317.1.2.1.10.520060
Status	current
Description	WARNING: Failed to control power port (Task: Task Name) to device (Name: Port Name, ID: DID).

- taskExportLogFail

OID	1.3.6.1.4.1.21317.1.2.1.10.520070
Status	current
Description	WARNING: Failed to export system log (Task: Task Name).

- taskExportDevLogFail

OID	1.3.6.1.4.1.21317.1.2.1.10.520071
Status	current
Description	WARNING: Failed to export device log (Task: Task Name).

- taskExportHistoryFail

OID	1.3.6.1.4.1.21317.1.2.1.10.520072
Status	current
Description	WARNING: Failed to export serial console history (Task: Task Name).

- taskBackupDBaseFail

OID	1.3.6.1.4.1.21317.1.2.1.10.510080
Status	current
Description	CRITICAL: Failed to backup database (Server: Server Name, Task: Task Name).

- taskReplicateDBaseFail

OID	1.3.6.1.4.1.21317.1.2.1.10.510090
Status	current
Description	CRITICAL: Failed to replicate database (Local server: Local Server Name, Remote server: Remote Server Name, IP: Remote Server IP).

- taskReplicateDBase

OID	1.3.6.1.4.1.21317.1.2.1.10.530091
Status	current
Description	INFORMATIONAL: Succeeded to replicate database (Local server: Local Server Name, Local time (GMT): Local Time, Remote server: Remote Server Name, IP: Remote Server IP, Remote time (GMT): Remote Time).

- deviceConfigModify

OID	1.3.6.1.4.1.21317.1.2.1.10.630000
Status	current
Description	INFORMATIONAL: Device (Name: Device Name, Type: Model Name, ID: DI) configuration was modified.

- portConfigModify

OID	1.3.6.1.4.1.21317.1.2.1.10.630020
Status	current
Description	INFORMATIONAL: Port (Name: Port Name, Device Type: Model Name, ID: DI) configuration was modified.

- portPowerOn

OID	1.3.6.1.4.1.21317.1.2.1.10.630040
Status	current
Description	INFORMATIONAL: Power on. (Device name: Device Name, Port(s): Port Lists).

- portPowerOff

OID	1.3.6.1.4.1.21317.1.2.1.10.630041
Status	current
Description	INFORMATIONAL: Power off. (Device name: Device Name, Port(s): Port Lists).

- portPowerRestart

OID	1.3.6.1.4.1.21317.1.2.1.10.630042
Status	current
Description	INFORMATIONAL: Power restart. (Device name: Device Name, Port(s): Port Lists).

- telnetConnect

OID	1.3.6.1.4.1.21317.1.2.1.10.630060
Status	current
Description	INFORMATIONAL: Telnet connection established. (Device name: Device Name, Port(s): Port Lists).

- sshConnect

OID	1.3.6.1.4.1.21317.1.2.1.10.630080
Status	current
Description	INFORMATIONAL: SSH connection established. (Device name: Device Name, Port(s): Port Lists).

- kvmConnect

OID	1.3.6.1.4.1.21317.1.2.1.10.630100
Status	current
Description	INFORMATIONAL: KVM connection established. (Device name: Device Name, Port(s): Port Lists).

- deviceConfigRestoreFail

OID	1.3.6.1.4.1.21317.1.2.1.10.630161
Status	current
Description	INFORMATIONAL: Failed to restore device configuration to device (Device Name: Device Name, ID: DID).

- deviceNameSync

OID	1.3.6.1.4.1.21317.1.2.1.10.630171
Status	current
Description	INFORMATIONAL: Synchronizing device (Name: Device Name, ID: DID) and port names with the CC2000 succeeded.

- deviceNameSyncFail

OID	1.3.6.1.4.1.21317.1.2.1.10.630172
Status	current
Description	INFORMATIONAL: Synchronizing device (Name: Device Name, ID: DID) and port names with the CC2000 failed.

- deviceWebDirect

OID	1.3.6.1.4.1.21317.1.2.1.10.630180
Status	current
Description	INFORMATIONAL: ATEN/ALTUSEN device direct Web connection. (Name: Device Name, ID: DID).

- deviceWebDirectFail

OID	1.3.6.1.4.1.21317.1.2.1.10.630181
Status	current
Description	INFORMATIONAL: Failed to establish ATEN/ALTUSEN device direct Web connection. (Name: Device Name, ID: DID).

- multiportConnect

OID	1.3.6.1.4.1.21317.1.2.1.10.630190
Status	current
Description	INFORMATIONAL: Multi-port connection established. (Device name: Device Name, Port(s): Port ID Lists).

- genericSshConnect

OID	1.3.6.1.4.1.21317.1.2.1.10.630200
Status	current
Description	INFORMATIONAL: Generic SSH connection established. (Name: Device Name, IP: Device IP, ID: DID).

- genericTelnetConnect

OID	1.3.6.1.4.1.21317.1.2.1.10.630201
Status	current
Description	INFORMATIONAL: Generic Telnet connection established. (Name: Device Name, IP: Device IP, ID: DID).

- genericWebConnect

OID	1.3.6.1.4.1.21317.1.2.1.10.630202
Status	current
Description	INFORMATIONAL: Generic Web connection established. (Name: Device Name, URL: URL, ID: DID).

- virtualMachineConnect

OID	1.3.6.1.4.1.21317.1.2.1.10.630210
Status	current
Description	INFORMATIONAL: Virtual machine connection established. (Name: VM Name, ID: VM ID).

- deviceInformationTrap

OID	1.3.6.1.4.1.21317.1.2.1.10.730000
Status	current
Description	INFORMATIONAL: Information trap from device (Name: Device Name, ID: DI) Trap Details.

- deviceWarningTrap

OID	1.3.6.1.4.1.21317.1.2.1.10.720001
Status	current
Description	WARNING: Warning trap from device (Name: Device Name, ID: DI) Trap Details.

- deviceCriticalTrap

OID	1.3.6.1.4.1.21317.1.2.1.10.710002
Status	current
Description	CRITICAL: Critical trap from device (Name: Device Name, ID: DI) Trap Details.

- monitorAdd

OID	1.3.6.1.4.1.21317.1.2.1.10.830000
Status	current
Description	INFORMATIONAL: Monitor (Name: Monitor Name, Type: Classification, Source: Device Name) was added.

- monitorDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.830001
Status	current
Description	INFORMATIONAL: Monitor (Name: Monitor Name, Type: Classification, Folder: Folder Name, Source: Device Name) was deleted.

- monitorModify

OID	1.3.6.1.4.1.21317.1.2.1.10.830002
Status	current
Description	INFORMATIONAL: Monitor (Name: Monitor Name, Type: Classification, Source: Device Name) properties were modified.

- monitorOptionModify

OID	1.3.6.1.4.1.21317.1.2.1.10.830005
Status	current
Description	INFORMATIONAL: Monitor options were modified.

- monitorRecordsDelete

OID	1.3.6.1.4.1.21317.1.2.1.10.830006
Status	current
Description	INFORMATIONAL: All records for Monitors were deleted.

- monitorAlertCurrent

OID	1.3.6.1.4.1.21317.1.2.1.10.820010
Status	current
Description	WARNING: Threshold alert for current (Name: Monitor Name, Installation Place: Monitor Location, Folder: Folder Name, Source: Device Name, Reading: Value, Threshold: [Min: TH Min, Max: TH Max]) was detected.

- monitorAlertVoltage

OID	1.3.6.1.4.1.21317.1.2.1.10.820011
Status	current
Description	WARNING: Threshold alert for voltage (Name: Monitor Name, Installation Place: Monitor Location, Folder: Folder Name, Source: Device Name, Reading: Value, Threshold: [Min: TH Min, Max: TH Max]) was detected.

- monitorAlertPower

OID	1.3.6.1.4.1.21317.1.2.1.10.820012
Status	current
Description	WARNING: Threshold alert for power (Name: Monitor Name, Installation Place: Monitor Location, Folder: Folder Name, Source: Device Name, Reading: Value, Threshold: [Max: TH Max]) was detected.

- monitorAlertPD

OID	1.3.6.1.4.1.21317.1.2.1.10.820013
Status	current
Description	WARNING: Threshold alert for power dissipation (Name: Monitor Name, Installation Place: Monitor Location, Folder: Folder Name, Source: Device Name, Reading: Value, Threshold: [Max: TH Max]) was detected.

- monitorAlertTemperature

OID	1.3.6.1.4.1.21317.1.2.1.10.820014
Status	current
Description	WARNING: Threshold alert for temperature (Name: Monitor Name, Installation Place: Monitor Location, Folder: Folder Name, Source: Device Name, Reading: Value, Threshold: [Min: TH Min, Max: TH Max]) was detected.

- monitorAlertHumidity

OID	1.3.6.1.4.1.21317.1.2.1.10.820015
Status	current
Description	WARNING: Threshold alert for humidity (Name: Monitor Name, Installation Place: Monitor Location, Folder: Folder Name, Source: Device Name, Reading: Value, Threshold: [Min: TH Min, Max: TH Max]) was detected.

- monitorAlertPressure

OID	1.3.6.1.4.1.21317.1.2.1.10.820016
Status	current
Description	WARNING: Threshold alert for pressure (Name: Monitor Name, Installation Place: Monitor Location, Folder: Folder Name, Source: Device Name, Reading: Value, Threshold: [Min: TH Min, Max: TH Max]) was detected.

- monitorAlertDoor

OID	1.3.6.1.4.1.21317.1.2.1.10.820017
Status	current
Description	WARNING: Door open alert (Name: Monitor Name, Installation Place: Monitor Location, Folder: Folder Name, Source: Device Name) was detected.

- monitorAlertWater

OID	1.3.6.1.4.1.21317.1.2.1.10.820018
Status	current
Description	WARNING: Water leak alert (Name: Monitor Name, Installation Place: Monitor Location, Folder: Folder Name, Source: Device Name) was detected.

- monitorNormalCurrent

OID	1.3.6.1.4.1.21317.1.2.1.10.830030
Status	current
Description	INFORMATIONAL: The current monitor (Name: Monitor Name, Installation Place: Monitor Location, Folder: Folder Name, Source: Device Name, Reading: Value) returned to normal condition.

- monitorNormalVotage

OID	1.3.6.1.4.1.21317.1.2.1.10.830031
Status	current
Description	INFORMATIONAL: The voltage (Name: Monitor Name, Installation Place: Monitor Location, Folder: Folder Name, Source: Device Name, Reading: Value) returned to normal condition.

- monitorNormalPower

OID	1.3.6.1.4.1.21317.1.2.1.10.830032
Status	current
Description	INFORMATIONAL: The power monitor (Name: Monitor Name, Installation Place: Monitor Location, Folder: Folder Name, Source: Device Name, Reading: Value) returned to normal condition.

- monitorNormalPD

OID	1.3.6.1.4.1.21317.1.2.1.10.830033
Status	current
Description	INFORMATIONAL: The power dissipation monitor (Name: Monitor Name, Installation Place: Monitor Location, Folder: Folder Name, Source: Device Name, Reading: Value) returned to normal condition.

- monitorNormalTemperature

OID	1.3.6.1.4.1.21317.1.2.1.10.830034
Status	current
Description	INFORMATIONAL: The temperature monitor (Name: Monitor Name, Installation Place: Monitor Location, Folder: Folder Name, Source: Device Name, Reading: Value) returned to normal condition.

- monitorNormalHumidity

OID	1.3.6.1.4.1.21317.1.2.1.10.830035
Status	current
Description	INFORMATIONAL: The humidity monitor (Name: Monitor Name, Installation Place: Monitor Location, Folder: Folder Name, Source: Device Name, Reading: Value) returned to normal condition.

- monitorNormalPressure

OID	1.3.6.1.4.1.21317.1.2.1.10.830036
Status	current
Description	INFORMATIONAL: The pressure monitor (Name: Monitor Name, Installation Place: Monitor Location, Folder: Folder Name, Source: Device Name, Reading: Value) returned to normal condition.

- monitorNormalDoor

OID	1.3.6.1.4.1.21317.1.2.1.10.830037
Status	current
Description	INFORMATIONAL: The door open monitor (Name: Monitor Name, Installation Place: Monitor Location, Folder: Folder Name, Source: Device Name) returned to normal condition.

- monitorNormalWater

OID	1.3.6.1.4.1.21317.1.2.1.10.830038
Status	current
Description	INFORMATIONAL: The water leak monitor (Name: Monitor Name, Installation Place: Monitor Location, Folder: Folder Name, Source: Device Name) returned to normal condition.