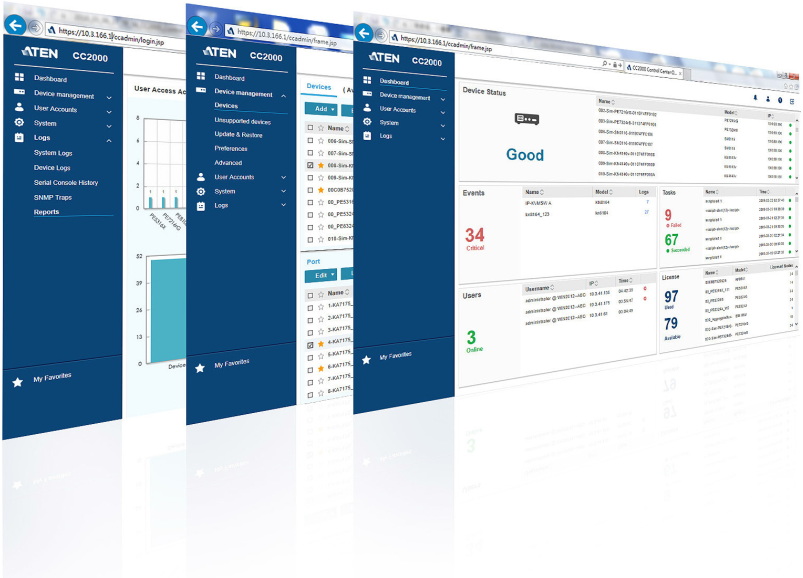
CC2000 Centralized Management Software
User Manual



www.aten.com

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 of this system is not responsible for any radio and/or TV interference caused by unauthorized modifications to this device. It is the responsibility of the user to correct such interference.

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

The CC2000 package consists of:

1 CC2000 USB License Key

1 Software CD

1 User Instructions*

Check to make sure that all of the components are present and in good order. If anything is missing, or was damaged in shipping, contact your dealer.

Read this manual thoroughly and follow the installation and operation procedures carefully to prevent any damage to the switch or to any other devices on the CC2000 installation.

* Features may have been added to the CC2000 since this manual was published. Please visit our website to download the most up-to-date version.

Manual Date: 2019/07/01

Contents

User Information ii
Online Registration ii
Telephone Support ii
User Notice ii
Package Contents iii
About this Manual xi
Overview xi
Conventions xii
Product Information xii
Important Note about Firmware xiii

*Chapter 1.*Introduction
Overview 1
Features 3
Requirements 5
Server Requirements 5
Client Requirements 6
Hardware Requirements 6
Operating Systems 6
Browsers 7
Device Requirements 7
Licenses 8
Nodes 8
Secondaries 8

*Chapter 2.*Server Installation
Overview 9
Switching to CC2000 v3.0 9
Stop CC2000 Service 10
Windows Version Installation 12
Before You Begin 12
Starting the Installation 12
Post-installation Check 18
Linux Version Installation 19
Before you Begin 19
Installing 20
Post-installation Check 21
Post-Installation Setup 21
Uninstalling the CC2000 22
Uninstalling from a Windows System 22
Uninstalling from a Linux System 22
Upgrading the CC2000 23
Preliminary Steps 23
CC2000 Secondary Servers 24

CC2000 Redundant Secondary Servers 24

*Chapter 3.*Browser Operation

Logging In 25
The Interface 27
Screen Components 27
Message Box 29
Inbox 29
Sent 31
Drafts 32

*Chapter 4.*Dashboard and Basic Operation

Overview 33
Device Status 34
Events 35
Tasks 36
Users 37
License 38
Basic Operations 39
Filter 39
Search 40
Table Headings 41
Edit / Further Options 41
Modifications on Interactive Display Panel 41

*Chapter 5.*Device Management

Overview 43
Preliminary Procedures 44
Using VPN 44
Devices 45
Table Headings 48
Adding Device 50
Adding ATEN KVM 50
Adding ATEN PDU 54
Adding an APC PDU 57
Adding a Virtual Host 60
Adding a Blade Chassis 64
Adding an Aggregate Device 68
Adding a Generic Device 72
Adding a Group Device 73
Auto Discovery 75
Search by IP 76
Editing Devices 79
Access rights 79
Device Configuration 84
Properties 84
All Nodes Properties 85

Deleting Devices 85
More 86
Transfer Settings 86
Category Management 87
Locking / Unlocking Devices 88
Diagnose & Fix 89
Go to Associate 89
Operation 90
CC Viewer / KVM Viewer / SN Viewer 90
Web Access 96
Power ON / OFF 97
SSH / Telnet Session 97
Panel Array Mode 97
Ports 99
Launch Viewer 99
Unsupported Devices 100
Update & Restore 102
Firmware Upgrade 102
Upload a File to Upgrade 102
Upgrade with Firmware Repository 103
Firmware Repository 104
Adding Firmware Files 105
Deleting Firmware Files 105
Backup Configuration 106
Restore Configuration 107
Restore 107
Delete 108
Preferences 109
Device/Port Alias 109
Serial Ports Broadcast 111
Misc 112
Advanced 113
General 113
Default Access Rights 114
System Broadcast 114
Broadcast IP address and port number to the devices 114
Broadcast changed IP address and port number to the devices. 115
Device Sync 116
My Favorites 117
Add Favorites 117
Remove Favorites 118

*Chapter 6.*User Accounts

Overview 119
Users 120
User. 120

Add User 120
Edit User 123
Delete User 125
User Types 125
System User Types 126
Custom User Types 126
Delete User Type 127
Groups 128
Groups Tab 128
Add Group 128
Edit Group 130
Delete Group 131
Domain Groups tab 132
Add Domain Group 132
Authentication Services 134
Add Authentication Services 135
Server Information 136
CC2000 Authentication 140
Delete an Authentication Server 141

*Chapter 7.*System

Overview 143
System Info 144
General 144
Time 145
Server IPs 146
Notification 147
SMTP 147
SNMP Traps 149
Syslog 150
Advanced 151
Adding Notification Settings 152
Edit Notification Settings 153
Testing Event Notifications 153
Deleting Notification Settings 154
SNMP 155
SNMP Agent 155
SNMP Manager 157
Security 159
Access Protection 159
IP Filtering 159
MAC Filtering 160
Virtual Media Security Filters 161
Single Sign On Settings 161
Certificate 162
Changing a Self-Signed Certificate 163

. . . . 164
Importing a Signed SSL Server Certificate 165
Import Private Key and Certificate. 166
Disclaimer 167
License 168
Updating the License. 168
License Sharing. 169
License Conflict 170
Task Manager 171
Add 172
Backup Primary Server Database 173
Power Control a Device. 175
Auto upgrade with latest device firmware 176
Upgrade device firmware 178
Backup Device Configuration 179
Export Event Logs 180
Export Device Logs 181
Export serial console history 184
Editing a Task 186
Run Now 186
Deleting a Task 186
Replicate Database 187
VMware Settings 188
VMRC Plugin. 188
Installing Xterm 188
Redundant Servers 189
Primary/Secondary Servers 189
View Properties 190
Register 191
Primary Server View 192
Secondary Server View. 192
Advanced 194
Login policy 194
Lockout Policy 194
User role restriction policy 195
Power control 195

Chapter 8.**Logs**
Overview. 197
System Logs 198
System Logs 198
Export 199
Import 200
Print. 201
Options 201
Device Logs 204

Device Logs . . . 204
Export . . . 205
Options . . . 205
Serial Console History . . . 207
Serial Console History . . . 207
Export . . . 209
Print . . . 209
Options . . . 210
SNMP Traps . . . 211
SNMP Traps . . . 211
Export . . . 211
Print . . . 212
Options . . . 212
Reports . . . 214
User Access Activity . . . 214
Device Access . . . 215
Port Access . . . 217
Asset Statistics . . . 218
Options . . . 219

Technical Information

License Agreement . . . 221
1. DEFINITIONS: . . . 221
2. GRANT OF RIGHTS: . . . 221
3. LIMITED WARRANTY. . . . 222
4. Limitation of Liability. . . . 223
5. Export Regulations. . . . 223
6. TERMINATION: . . . 224
7. MISCELLANEOUS: . . . 224
Technical Support . . . 225
International . . . 225
North America . . . 225
USB Authentication Key Specifications. . . . 225
Supported Aten/Altusen Products . . . 226
Device ANMS Settings . . . 226
VPNs . . . 227
Firewalls . . . 228
CC2000 Proxy Function . . . 229
Name, Description and Range Parameters . . . 230
Trusted Certificates . . . 233
Overview . . . 233
Troubleshooting . . . 234
Self-Signed Private Certificates . . . 239
Examples . . . 239
Importing the Files . . . 239

The CC2000 Utility

Overview . . . 241
System Settings . . . 242
Restore . . . 243
View License . . . 244

Authentication Key Utility

Overview . . . 245
Key Status Information . . . 245
Key Utilities . . . 245
Key Firmware Upgrade . . . 246
Starting the Upgrade . . . 246
Upgrade Succeeded . . . 249
Key License Upgrade . . . 250
Overview . . . 250
Online Upgrade . . . 251
Upgrade Succeeded . . . 255
Offline Upgrade . . . 256
Preliminary Steps . . . 256
Performing the Upgrade . . . 257
Offline Upgrade Failure . . . 262
Order Expiration . . . 263

External Authentication Services

Overview . . . 265
Approved Services . . . 265
LDAP/LDAPS – OpenLDAP Setting Example . . . 265
Active Directory Settings Example . . . 267
RADIUS Settings Example . . . 268
TACACS+ Settings Example . . . 270
NT Domain Settings Example . . . 272
LDAP Group Authorization Setting Examples . . . 273
Example 1 . . . 273
Example 2 . . . 275
Active Directory Group Authorization Setting Example . . . 278

SSO HTML Sample Codes

Overview . . . 281
SSO HTML Sample Codes . . . 281

About this Manual

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

Generally speaking, chapters 1, 3, and 4 are sufficient for basic users. The other chapters and appendixes are only required for specialized user types. For example, System Administrators, should read the entire manual; Device Administrators, chapters 6 and 8; User Managers, chapter 7. Custom user types will want to read the chapters appropriate to their assigned roles.

Overview

Chapter 1, Introduction, introduces you to the CC2000 System. Its purpose, features and benefits are presented, and its front and back panel components are described.

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

Chapter 3, Browser Operation, explains how to log into the CC2000 with a browser, and describes how to work with the CC2000's browser GUI interface.

Chapter 4, Dashboard and Basic Operation, explains the dashboard of the CC2000 server and goes over the basic operation when 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 Accounts, 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.

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 of configuring OpenLDAP for CC2000 authentication, and configuring RADIUS for CC2000 authentication in a Linux environment.

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

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 the option (on a menu or dialog box, for example), that comes next. For example, Start → Run means to open the *Start* menu, and then select *Run*.
⚠	Indicates critical information.

Product Information

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

International	http://www.aten.com

Important Note about Firmware

Due to database changes that have been made with a previous firmware release (V2.8.xxx), this version of CC2000 (v3.x.xxx) is not compatible with any previous CC2000 releases and will run as another application. For details, refer to Chapter 2.

This Page Intentionally Left Blank

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 PDU and other devices including blade servers and virtual machines for in-band and out-of-band management. The brand new CC2000 provides a single easy-to-use 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.

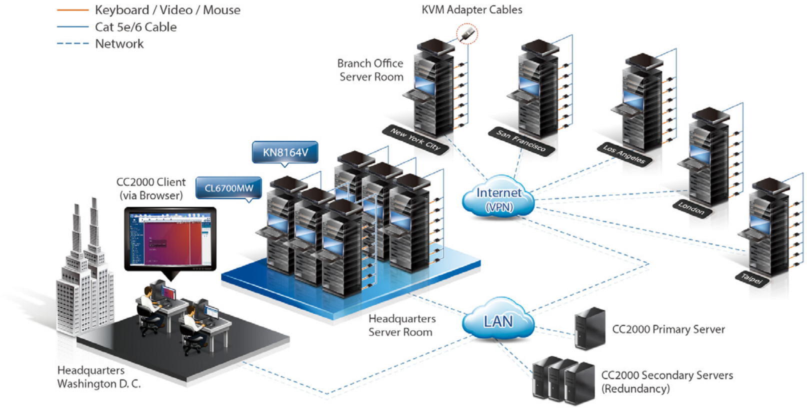
The CC2000's patented Panel DynaArray™ mode lets administrators view the output of multiple ports in individual panels on the same screen. The panel configuration can combine the ports from different over-IP KVM devices and give administrators a flexible choice-to select which devices they wish to monitor 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

- 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 the device status, device events, task results, online users, and licensed nodes usage
- Flexible remote access through service processors and IP tools including Dell iDRAC5/6/8, IBM RSA II, HP iLO2/3/5, Dell CMC, IBM AMM, HP OA, IPMI, IMM and RDP, VNC, SSH, and Telnet
- Supports access and control to virtualized environment over VMware vSphere 5.5/6.0/6.5 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 v1.2 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 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
- Add specific devices and ports to **My Favorites** for quick access

Requirements

Server Requirements

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

- Hardware Requirements
  - CPU: Pentium 4, 2.60 GHz or later
  - Memory: At least 512MB (1GB or more recommended)
  - Hard drive: 500MB or more free space
  - Ethernet: At least 1 Ethernet adapter (100Mbps or higher) – Giga LAN recommended
- Operating System Requirements
  - Windows: Server 2008, Server 2012, Windows Vista, Windows 8, Windows 10 or Server 2016 with Java Runtime Environment (JRE) 8 or later (with the latest service package for each installed)
  - Linux (with Java Runtime Environment (JRE) 8 or later)
    - 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

Client Requirements

Hardware Requirements

- CPU: We recommend that the computers used to access the switch have at least a Pentium 4 2GHz processor, with their 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 the Java Runtime Environment (JRE) must be installed.
- At least 205MB of memory must be available for the first viewer after logging in from the browser and 100MB for each additional viewer that is opened, thereafter.

Operating Systems

- Supported operating systems for client workstations that connect to the CC2000 are shown in the table below:

OS		Version
Windows		7 or later
Linux	RedHat	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 users that log into the CC2000 include Windows 2000 or later, and those capable of running the Java Runtime Environment (JRE) 8 or later.

Note: The Windows 2000 Client does not support the WinClient Viewer.

Browsers

Supported browsers for users that log into the CC2000 include the following:

Browser		Version
IE		10 or later
Edge		40 or later
Chrome		56 or later
Firefox	Windows	60 or later
	Linux	60 or later
	Sun	52 or later
Safari	Windows	4 or later
	Mac	10 or later
Opera		57 or later

Device Requirements

All ATEN/Altusen 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 102.

Note: 1. Devices must be configured to communicate on the same port that you configure for the CC2000's Device Port (see *Device port*, page 15).

2. For a list of supported devices see *Supported Aten/Altusen Products*, page 226.

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.

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. see *License* on page 168, for detailed information.

Nodes

- A node can either be a physical port, or an aggregate device. Each node requires a license.

  Aggregate devices can be created when a device (router, server, Ethernet switch, etc.,) managed through the CC2000 is capable of being accessed through several ATEN/Altusen 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, 2 serial ports and 8 outlet ports.

  Ports on ATEN/Altusen devices, when not part of an aggregate device, must be unlocked (see *Locking / Unlocking Devices*, page 88) 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.

Note: See *Devices* on page 45 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 24 for details regarding registering a Secondary with a primary.

Chapter 2
Server Installation

Overview

Recognizing the increasing importance of Linux in the server environment, the CC2000 Centralized Management Software system makes the CC2000's management services available on both the Windows and Linux platforms. This chapter describes how to install the CC2000 server on each of them.

Switching to CC2000 v3.0

CC2000 v3.0 will run as a new application in the system and does not support the upgrading from v2.8 or previous versions.

If you wish to install CC2000 v3.0 on the same computer as CC2000 v2.8, you must first stop CC2000 v2.8 service first by referring to *Stop CC2000 Service* on page 10, and follow the instructions in *Windows Version Installation* on page 12 (or *Linux Version Installation* on page 19) to install CC2000 v3.0.

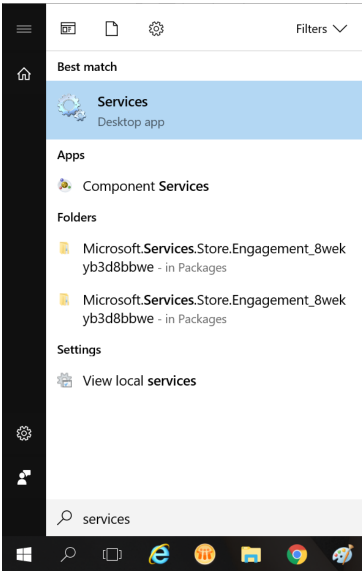
Note:

1. Only one CC2000 primary server can be present in the same local area network. If you have different versions of CC2000 primary servers active, refer to *Stop CC2000 Service* on page 10 to stop the unwanted service.
2. You can use the serial number/USB license key of CC2000 v2.8 for CC2000 v3.0 installation/license upgrade.

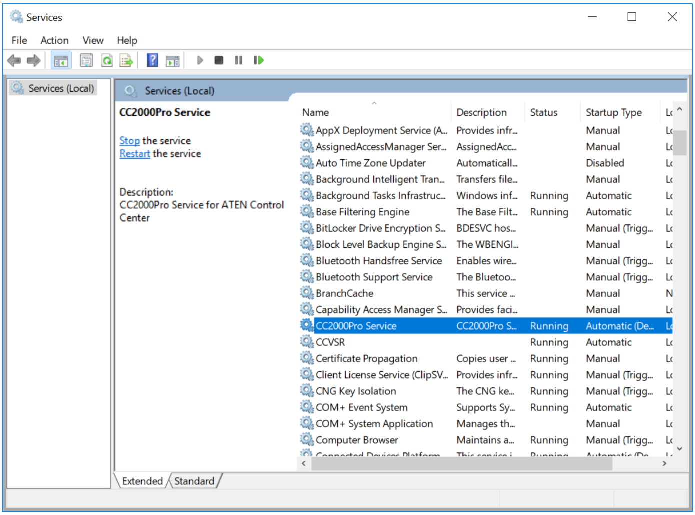
Stop CC2000 Service

Follow the steps below to stop a service:

1. On your windows desktop, search for the keyword *Services* and click to start this desktop app.


Filters
Best match
Services
Desktop app
Apps
Component Services
Folders
Microsoft.Services.Store.Engagement_8wekyb3d8bbwe - in Packages
Microsoft.Services.Store.Engagement_8wekyb3d8bbwe - in Packages
Settings
View local services
services

2. Click to select the CC2000 service.



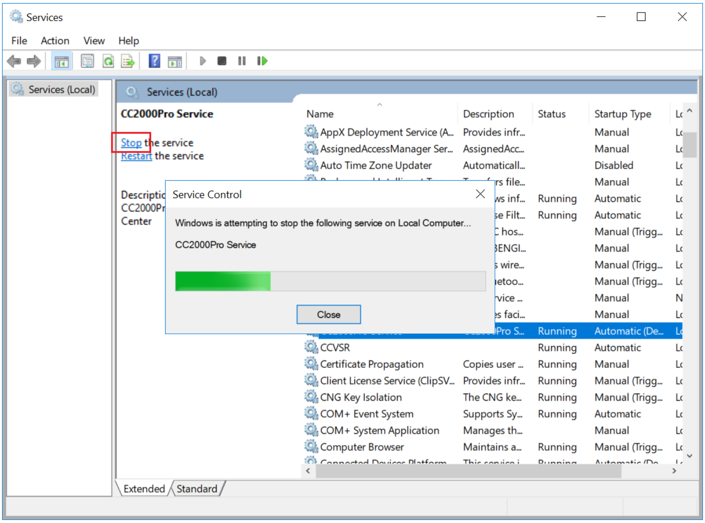
CC2000Pro Service

Stop the service
Restart the service

Description:
CC2000Pro Service for ATEN Control Center

Name	Description	Status	Startup Type	Lc
AppX Deployment Service (A...	Provides infr...		Manual	Lc
AssignedAccessManager Ser...	AssignedAcc...		Manual	Lc
Auto Time Zone Updater	Automaticall...		Disabled	Lc
Background Intelligent Tran...	Transfers file...		Manual	Lc
Background Tasks Infrastruc...	Windows inf...	Running	Automatic	Lc
Base Filtering Engine	The Base Filt...	Running	Automatic	Lc
BitLocker Drive Encryption S...	BDESVC hos...		Manual (Trigg...	Lc
Block Level Backup Engine S...	The WBENGI...		Manual	Lc
Bluetooth Handsfree Service	Enables wire...		Manual (Trigg...	Lc
Bluetooth Support Service	The Bluetoo...		Manual (Trigg...	Lc
BranchCache	This service ...		Manual	N
Capability Access Manager S...	Provides faci...		Manual	Lc
CC2000Pro Service	CC2000Pro S...	Running	Automatic (De...	Lc
CCVSR		Running	Automatic	Lc
Certificate Propagation	Copies user ...	Running	Manual	Lc
Client License Service (ClipSV...	Provides infr...	Running	Manual (Trigg...	Lc
CNG Key Isolation	The CNG ke...	Running	Manual (Trigg...	Lc
COM+ Event System	Supports Sy...	Running	Automatic	Lc
COM+ System Application	Manages th...		Manual	Lc
Computer Browser	Maintains a...	Running	Manual (Trigg...	Lc

3. Click *Stop* to stop the service.



CC2000Pro Service

Stop the service
Restart the service

Descriptic
CC2000Pr
Center

Service Control

Windows is attempting to stop the following service on Local Computer...

CC2000Pro Service

Name	Description	Status	Startup Type	Lc
AppX Deployment Service (A...	Provides infr...		Manual	Lc
AssignedAccessManager Ser...	AssignedAcc...		Manual	Lc
Auto Time Zone Updater	Automaticall...		Disabled	Lc
	rs file...		Manual	Lc
	ws inf...	Running	Automatic	Lc
	se Filt...	Running	Automatic	Lc
	C hos...		Manual (Trigg...	Lc
	BENGI...		Manual	Lc
	s wire...		Manual (Trigg...	Lc
	etoo...		Manual (Trigg...	Lc
	vice ...		Manual	N
	s faci...		Manual	Lc
	Pro S...	Running	Automatic (De...	Lc
CCVSR		Running	Automatic	Lc
Certificate Propagation	Copies user ...	Running	Manual	Lc
Client License Service (ClipSV...	Provides infr...	Running	Manual (Trigg...	Lc
CNG Key Isolation	The CNG ke...	Running	Manual (Trigg...	Lc
COM+ Event System	Supports Sy...	Running	Automatic	Lc
COM+ System Application	Manages th...		Manual	Lc
Computer Browser	Maintains a...	Running	Manual (Trigg...	Lc
Connected Devices Platform ...	This service i...	Running	Automatic (De...	Lc

Note: Service name for CC2000 v2.8 is *CC2000 Service*. Service name for CC2000 v3.0 is *CC2000Pro Service*.

Windows Version Installation

Before You Begin

Before running the installation program, make sure that Sun's Java Runtime Environment (JRE) 8 or higher has been installed on your system. If not, you will first need to download and install it. You can find the latest version on Java's official web site:

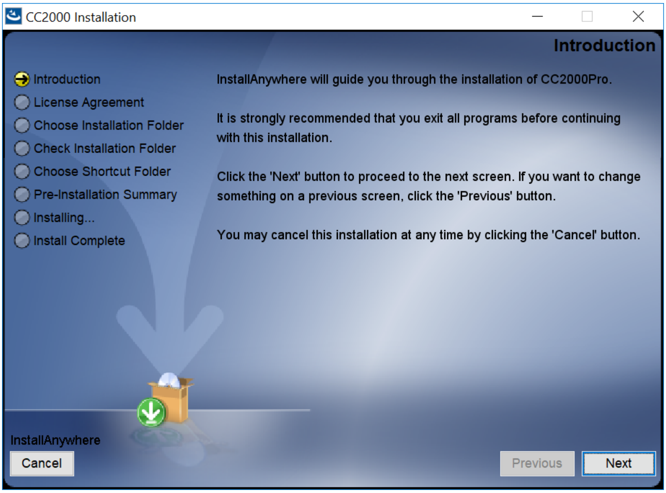
```
http://java.com
```

After JRE has been installed on your system, you will be ready to install 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:



InstallAnywhere will guide you through the installation of CC2000Pro.

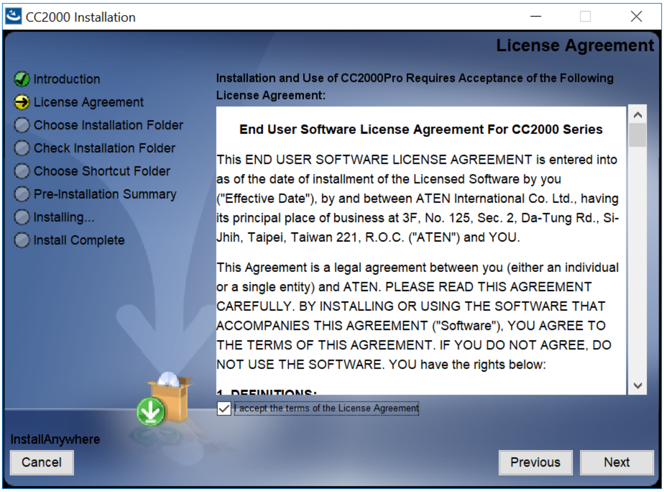
It is strongly recommended that you exit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

Click **Next** to continue.

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



Installation and Use of CC2000Pro Requires Acceptance of the Following License Agreement:

End User Software License Agreement For CC2000 Series

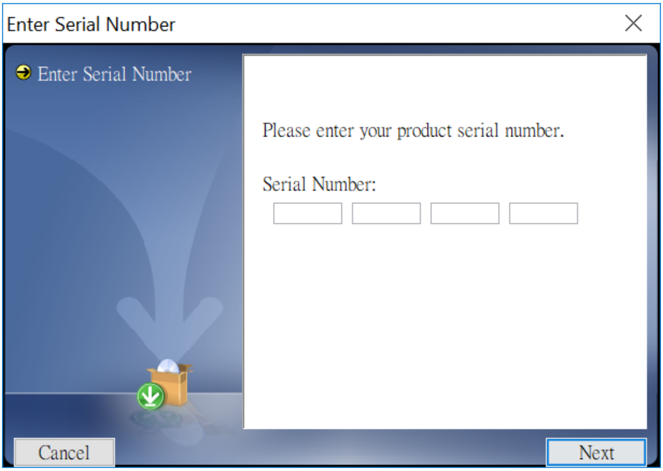
This END USER SOFTWARE LICENSE AGREEMENT is entered into as of the date of installment of the Licensed Software by you ("Effective Date"), by and between ATEN International Co. Ltd., having its principal place of business at 3F, No. 125, Sec. 2, Da-Tung Rd., Si-Jhih, Taipei, Taiwan 221, R.O.C. ("ATEN") 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:

☑ I accept the terms of the License Agreement

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.

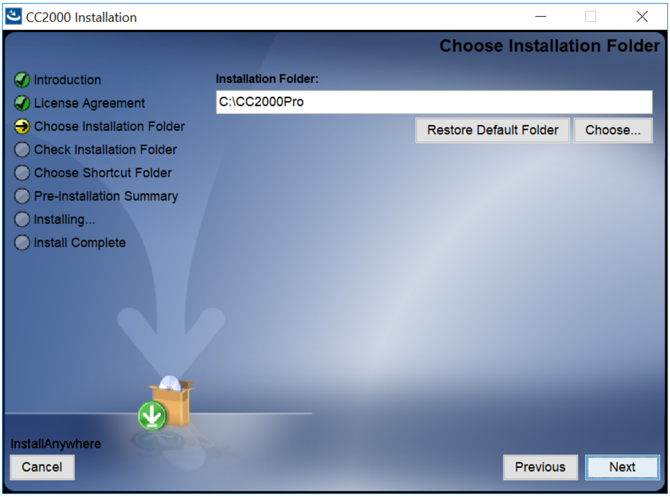


Please enter your product serial number.

Serial Number: □ □ □ □

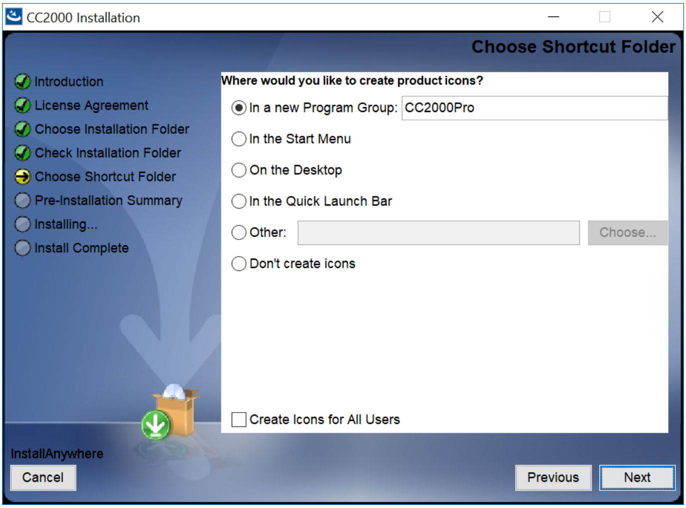
Note: We recommend that you save your software serial number in a safe place in case you need to use it for reinstallation.

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



Installation Folder: C:\CC2000Pro

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



Where would you like to create product icons?

● In a new Program Group: CC2000Pro

○ In the Start Menu

○ On the Desktop

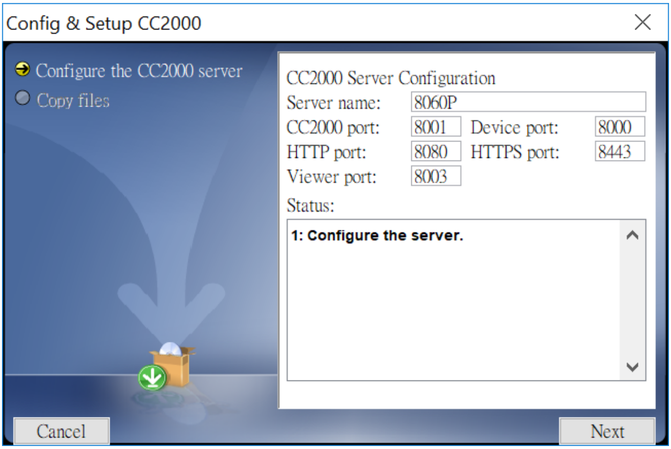
○ In the Quick Launch Bar

○ Other:

○ Don't create icons

□ Create Icons for All Users

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



CC2000 Server Configuration

Server name: 8060P

CC2000 port: 8001 Device port: 8000

HTTP port: 8080 HTTPS port: 8443

Viewer port: 8003

Status:

1: Configure the server.

Heading	Explanation
Server name	The dialog box presents the default name for the server – as defined in the Windows *Computer Name* setting. You can choose a different name to identify the server on the CC2000 installation, if you wish. The name can be from 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 189). 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 port that the CC2000 server uses to communicate with the 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.

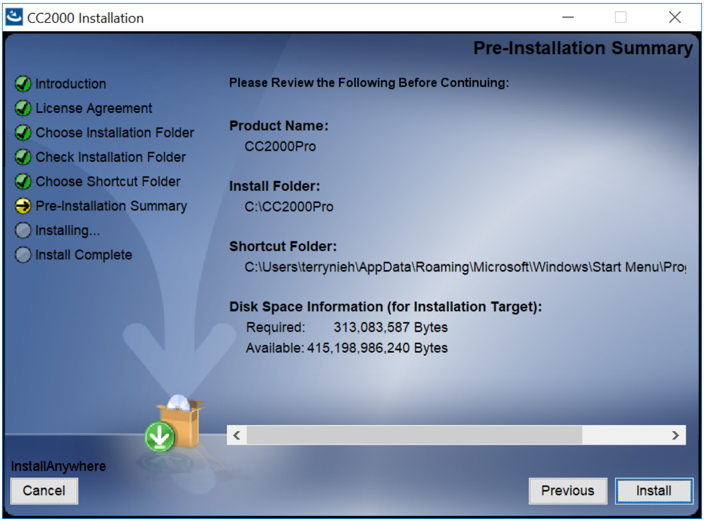
Heading	Explanation
HTTPS port	The port that the CC2000 server uses for secure web communication. The default is 8443. If you use a different port, users must specify the port number in the URL of their browsers.
Viewer Port	The default is 8003.

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 144, 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:



Please Review the Following Before Continuing:

Product Name:
CC2000Pro

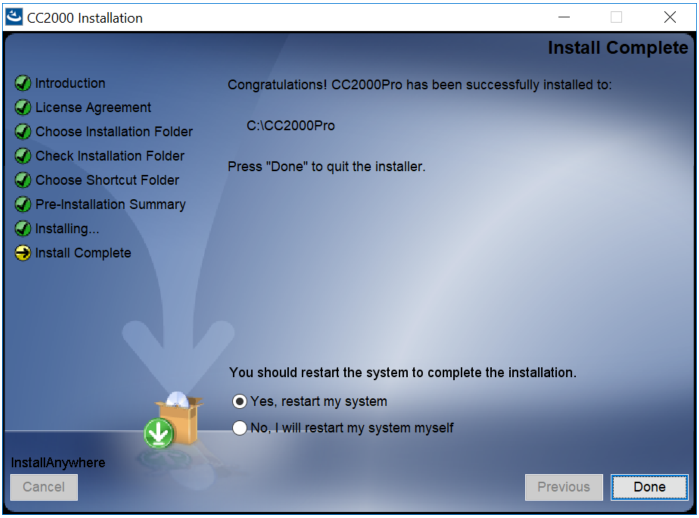
Install Folder:
C:\CC2000Pro

Shortcut Folder:
C:\Users\terrynieh\AppData\Roaming\Microsoft\Windows\Start Menu\Pro

Disk Space Information (for Installation Target):
Required: 313,083,587 Bytes
Available: 415,198,986,240 Bytes

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 system 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 you system.



Congratulations! CC2000Pro has been successfully installed to:

C:\CC2000Pro

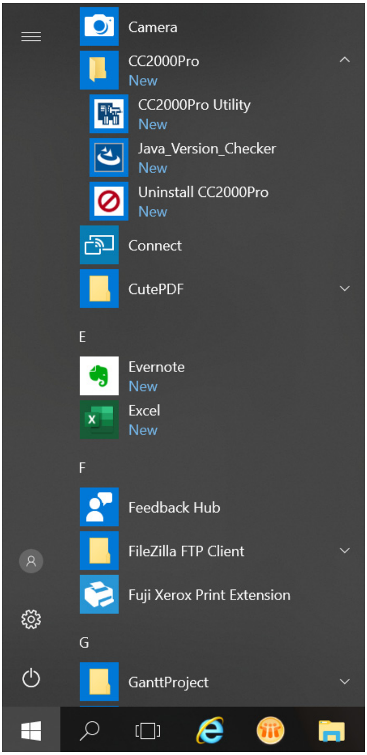
Press "Done" to quit the installer.

You should restart the system to complete the installation.

● Yes, restart my system

○ No, I will restart my system myself

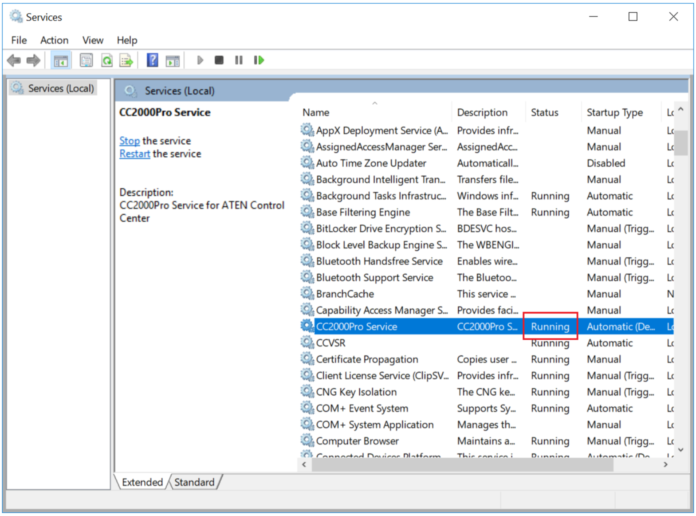
12. A CC2000Pro entry is created in the Windows *Start* menu.



Post-installation Check

After the installation, the CC2000 program starts automatically (and starts automatically with every bootup).

To check that the CC2000 has started, go to the Services desktop app (shown in *Stop CC2000 Service* on page 10) and see if *Running* is shown under the Status column.



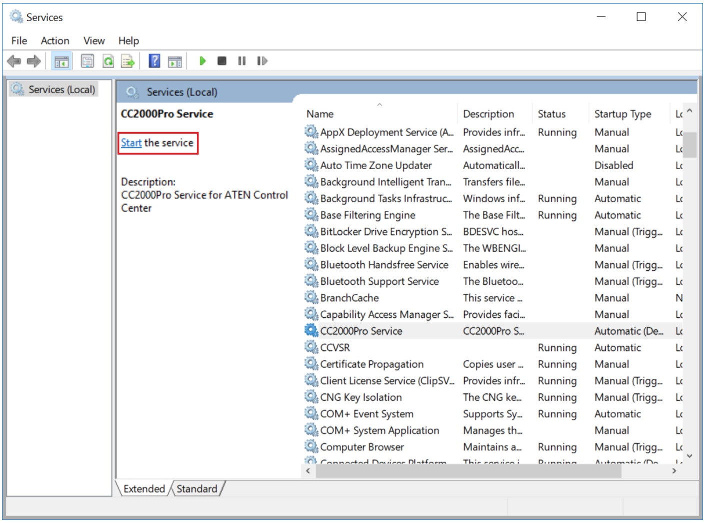
CC2000Pro Service

Stop the service
Restart the service

Description:
CC2000Pro Service for ATEN Control Center

Name	Description	Status	Startup Type	Lc
AppX Deployment Service (A...	Provides infr...		Manual	Lc
AssignedAccessManager Ser...	AssignedAcc...		Manual	Lc
Auto Time Zone Updater	Automaticall...		Disabled	Lc
Background Intelligent Tran...	Transfers file...		Manual	Lc
Background Tasks Infrastruc...	Windows inf...	Running	Automatic	Lc
Base Filtering Engine	The Base Filt...	Running	Automatic	Lc
BitLocker Drive Encryption S...	BDESVC hos...		Manual (Trigg...	Lc
Block Level Backup Engine S...	The WBENGI...		Manual	Lc
Bluetooth Handsfree Service	Enables wire...		Manual (Trigg...	Lc
Bluetooth Support Service	The Bluetoo...		Manual (Trigg...	Lc
BranchCache	This service ...		Manual	N
Capability Access Manager S...	Provides faci...		Manual	Lc
CC2000Pro Service	CC2000Pro S...	Running	Automatic (De...	Lc
CCVSR		Running	Automatic	Lc
Certificate Propagation	Copies user ...	Running	Manual	Lc
Client License Service (ClipSV...	Provides infr...	Running	Manual (Trigg...	Lc
CNG Key Isolation	The CNG ke...	Running	Manual (Trigg...	Lc
COM+ Event System	Supports Sy...	Running	Automatic	Lc
COM+ System Application	Manages th...		Manual	Lc
Computer Browser	Maintains a...	Running	Manual (Trigg...	Lc
Connected Devices Platform ...	This service i...	Running	Automatic (De...	L

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



CC2000Pro Service

Start the service

Description:
CC2000Pro Service for ATEN Control Center

Name	Description	Status	Startup Type	Lc
AppX Deployment Service (A...	Provides infr...	Running	Manual	Lc
AssignedAccessManager Ser...	AssignedAcc...		Manual	Lc
Auto Time Zone Updater	Automaticall...		Disabled	Lc
Background Intelligent Tran...	Transfers file...		Manual	Lc
Background Tasks Infrastruc...	Windows inf...	Running	Automatic	Lc
Base Filtering Engine	The Base Filt...	Running	Automatic	Lc
BitLocker Drive Encryption S...	BDESVC hos...		Manual (Trigg...	Lc
Block Level Backup Engine S...	The WBENGI...		Manual	Lc
Bluetooth Handsfree Service	Enables wire...		Manual (Trigg...	Lc
Bluetooth Support Service	The Bluetoo...		Manual (Trigg...	Lc
BranchCache	This service ...		Manual	N
Capability Access Manager S...	Provides faci...		Manual	Lc
CC2000Pro Service	CC2000Pro S...		Automatic (De...	Lc
CCVSR		Running	Automatic	Lc
Certificate Propagation	Copies user ...	Running	Manual	Lc
Client License Service (ClipSV...	Provides infr...	Running	Manual (Trigg...	Lc
CNG Key Isolation	The CNG ke...	Running	Manual (Trigg...	Lc
COM+ Event System	Supports Sy...	Running	Automatic	Lc
COM+ System Application	Manages th...		Manual	Lc
Computer Browser	Maintains a...	Running	Manual (Trigg...	Lc
Connected Devices Platform ...	This service i...	Running	Automatic (De...	L

Linux Version Installation

Before you Begin

The procedure for installing CC2000 on a Linux system is similar to that for Windows, but there are Java considerations to take note of first.

- 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 JRE versions 8 or higher. Some Linux distributions install earlier versions than the JRE 8. To find out the Java version on your system, open a terminal and enter the following:

  ```
  java -version
  ```

  If the version it displays do not fit the system requirement, please make sure you have a JRE version that is Version 8 or higher. (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 Java version. If the problem exists on your installation, 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:

   ```
   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 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.

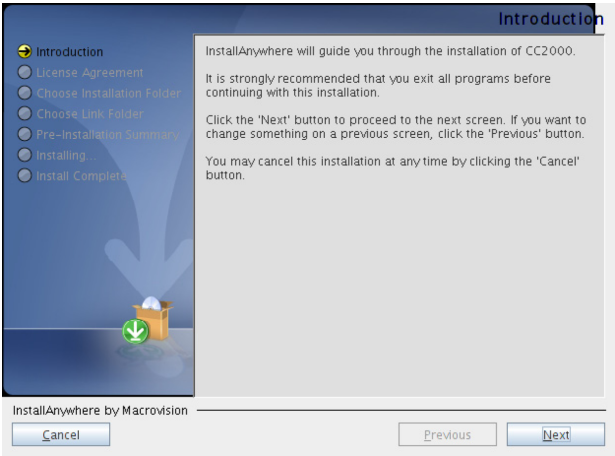
2. Go to the folder where the installation file (e.g. *CC2000_Setup_V3.0.0_ForLinux.exe*) is located and execute it.

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

2. Make sure that the installation file has executable permissions

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

A screen, similar to the one below, appears:



Introduction

InstallAnywhere will guide you through the installation of CC2000.

It is strongly recommended that you exit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

Click **Next** to move on.

4. From here, the installation procedure is the same as the one for Windows. Refer to the Windows installation procedure (see page 12), for details on how to proceed.

Post-installation Check

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

  To check that the CC2000 has started, start, stop, and restart, the service by issuing the following commands (as root) from a terminal console:

  - /etc/init.d/cc2000service start#to start the service
  - /etc/init.d/cc2000service stop#to stop the service
  - /etc/init.d/cc2000service restart#to restart the service
  - /etc/init.d/cc2000service status#to check the service status

- To check on the Java version your system is running, do the following:
  1. Open the *Start* menu.
  2. Navigate to the 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 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 25); go to the *License* page, and click **Upgrade** (see *Updating the License* on page 168, for details). The number of Secondaries and nodes that are 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 register it with the primary. See *View Properties* on page 190, 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 CC2000Pro*.

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 when you installed the program.

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.

Upgrading the CC2000

If the CC2000 program has already been installed, it is not necessary to perform a full install. You can upgrade to the latest CC2000 version by running the CC2000-Upgrade program:

- CC2000Upgrade_Win.exe (for Windows)
- CC2000Upgrade_Linux.bin (for Linux)

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

New versions of the Upgrade Program are put up 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 at the most current level across all of the CC2000 units. If a problem should occur after the upgrade, you can use the backup created with them to restore the database to its latest working level.

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

1. Replicate the database of each of the secondaries; use *Run Now* for the schedule setting (See *Replicate Database* on page 187).
2. After replication completes; go back and set the schedule to a time that will not take place during the upgrade time (next week, next month, etc.).
3. On the primary unit, do a Database Backup.

Once you have finished these preliminary steps you can upgrade 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 1 Primary and up to 31 Secondaries servers located anywhere throughout the world. The Primary server becomes automatically designated when you upgrade the demo license that came with your CC2000 software. See *License*, page 168, for details.

Once the Primary server has been set, you can then register each of the other CC2000 servers as Secondaries with the *Register* function. See *View Properties*, page 190, 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. Users can operate normally and the connected devices can still connect to the server. 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 189 on how you can appoint one of the secondary servers as the primary server.

Chapter 3
Browser Operation

To ensure multi-platform operability, access to the CC2000 is available through most standard web browsers. Once users log in and are authenticated, the CC2000's browser GUI comes up. This chapter explains the login procedure, and describes the CC2000's browser GUI components.

Logging In

Follow the steps below to log into CC2000.

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

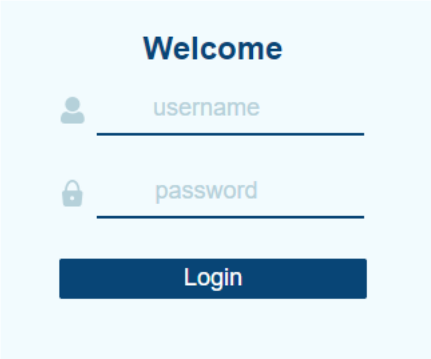
   If you created a shortcut on the desktop, opening the shortcut will bring you to the URL on your default browser.

   Note: If the system administrator has configured the HTTP or HTTPS port setting as something other than the known ports 80 and 443, 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, and a colon is inserted between it and the IP address.

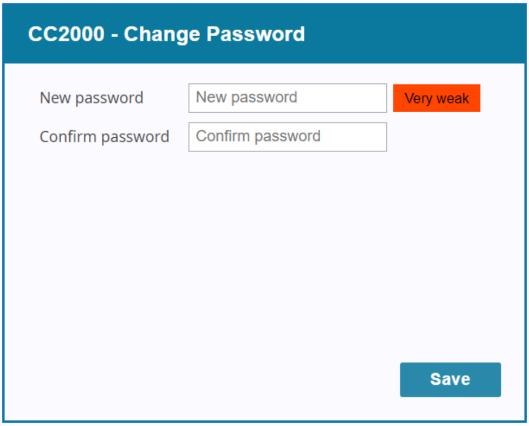
2. If any Security Alert dialog boxes appear, accept the certificate – it can be trusted. See *Trusted Certificates*, page 233 for details. After a moment, the Login page appears:



3. Provide your CC2000 Username and Password, then click *Login*.

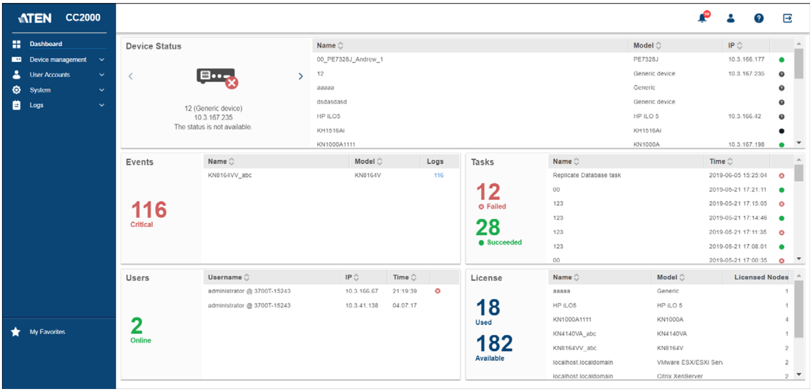
> **Note:** The pre-installed system administrator account's username is "administrator" and the password is "password".

4. The system will immediately prompt you to change the login password as shown:



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

5. The system will bring you to the Dashboard.



Device Status

12 (Generic device)
10.3.167.235
The status is not available.

Name	Model	IP	
00_PE7328J_Andrew_1	PE7328J	10.3.166.177	●
12	Generic device	10.3.167.235	?
aaaaa	Generic		?
dsdasdasd	Generic device		?
HP ILO5	HP ILO 5	10.3.166.42	?
KH1516Ai	KH1516Ai		●
KN1000A1111	KN1000A	10.3.167.198	●

Events

116
Critical

Name	Model	Logs
KN8164VV_abc	KN8164V	116

Tasks

12
⊗ Failed

28
● Succeeded

Name	Time	
Replicate Database task	2019-06-05 15:25:04	⊗
00	2019-05-21 17:21:11	●
123	2019-05-21 17:15:05	⊗
123	2019-05-21 17:14:46	●
123	2019-05-21 17:11:35	⊗
123	2019-05-21 17:08:01	●
00	2019-05-21 17:00:35	⊗

Users

2
Online

Username	IP	Time	
administrator @ 3700T-15243	10.3.166.67	21:19:39	⊗
administrator @ 3700T-15243	10.3.41.138	04:07:17	

License

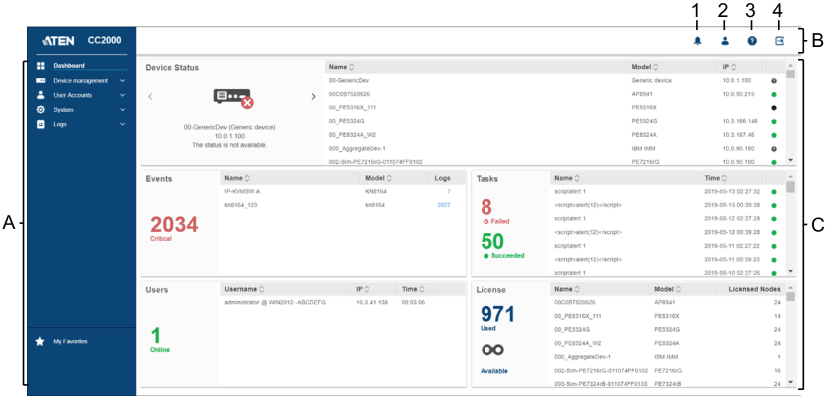
18
Used

182
Available

Name	Model	Licensed Nodes
aaaaa	Generic	1
HP iLO5	HP iLO 5	1
KN1000A1111	KN1000A	4
KN4140VA_abc	KN4140VA	1
KN8164VV_abc	KN8164V	2
localhost.localdomain	VMware ESX/ESXi Serv	2
localhost.localdomain	Citrix XenServer	2

The Interface

Upon logging in, the interface should look like the diagram below:



Device Status

00-GenericDev (Generic device)
10.0.1.100
The status is not available.

Name	Model	IP	
00-GenericDev	Generic device	10.0.1.100	?
00C0B7520626	AP8941	10.0.90.215	●
00_PE5316X_111	PE5316X		●
00_PE5324G	PE5324G	10.3.166.146	●
00_PE8324A_W2	PE8324A	10.3.167.46	●
000_AggregateDev-1	IBM IMM	10.0.90.180	?
002-Sim-PE7216rG-011074FF0102	PE7216rG	10.0.90.180	●

Events

2034 Critical

Name	Model	Logs
IP-KVMSW A	KN8164	7
kn8164_123	kn8164	2027

Tasks

8 Failed

50 Succeeded

Name	Time	
scriptalert 1	2019-05-13 02:27:32	●
<script>alert(12)</script>	2019-05-13 00:39:38	●
scriptalert 1	2019-05-12 02:27:28	●
<script>alert(12)</script>	2019-05-12 00:39:28	●
scriptalert 1	2019-05-11 02:27:22	●
<script>alert(12)</script>	2019-05-11 00:39:23	●
scriptalert 1	2019-05-10 02:27:26	●

Users

1 Online

Username	IP	Time
administrator @ WIN2012--ABCDEFG	10.3.41.138	00:03:06

License

971 Used

∞ Available

Name	Model	Licensed Nodes
00C0B7520626	AP8941	24
00_PE5316X_111	PE5316X	14
00_PE5324G	PE5324G	24
00_PE8324A_W2	PE8324A	24
000_AggregateDev-1	IBM IMM	1
002-Sim-PE7216rG-011074FF0102	PE7216rG	16
003-Sim-PE7324rB-011074FF0103	PE7324rB	24

Screen Components

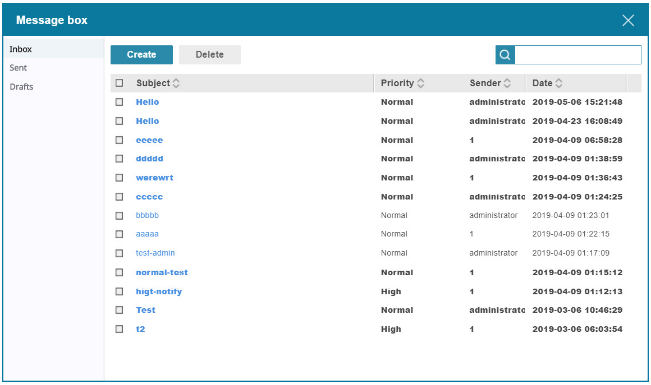
The screen components are described in the table below:

No.	Item	Description
A	Sidebar Menu	The Sidebar Menu is the main selection menu. Click to select the category you wish to view/configure. Clicking the category may expand into submenus for a further configurations.
B	Task Bar	The task bar contains notifications, personal settings (language & password), help and logout.
C	Interactive Display Panel	This 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 – see *The Interface*, page 27.

No.	Item	Description
1	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 198). Click *View message box* to open message box window. Refer to see *Message Box*, page 29 on how to use message box.
2	Personal	Clicking this icon will display the username of this session, the time the user last logged in, user preference option and the change password option. Click *Preferences* to change the language of the interface and whether you wish to *Resume CC2000 to my previous logout status when logging in*. Click *Change password* to change the password for this user.
3	About	Clicking this icon for CC2000 information. Click *Help* for the CC2000 user manual. Click *About* for information of your CC2000.
4	Logout	Click this icon to log out of your CC2000 session.

Message Box

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



□	Subject	Priority	Sender	Date
□	Hello	Normal	administratc	2019-05-06 15:21:48
□	Hello	Normal	administratc	2019-04-23 16:08:49
□	eeeee	Normal	1	2019-04-09 06:58:28
□	ddddd	Normal	administratc	2019-04-09 01:38:59
□	werewrt	Normal	1	2019-04-09 01:36:43
□	ccccc	Normal	administratc	2019-04-09 01:24:25
□	bbbbb	Normal	administrator	2019-04-09 01:23:01
□	aaaaa	Normal	1	2019-04-09 01:22:15
□	test-admin	Normal	administrator	2019-04-09 01:17:09
□	normal-test	Normal	1	2019-04-09 01:15:12
□	higt-notify	High	1	2019-04-09 01:12:13
□	Test	Normal	administratc	2019-03-06 10:46:29
□	t2	High	1	2019-03-06 06:03:54

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 top right-hand corner to filter the messages.

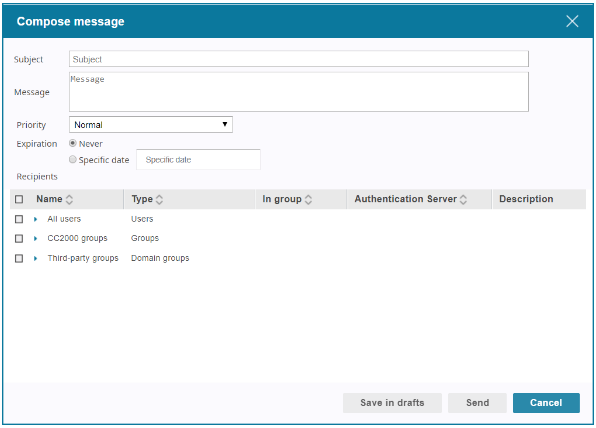
Click the column headings to sort the order of display.

Inbox

■ Create Notification

Follow the steps below to create a notification:

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



Subject: Subject

Message: Message

Priority: Normal ▾

Expiration: ● Never ○ Specific date Specific date

Recipients

□	Name	Type	In group	Authentication Server	Description
□	▸ All users	Users			
□	▸ CC2000 groups	Groups			
□	▸ Third-party groups	Domain groups			

2. Fill in the **Subject** and **Message** fields.

3. Select a priority type using the **Priority** drop-down menu.

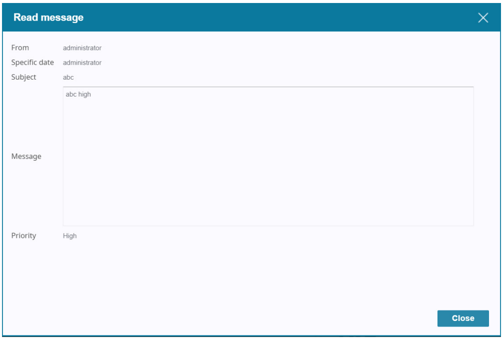
4. Select the **Expiration** option: Never or Specific date. Set the date for the system message to expire if Specific date is selected.

5. Select the **Recipients** by checking the checkbox(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:



From: administrator

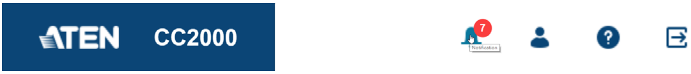
Specific date: administrator

Subject: abc

Message: abc high

Priority: High

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 checkbox(es) of the notification(s) and click **Delete**. A confirmation message will be shown, click **Yes** to confirm.

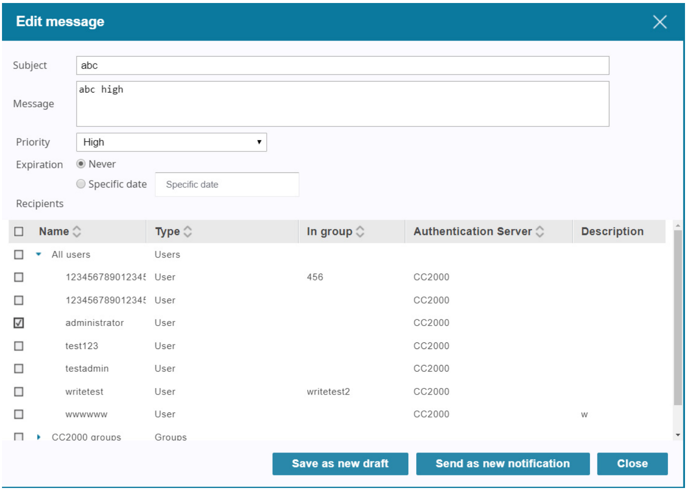
Sent

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 checkbox of the notification and click **Edit**.



Edit message

Subject: abc

Message: abc high

Priority: High

Expiration: ● Never ○ Specific date Specific date

Recipients

□	Name	Type	In group	Authentication Server	Description
□	▾ All users	Users			
□	123456789012345	User	456	CC2000	
□	123456789012345	User		CC2000	
☑	administrator	User		CC2000	
□	test123	User		CC2000	
□	testadmin	User		CC2000	
□	writetest	User	writetest2	CC2000	
□	wwwwww	User		CC2000	w
□	▸ CC2000 groups	Groups			

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 checkbox(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.

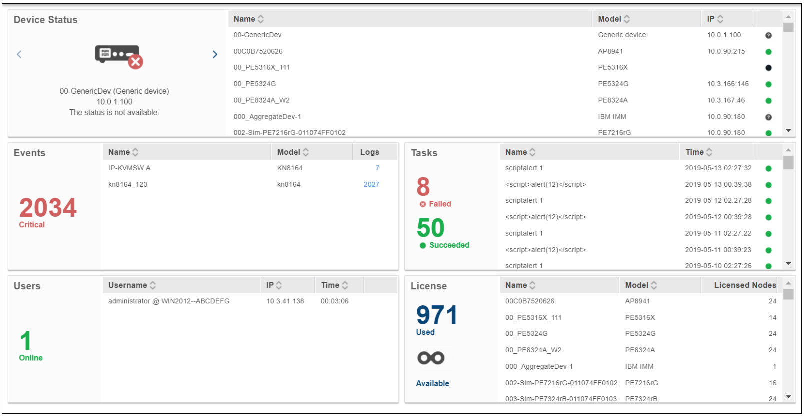
Note: The Edit and Delete options works similar to the ones described in the Sent folder. Refer back to page 31 where necessary.

Chapter 4
Dashboard and Basic Operation

Overview

Dashboard provides a summarized status of the system separated into the following information panels:

Device Status, Events, Users, Tasks and License.



Device Status

00-GenericDev (Generic device)
10.0.1.100
The status is not available.

Name	Model	IP	
00-GenericDev	Generic device	10.0.1.100	?
00C0B7520626	AP8941	10.0.90.215	●
00_PE5316X_111	PE5316X		●
00_PE5324G	PE5324G	10.3.166.146	●
00_PE8324A_W2	PE8324A	10.3.167.46	●
000_AggregateDev-1	IBM IMM	10.0.90.180	?
002-Sim-PE7216rG-011074FF0102	PE7216rG	10.0.90.180	●

Events

2034
Critical

Name	Model	Logs
IP-KVMSW A	KN8164	7
kn8164_123	kn8164	2027

Tasks

8
Failed

50
Succeeded

Name	Time	
scriptalert 1	2019-05-13 02:27:32	●
<script>alert(12)</script>	2019-05-13 00:39:38	●
scriptalert 1	2019-05-12 02:27:28	●
<script>alert(12)</script>	2019-05-12 00:39:28	●
scriptalert 1	2019-05-11 02:27:22	●
<script>alert(12)</script>	2019-05-11 00:39:23	●
scriptalert 1	2019-05-10 02:27:26	●

Users

1
Online

Username	IP	Time
administrator @ WIN2012--ABCDEFG	10.3.41.138	00:03:06

License

971
Used

∞
Available

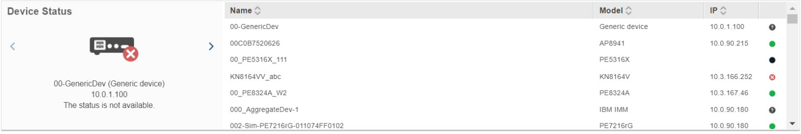
Name	Model	Licensed Nodes
00C0B7520626	AP8941	24
00_PE5316X_111	PE5316X	14
00_PE5324G	PE5324G	24
00_PE8324A_W2	PE8324A	24
000_AggregateDev-1	IBM IMM	1
002-Sim-PE7216rG-011074FF0102	PE7216rG	16
003-Sim-PE7324rB-011074FF0103	PE7324rB	24

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

Device Status

Upon logging into the system for the first time, the Device Status panel will remind you to add devices at the *Device Management* sidebar menu.

With devices added to the system, this panel will display the status of all the devices in a table. The left of the panel displays detailed status of a device while the aforementioned table is on the right. An example is shown below:



Device Status

00-GenericDev (Generic device)
10.0.1.100
The status is not available.

Name	Model	IP	
00-GenericDev	Generic device	10.0.1.100	?
00C0B7520626	AP8941	10.0.90.215	🟢
00_PE5316X_111	PE5316X		●
KN8164VV_abc	KN8164V	10.3.166.252	⊗
00_PE8324A_W2	PE8324A	10.3.167.46	🟢
000_AggregateDev-1	IBM IMM	10.0.90.180	?
002-Sim-PE7216rG-011074FF0102	PE7216rG	10.0.90.180	🟢

If a device is offline or a critical event happened*, the device will be shown on the left with its status shown below. For more than one device, click the left or right arrow to cycle through the devices.

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

Click the column headings of the table to sort the order of display.

The last entry of the table is a visual status display of the device.

🟢 represents online.

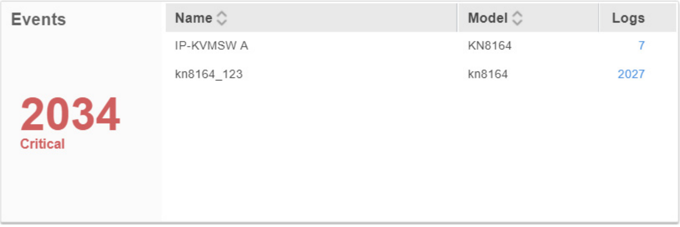
● represents offline.

⊗ represents abnormal.

? represents unknown.

Events

The system will collect all the critical device logs of the past 3 months and display them in this panel.



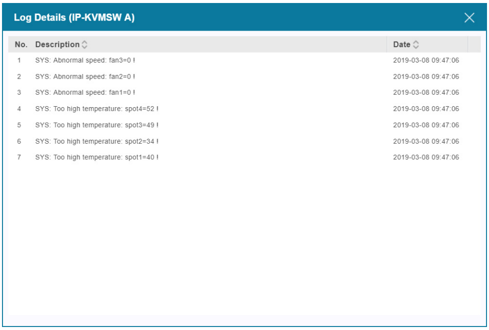
Events

2034
Critical

Name	Model	Logs
IP-KVMSW A	KN8164	7
kn8164_123	kn8164	2027

The number on the left is the total number of critical logs collected.

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:

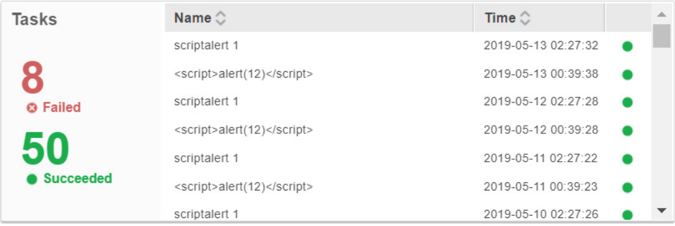


Log Details (IP-KVMSW A)

No.	Description	Date
1	SYS: Abnormal speed: fan3=0 !	2019-03-08 09:47:06
2	SYS: Abnormal speed: fan2=0 !	2019-03-08 09:47:06
3	SYS: Abnormal speed: fan1=0 !	2019-03-08 09:47:06
4	SYS: Too high temperature: spot4=52 !	2019-03-08 09:47:06
5	SYS: Too high temperature: spot3=49 !	2019-03-08 09:47:06
6	SYS: Too high temperature: spot2=34 !	2019-03-08 09:47:06
7	SYS: Too high temperature: spot1=40 !	2019-03-08 09:47:06

Tasks

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



Tasks

8
⊗ Failed

50
● Succeeded

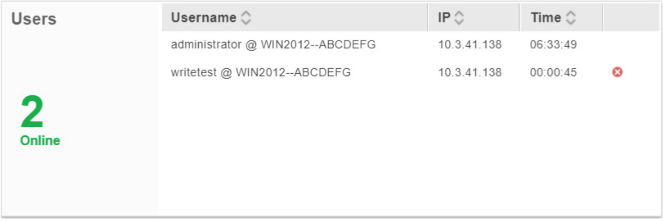
Name	Time	
scriptalert 1	2019-05-13 02:27:32	●
<script>alert(12)</script>	2019-05-13 00:39:38	●
scriptalert 1	2019-05-12 02:27:28	●
<script>alert(12)</script>	2019-05-12 00:39:28	●
scriptalert 1	2019-05-11 02:27:22	●
<script>alert(12)</script>	2019-05-11 00:39:23	●
scriptalert 1	2019-05-10 02:27:26	●

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.

Users

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



Users

2
Online

Username	IP	Time	
administrator @ WIN2012--ABCDEFG	10.3.41.138	06:33:49	
writetest @ WIN2012--ABCDEFG	10.3.41.138	00:00:45	⊗

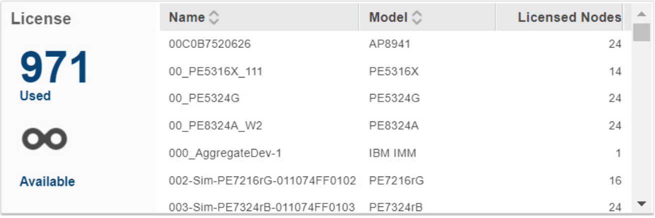
The number on the left shows how many users are currently online.

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

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

License

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



License

971
Used

∞

Available

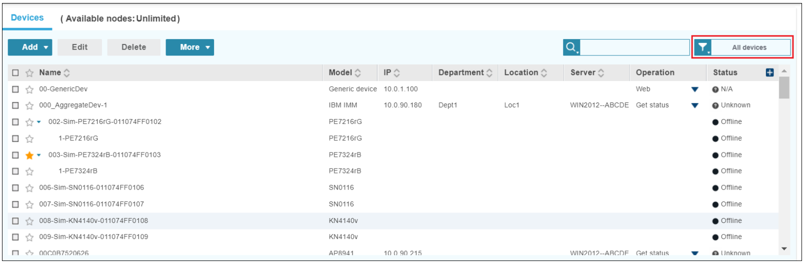
Name	Model	Licensed Nodes
00C0B7520626	AP8941	24
00_PE5316X_111	PE5316X	14
00_PE5324G	PE5324G	24
00_PE8324A_W2	PE8324A	24
000_AggregateDev-1	IBM IMM	1
002-Sim-PE7216rG-011074FF0102	PE7216rG	16
003-Sim-PE7324rB-011074FF0103	PE7324rB	24

Basic Operations

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

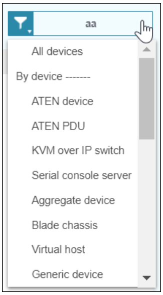
Filter

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:



	Name	Model	IP	Department	Location	Server	Operation	Status
□ ☆	00-GenericDev	Generic device	10.0.1.100				Web	N/A
□ ☆	000_AggregateDev-1	IBM IMM	10.0.90.180	Dept1	Loc1	WIN2012--ABCDE	Get status	Unknown
□ ☆	002-Sim-PE7216rG-011074FF0102	PE7216rG						● Offline
□ ☆	1-PE7216rG	PE7216rG						● Offline
□ ★	003-Sim-PE7324rB-011074FF0103	PE7324rB						● Offline
□ ☆	1-PE7324rB	PE7324rB						● Offline
□ ☆	006-Sim-SN0116-011074FF0106	SN0116						● Offline
□ ☆	007-Sim-SN0116-011074FF0107	SN0116						● Offline
□ ☆	008-Sim-KN4140v-011074FF0108	KN4140v						● Offline
□ ☆	009-Sim-KN4140v-011074FF0109	KN4140v						● Offline
□ ☆	00C0B7520626	AP8941	10.0.90.215			WIN2012--ABCDE	Get status	Unknown

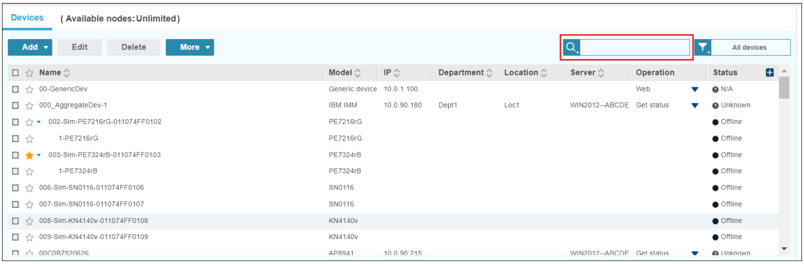
Click the filter bar for a drop-down menu that includes different filter options. An example is shown:



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

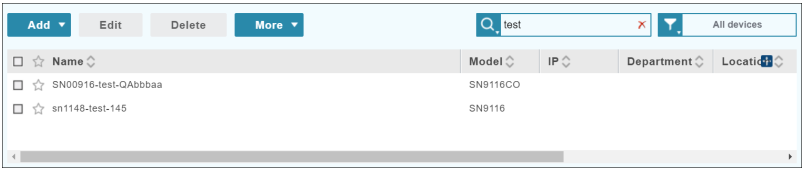
Search allows you to search for items using keywords relating to the search options. Search for a particular table is also located at the top right-hand corner above the table:



□	☆	Name	Model	IP	Department	Location	Server	Operation	Status
□	☆	00-GenericDev	Generic device	10.0.1.100				Web	N/A
□	☆	000_AggregateDev-1	IBM IMM	10.0.90.180	Dept1	Loc1	WIN2012--ABCDE	Get status	Unknown
□	☆	002-Sim-PE7216rG-011074FF0102	PE7216rG						● Offline
□	☆	1-PE7216rG	PE7216rG						● Offline
□	★	003-Sim-PE7324rB-011074FF0103	PE7324rB						● Offline
□	☆	1-PE7324rB	PE7324rB						● Offline
□	☆	006-Sim-SN0116-011074FF0106	SN0116						● Offline
□	☆	007-Sim-SN0116-011074FF0107	SN0116						● Offline
□	☆	008-Sim-KN4140v-011074FF0108	KN4140v						● Offline
□	☆	009-Sim-KN4140v-011074FF0109	KN4140v						● Offline
□	☆	00C0B7520626	AP8941	10.0.90.215			WIN2012--ABCDE	Get status	Unknown

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

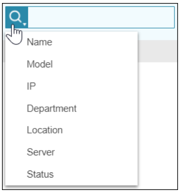
The table will be updated to reflect your search result. An example is shown:



□	☆	Name	Model	IP	Department	Locatio
□	☆	SN00916-test-QAbbbaa	SN9116CO			
□	☆	sn1148-test-145	SN9116			

You can click the ✕ 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:

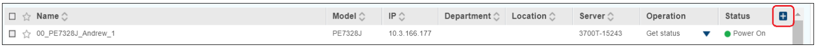


Click the search options (multiple selections available) to check the category(s) you wish to search for. For the example shown here, you can check *Model*, *Location*, and enter something in the blank field to search for something in the *Model* and *Location* categories.

Table Headings

Click the table column headings to sort the display priority.

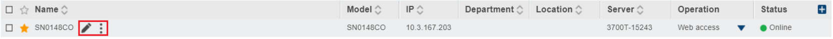
Note: The headings at the top of the table don't all appear for each view. Click the + icon to select the headings you wish to view.



□	☆	Name	Model	IP	Department	Location	Server	Operation	Status
□	☆	00_PE7328J_Andrew_1	PE7328J	10.3.166.177			3700T-15243	Get status ▼	● Power On

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:

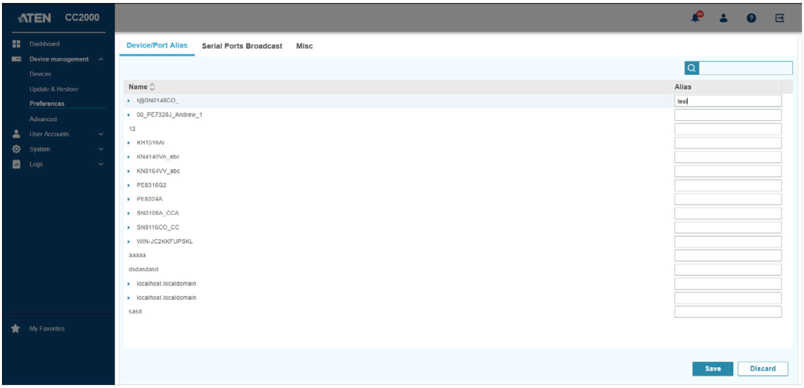


□	☆	Name	Model	IP	Department	Location	Server	Operation	Status
□	★	SN0148CO	SN0148CO	10.3.167.203			3700T-15243	Web access ▼	● Online

Click one of the icons for a drop-down menu and click to select what you wish to configure.

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.



Name	Alias
!@SN0148CO_	test
00_PE7328J_Andrew_1	
12	
KH1516Ai	
KN4140VA_abc	
KN8164VV_abc	
PE8316G2	
PE8324A	
SN0108A_CCA	
SN9116CO_CC	
WIN-JC2KKFUPSKL	
aaaaa	
dsdasdasd	
localhost.localdomain	
localhost.localdomain	
sasd	

This Page Intentionally Left Blank

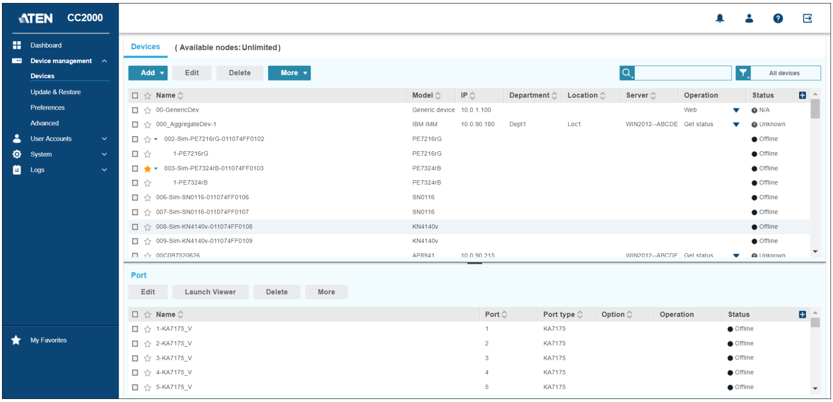
Chapter 5
Device Management

Overview

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

A *My Favorites* quick device access page is also available, see *My Favorites* on page 117.

Clicking *Device management* will bring you to the *Devices* submenu and its main panel as shown:



Name	Model	IP	Department	Location	Server	Operation	Status
00-GenericDev	Generic device	10.0.1.100				Web	N/A
000_AggregateDev-1	IBM IMM	10.0.90.180	Dept1	Loc1	WIN2012--ABCDE	Get status	Unknown
002-Sim-PE7216rG-011074FF0102	PE7216rG						Offline
1-PE7216rG	PE7216rG						Offline
003-Sim-PE7324rB-011074FF0103	PE7324rB						Offline
1-PE7324rB	PE7324rB						Offline
006-Sim-SN0116-011074FF0106	SN0116						Offline
007-Sim-SN0116-011074FF0107	SN0116						Offline
008-Sim-KN4140v-011074FF0108	KN4140v						Offline
009-Sim-KN4140v-011074FF0109	KN4140v						Offline
00C0B7520626	AP8941	10.0.90.215			WIN2012--ABCDE	Get status	Unknown

Name	Port	Port type	Option	Operation	Status
1-KA7175_V	1	KA7175			Offline
2-KA7175_V	2	KA7175			Offline
3-KA7175_V	3	KA7175			Offline
4-KA7175_V	4	KA7175			Offline
5-KA7175_V	5	KA7175			Offline

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.

Preliminary Procedures

Before devices can be managed, they must first be added into the system. This involves four basic steps:

1. Connecting the devices to the same network segment as the CC2000. You must do this for the Primary and each of the Secondaries.
2. Once the devices have been connected to the same network segment as the CC2000, 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 226), or with the *Initialize devices IP/Port* function in System Broadcast (see *System Broadcast* on page 114). Each of the Secondaries, then notifies the Primary of the devices connected to it.

Note: 1. 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.

2. Devices that already have been added to the CC2000 management system do not show in the list of available devices.

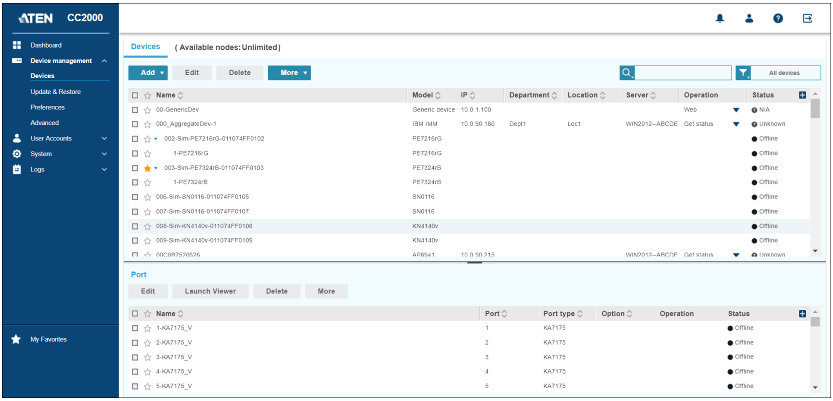
3. From the Primary CC2000 unit, the devices recognized in step 2 must be added to the CC2000's management system (see page 50).
4. Finally, devices can be created either as actual physical port devices (by unlocking each port), or by combining various ports into logical device constructs (Aggregate Devices, Group Devices, etc.). See *Adding an Aggregate Device*, page 68, 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 226) and keying in the IP address of the CC2000 Primary you want the device to be recognized by. See *VPNs*, page 227, for more details.

Devices

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



□	☆	Name	Model	IP	Department	Location	Server	Operation	Status
□	☆	00-GenericDev	Generic device	10.0.1.100				Web	N/A
□	☆	000_AggregateDev-1	IBM IMM	10.0.90.180	Dept1	Loc1	WIN2012--ABCDE	Get status	Unknown
□	☆	002-Sim-PE7216rG-011074FF0102	PE7216rG						● Offline
□	☆	1-PE7216rG	PE7216rG						● Offline
□	★	003-Sim-PE7324rB-011074FF0103	PE7324rB						● Offline
□	☆	1-PE7324rB	PE7324rB						● Offline
□	☆	006-Sim-SN0116-011074FF0106	SN0116						● Offline
□	☆	007-Sim-SN0116-011074FF0107	SN0116						● Offline
□	☆	008-Sim-KN4140v-011074FF0108	KN4140v						● Offline
□	☆	009-Sim-KN4140v-011074FF0109	KN4140v						● Offline
□	☆	00C0B7520626	AP8941	10.0.90.215			WIN2012--ABCDE	Get status	Unknown

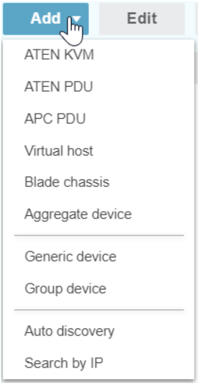
□	☆	Name	Port	Port type	Option	Operation	Status
□	☆	1-KA7175_V	1	KA7175			● Offline
□	☆	2-KA7175_V	2	KA7175			● Offline
□	☆	3-KA7175_V	3	KA7175			● Offline
□	☆	4-KA7175_V	4	KA7175			● Offline
□	☆	5-KA7175_V	5	KA7175			● Offline

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.

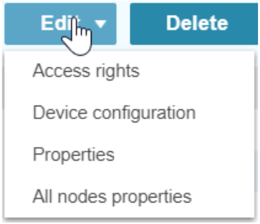
The lower screen is used to access and control the ports and outlets of the devices from the upper screen. Click to highlight a device in the upper screen to display its ports/outlets in the lower screen.

On the top left-hand corner are the general functions of this page.

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

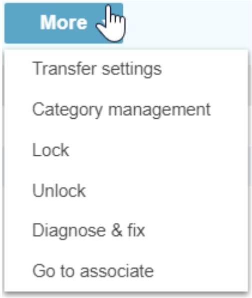


If you wish to edit a device, check the device and click *Edit* for a drop-down menu:



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

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



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

Type	Purpose
ATEN KVM	Select this type to add ATEN/Altusen KVM devices into the CC2000 management system. CC2000 supports CN, CS, 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 ATEN PDU*, page 54, for details. **Note:** When devices are added all of their ports are locked by default and must be unlocked. See *Transfer Settings*, page 86, 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 PDUs	Select this type to add PE Series Energy Intelligence PDUs into the CC2000 management system. The “PE series” here excludes ARM-based PE series products. If you want to add PE series products that are ARM-based see *Adding ATEN KVM*, page 50, for details.
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 57.
Aggregate Device	Select this to create a logical device consisting of ports selected from ATEN/Altusen devices and some SPMs (e.g. IPMI, HP iLO2, HP iLO3, HP iLO5, IBM RSA II, Dell DRAC 5, Dell iDRAC 6, Dell iDRAC 8) 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 68, 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.
Generic Device	Third party generic devices (routers, switches, etc.) can consist of any device that contains an Ethernet interface and can be accessed by its URL or IP Address via HTTP/HTTPS, or Telnet/SSH. Since these devices have no provision for CC management, they cannot be authenticated through the 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 229) 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.

Type	Purpose
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/ Altusen 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 with any other Aggregate Device – whereas a physical port can be added to any number of Group Devices **Note:** 1. Group Devices do not count against the number of licensed nodes. 2. A physical port that is added to more than one Group Device only counts as one license no matter 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 97.

Table Headings

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

Device Column Headings

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 displays here.
MAC Address	For physical devices – the device's MAC Address displays here.
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 90.
Type	The type category of the device.

Heading	Explanation
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.

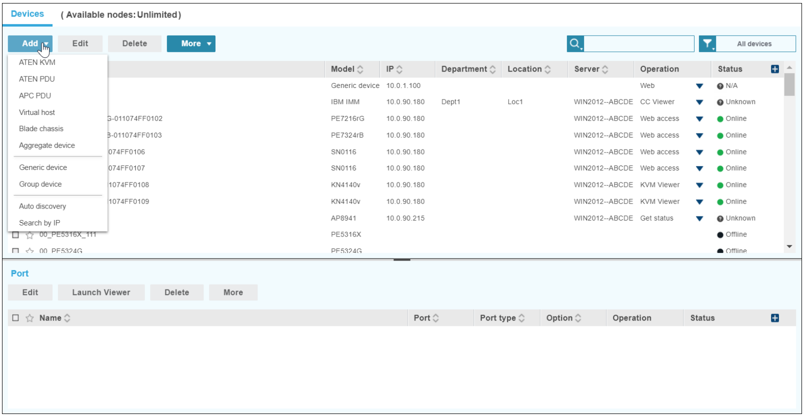
Port Column Headings

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.

Adding Device

Follow the steps below to add a device.

1. Click **Add** for a drop-down menu:



	Model	IP	Department	Location	Server	Operation	Status
	Generic device	10.0.1.100				Web	N/A
	IBM IMM	10.0.90.180	Dept1	Loc1	WIN2012--ABCDE	CC Viewer	Unknown
G-011074FF0102	PE7216rG	10.0.90.180			WIN2012--ABCDE	Web access	● Online
B-011074FF0103	PE7324rB	10.0.90.180			WIN2012--ABCDE	Web access	● Online
074FF0106	SN0116	10.0.90.180			WIN2012--ABCDE	Web access	● Online
074FF0107	SN0116	10.0.90.180			WIN2012--ABCDE	Web access	● Online
1074FF0108	KN4140v	10.0.90.180			WIN2012--ABCDE	KVM Viewer	● Online
1074FF0109	KN4140v	10.0.90.180			WIN2012--ABCDE	KVM Viewer	● Online
	AP8941	10.0.90.215			WIN2012--ABCDE	Get status	Unknown
00_PE5316X_111	PE5316X						● Offline
00_PE5324G	PE5324G						● Offline

□ ☆ Name	Port	Port type	Option	Operation	Status

2. Click to select the type of device you would like to add from the list. A window will pop-up to add the device. The interface of the window depends on your selection.

The sections that follow describe the procedures involved for setting up each of the devices listed.

Adding ATEN KVM

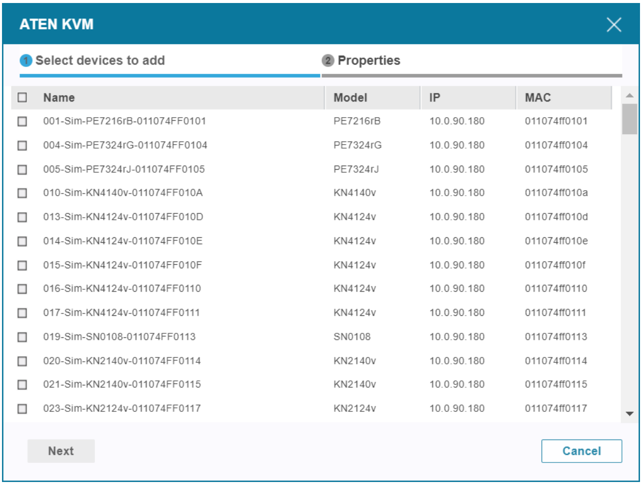
This item refers to adding Aten KVM device into the CC2000 management system. CC2000 supports CN, CS, KH, KL, KN, PN, SN and PE series devices. The “PE series” here only refers to the ARM-based products.

If you want to add PE series products that are not ARM-based see *Adding ATEN PDU*, page 54, 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 44, for details.

To add an Aten KVM,

1. Select *ATEN KVM* from the drop-down menu, a window will pop-up listing all the online devices that can be added:



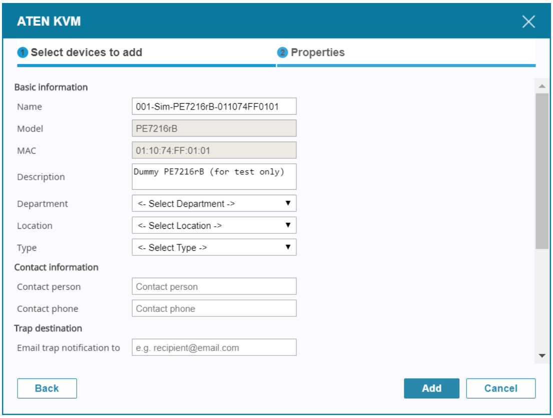
ATEN KVM

□	Name	Model	IP	MAC
□	001-Sim-PE7216rB-011074FF0101	PE7216rB	10.0.90.180	011074ff0101
□	004-Sim-PE7324rG-011074FF0104	PE7324rG	10.0.90.180	011074ff0104
□	005-Sim-PE7324rJ-011074FF0105	PE7324rJ	10.0.90.180	011074ff0105
□	010-Sim-KN4140v-011074FF010A	KN4140v	10.0.90.180	011074ff010a
□	013-Sim-KN4124v-011074FF010D	KN4124v	10.0.90.180	011074ff010d
□	014-Sim-KN4124v-011074FF010E	KN4124v	10.0.90.180	011074ff010e
□	015-Sim-KN4124v-011074FF010F	KN4124v	10.0.90.180	011074ff010f
□	016-Sim-KN4124v-011074FF0110	KN4124v	10.0.90.180	011074ff0110
□	017-Sim-KN4124v-011074FF0111	KN4124v	10.0.90.180	011074ff0111
□	019-Sim-SN0108-011074FF0113	SN0108	10.0.90.180	011074ff0113
□	020-Sim-KN2140v-011074FF0114	KN2140v	10.0.90.180	011074ff0114
□	021-Sim-KN2140v-011074FF0115	KN2140v	10.0.90.180	011074ff0115
□	023-Sim-KN2124v-011074FF0117	KN2124v	10.0.90.180	011074ff0117

For information about **Restrictions** or **CC2000 Options**, see *Restrictions*, page 52 or *CC2000 Options*, page 53.

2. Click to check the checkbox of the device you wish to add.

3. Click **Next** for the Properties page:



ATEN KVM

Basic information

Name	001-Sim-PE7216rB-011074FF0101
Model	PE7216rB
MAC	01:10:74:FF:01:01
Description	Dummy PE7216rB (for test only)
Department	<- Select Department -> ▾
Location	<- Select Location -> ▾
Type	<- Select Type -> ▾

Contact information

Contact person	Contact person
Contact phone	Contact phone

Trap destination

Email trap notification to	e.g. recipient@email.com

4. 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. 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 displays 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 87), 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 87), and click on the one you want the device to belong to. **Type:** For organizational purposes you can specify the type of device that this is. If you wish to do so, drop down the list of types (you have previously created – see *Category Management* on page 87), 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	The name and telephone number of the device administrator. These fields are optional.
Trap Destination	The email address of the person you want to receive trap notifications. This field is optional.
Restrictions	**Hide IP Address from general users:** As an added security measure, if this feature is enabled, it keeps 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 keeps the device's MAC address from appearing in the Device List when users log in via their browser.

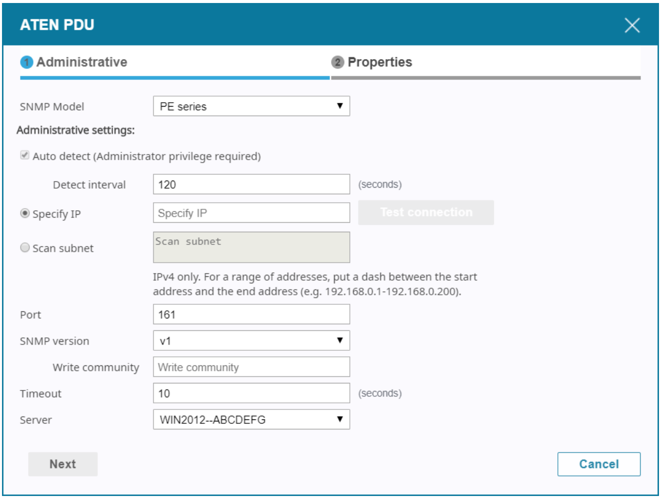
Field	Information
CC2000 Options	**Allow users to access the device through viewer or its web login page:** As an added security measure, if this feature is not enabled, the device will only accept logins through the CC2000. While the device is connected to the CC2000 system, users cannot log in to the 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 not time out.

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

Note: For Cat5 KVM switches, only the ports that are have a KVM adapter cable attached and are online are 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.

Adding ATEN PDU

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



ATEN PDU

1 Administrative

2 Properties

SNMP Model: PE series

Administrative settings:

☑ Auto detect (Administrator privilege required)

Detect interval: 120 (seconds)

● Specify IP: Specify IP

○ Scan subnet: Scan subnet

IPv4 only. For a range of addresses, put a dash between the start address and the end address (e.g. 192.168.0.1-192.168.0.200).

Port: 161

SNMP version: v1

Write community: Write community

Timeout: 10 (seconds)

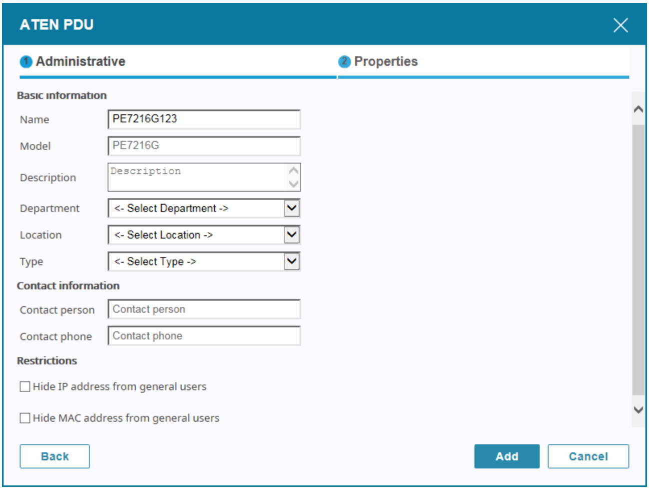
Server: WIN2012--ABCDEFG

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

Field	Information
SNMP Model	The “PE series” here refers to Energy Intelligence PDUs that are not ARM-based products. **Note:** To add PE series ARM-based products see *Adding ATEN KVM*, page 50, for details.
Auto detect	Enable this function to allow the system to automatically check if the device is online. Only a user with administrator privileges can enable this function.
Detect interval	Set the detect interval by entering a value between 30 and 300 seconds. This sets how often the system automatically checks that the device is online.
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.

Field	Information
Timeout	Key in the server timeout value. The range is between 10 and 120.
Server	Select the server to use.

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



Basic information

Name: PE7216G123

Model: PE7216G

Description: Description

Department: <- Select Department ->

Location: <- Select Location ->

Type: <- Select Type ->

Contact information

Contact person: Contact person

Contact phone: Contact phone

Restrictions

□ Hide IP address from general users

□ Hide MAC address from general users

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 purpose you can establish department categories (R&D, for example), and assign devices to them (see *Category Management* on page 87). 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 87). 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.

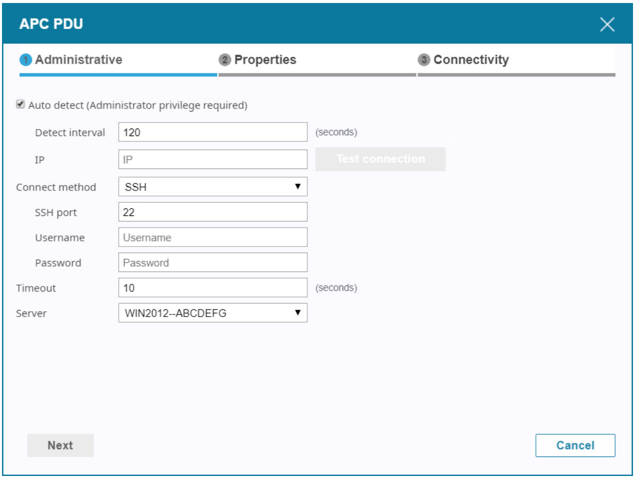
Field	Information
Contact Information	Enter the name and telephone number of the administrator. These fields are optional.
Restrictions	**Hide IP Address from general users:** As an added security measure, if this feature is enabled, it keeps the device's IP address from appearing in the Device List when users log in via their browser. **Hide MAC Address from general users:** As an added security measure, if this feature is enabled, it keeps 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 **Add**.

Note: After adding a device, its ports are locked. See *Locking / Unlocking Devices*, page 88.

Adding an APC PDU

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



APC PDU

1 Administrative 2 Properties 3 Connectivity

☑ Auto detect (Administrator privilege required)

Detect interval: 120 (seconds)

IP: IP

Connect method: SSH

SSH port: 22

Username: Username

Password: Password

Timeout: 10 (seconds)

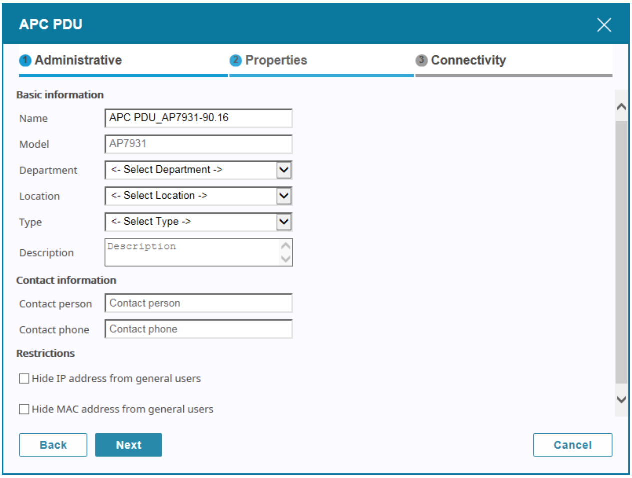
Server: WIN2012--ABCDEFG

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	If you are adding one of the specifically mentioned types and enable Auto detect, the CC2000 will check if the device is online. 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 automatically checks that the APC PDU is online.
IP	Key in the APC PDUs 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 cancelling 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.



APC PDU

Basic information

Name: APC PDU_AP7931-90.16

Model: AP7931

Department: <- Select Department ->

Location: <- Select Location ->

Type: <- Select Type ->

Description: Description

Contact information

Contact person: Contact person

Contact phone: Contact phone

Restrictions

□ Hide IP address from general users

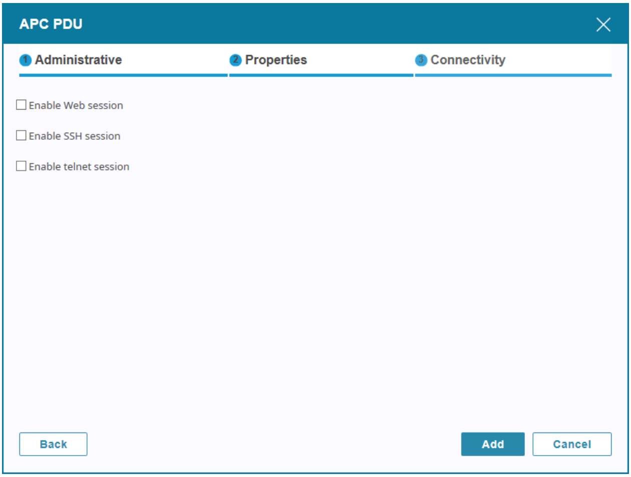
□ Hide MAC address from general users

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 87). 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 87). 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	The name and telephone number of the device administrator. These fields are optional.

Field	Information
Restrictions	**Hide IP Address from general users:** As an added security measure, if this feature is enabled, it keeps 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 keeps 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 Properties page appears. Check to enable web / SSH / Telnet sessions.


APC PDU

☐ Enable Web session

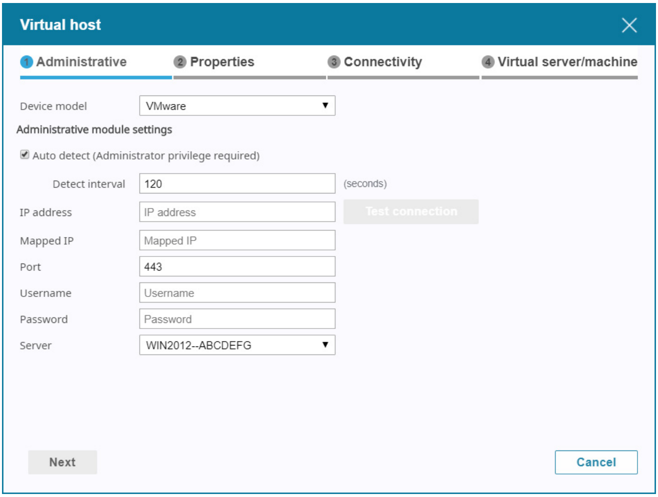
☐ Enable SSH session

☐ Enable telnet session

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.



Device model: VMware ▾

Administrative module settings

☑ Auto detect (Administrator privilege required)

Detect interval: 120 (seconds)

IP address: IP address

Mapped IP: Mapped IP

Port: 443

Username: Username

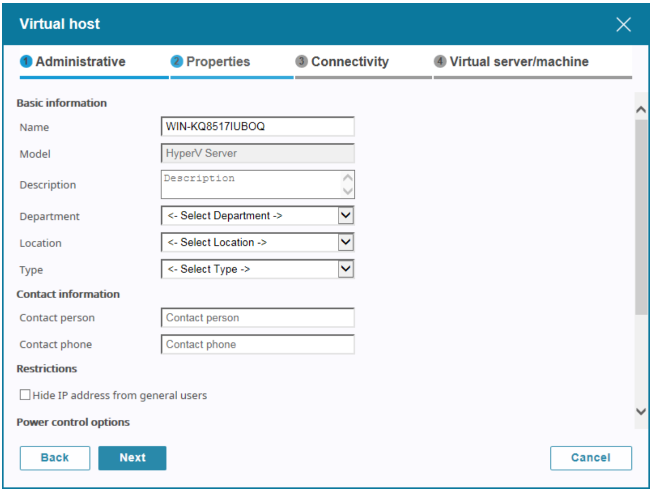
Password: Password

Server: WIN2012--ABCDEFG ▾

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.
Auto Detect	Enable this function so the system automatically checks that the virtual machine is online. 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 automatically checks that the virtual machine is online.
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.



Virtual host

1 Administrative — 2 Properties — 3 Connectivity — 4 Virtual server/machine

Basic information

Name: WIN-KQ8517IUBOQ

Model: HyperV Server

Description: Description

Department: <- Select Department ->

Location: <- Select Location ->

Type: <- Select Type ->

Contact information

Contact person: Contact person

Contact phone: Contact phone

Restrictions

□ Hide IP address from general users

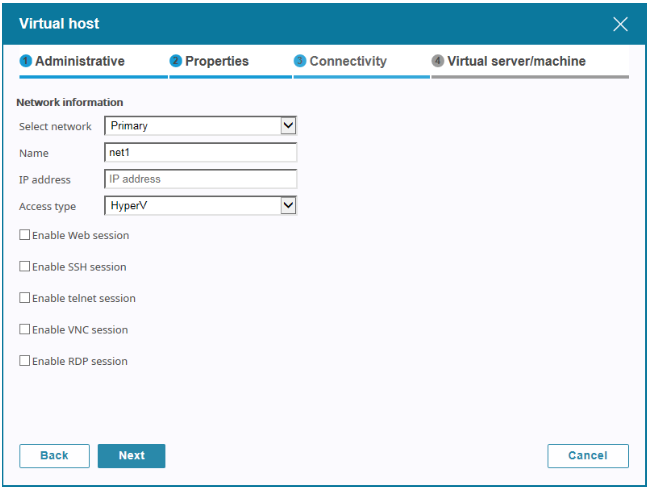
Power control options

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 87). 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 87). 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	The name and telephone number of the device administrator. These fields are optional.

Field	Information
Restrictions	**Hide IP Address from general users:** As an added security measure, if this feature is enabled, it keeps 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 keeps 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.



Virtual host

Network information

Select network: Primary

Name: net1

IP address: IP address

Access type: HyperV

□ Enable Web session

□ Enable SSH session

□ Enable telnet session

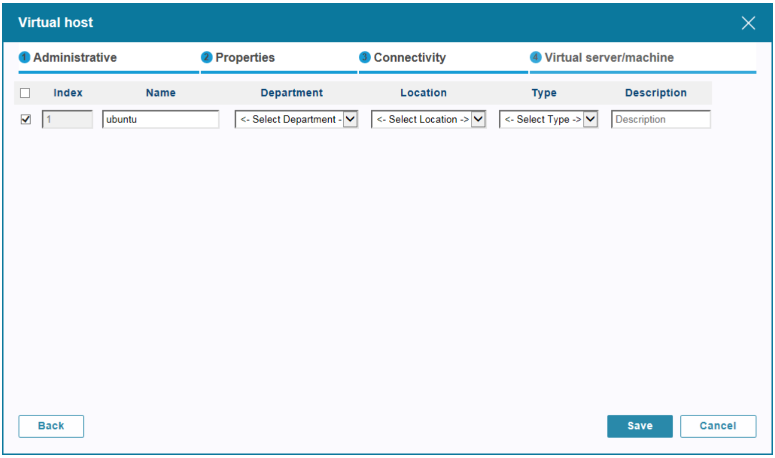
□ Enable VNC session

□ Enable RDP session

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.

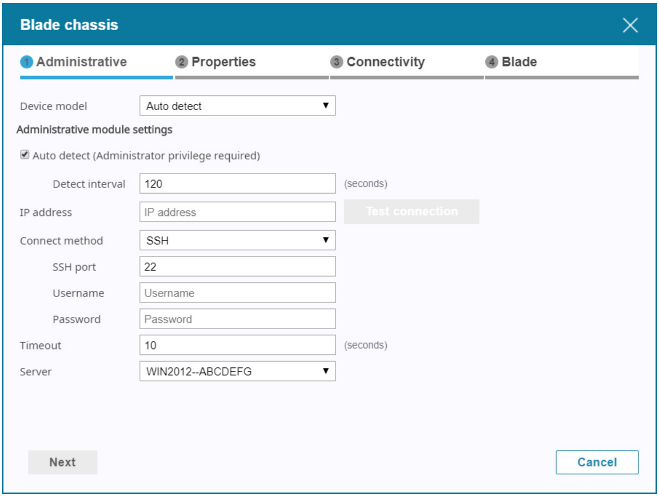


□	Index	Name	Department	Location	Type	Description
☑	1	ubuntu	<- Select Department -	<- Select Location ->	<- Select Type ->	Description

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:



Device model: Auto detect

Administrative module settings

☑ Auto detect (Administrator privilege required)

Detect interval: 120 (seconds)

IP address: IP address

Connect method: SSH

SSH port: 22

Username: Username

Password: Password

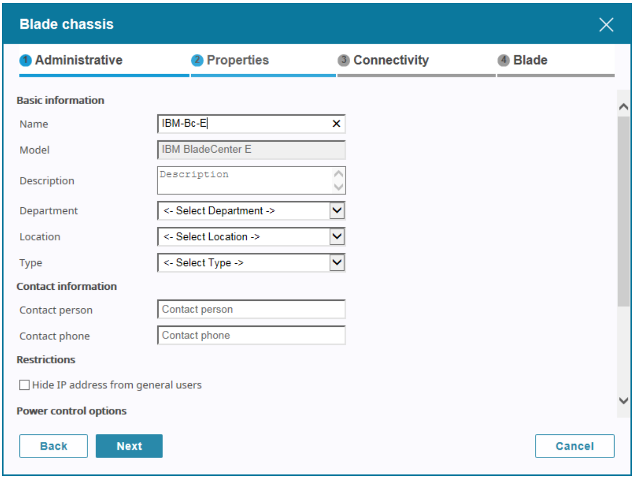
Timeout: 10 (seconds)

Server: WIN2012--ABCDEFG

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	If you are adding one of the specifically mentioned Blade chassis Model types and enable Auto detect, the CC2000 will check if the device is online. 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 automatically checks that the blade server is online.
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.



Basic information

Name: IBM-Bc-E

Model: IBM BladeCenter E

Description: Description

Department: <- Select Department ->

Location: <- Select Location ->

Type: <- Select Type ->

Contact information

Contact person: Contact person

Contact phone: Contact phone

Restrictions

□ Hide IP address from general users

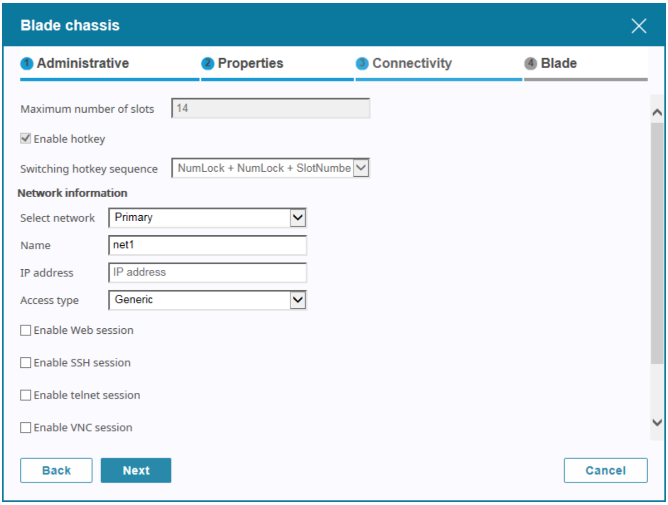
Power control options

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 87). 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 87). 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	The name and telephone number of the device administrator. These fields are optional.

Field	Information
Restrictions	**Hide IP Address from general users:** As an added security measure, if this feature is enabled, it keeps 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 keeps 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.



Blade chassis

Maximum number of slots 14

☑ Enable hotkey

Switching hotkey sequence NumLock + NumLock + SlotNumbe

Network information

Select network Primary

Name net1

IP address IP address

Access type Generic

□ Enable Web session

□ Enable SSH session

□ Enable telnet session

□ Enable VNC session

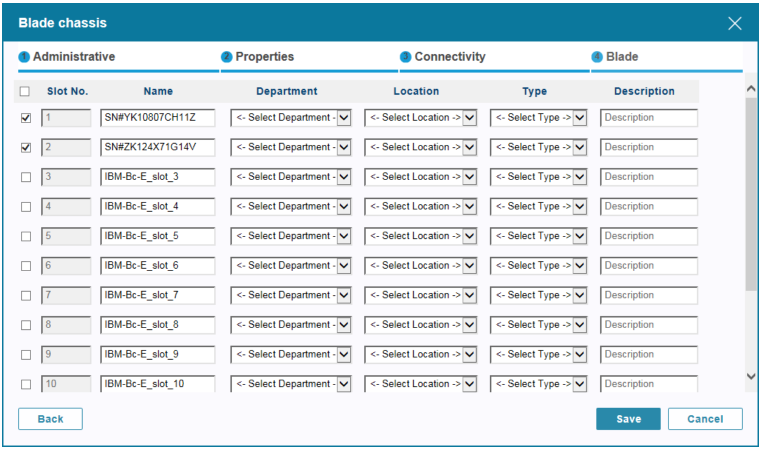
5. Fill in the fields according to the information in the table below:

   - 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.



Blade chassis

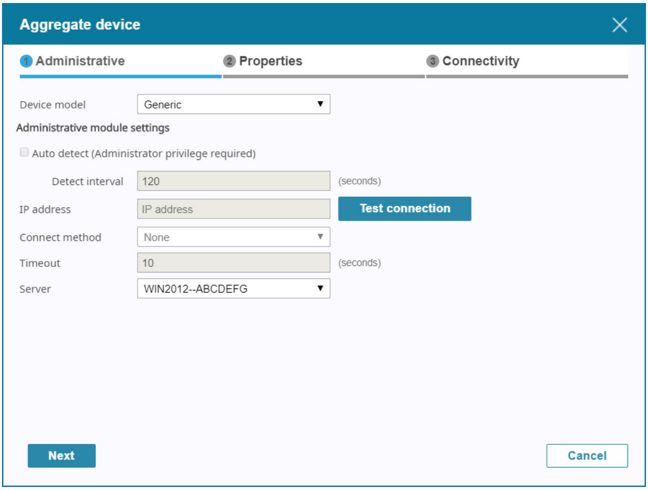
□	Slot No.	Name	Department	Location	Type	Description
☑	1	SN#YK10807CH11Z	<- Select Department -	<- Select Location ->	<- Select Type ->	Description
☑	2	SN#ZK124X71G14V	<- Select Department -	<- Select Location ->	<- Select Type ->	Description
□	3	IBM-Bc-E_slot_3	<- Select Department -	<- Select Location ->	<- Select Type ->	Description
□	4	IBM-Bc-E_slot_4	<- Select Department -	<- Select Location ->	<- Select Type ->	Description
□	5	IBM-Bc-E_slot_5	<- Select Department -	<- Select Location ->	<- Select Type ->	Description
□	6	IBM-Bc-E_slot_6	<- Select Department -	<- Select Location ->	<- Select Type ->	Description
□	7	IBM-Bc-E_slot_7	<- Select Department -	<- Select Location ->	<- Select Type ->	Description
□	8	IBM-Bc-E_slot_8	<- Select Department -	<- Select Location ->	<- Select Type ->	Description
□	9	IBM-Bc-E_slot_9	<- Select Department -	<- Select Location ->	<- Select Type ->	Description
□	10	IBM-Bc-E_slot_10	<- Select Department -	<- Select Location ->	<- Select Type ->	Description

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:



Aggregate device

1 Administrative | 2 Properties | 3 Connectivity

Device model: Generic

Administrative module settings

□ Auto detect (Administrator privilege required)

Detect interval: 120 (seconds)

IP address: IP address

Connect method: None

Timeout: 10 (seconds)

Server: WIN2012--ABCDEFG

Note: See *Aggregate Device*, page 47, for further details.

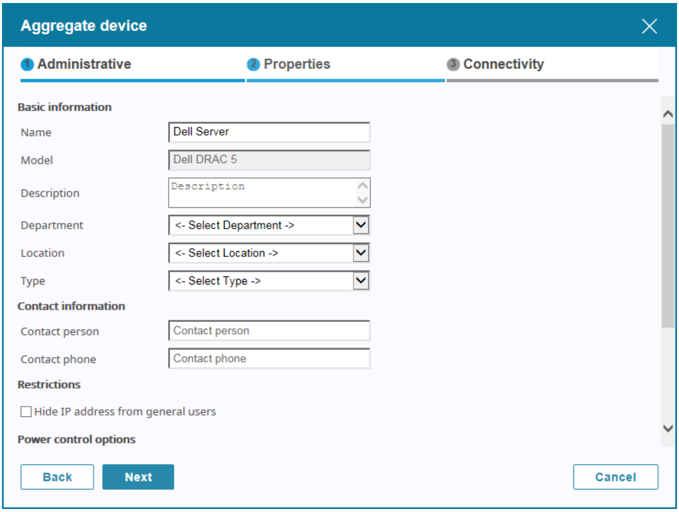
Follow the steps below to add an Aggregate Device.

1. Select the Aggregate Device Model from the drop-down menu and fill in the fields according to the information provided in the table below:

Field	Information
Auto Detect	If you are adding one of the specifically mentioned Aggregate Device Model types and enable Auto detect, the CC2000 will check if the device is online. 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 automatically checks that the Aggregate Device is online.
IP	Key in the Aggregate Device'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.
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 Aggregate Device.

Field	Information
Login name field / password field	Key in the information so the CC2000 knows where to put the login name and password information under certain single sign-on situations
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 you have finished with this page, click **Next**. The Properties page appears.



Aggregate device

Basic information

Name: Dell Server

Model: Dell DRAC 5

Description: Description

Department: <- Select Department ->

Location: <- Select Location ->

Type: <- Select Type ->

Contact information

Contact person: Contact person

Contact phone: Contact phone

Restrictions

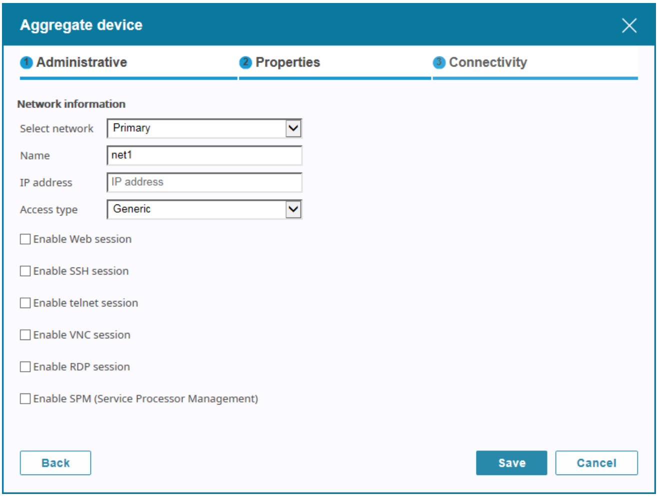
□ Hide IP address from general users

Power control options

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 87). 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 87). 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	The name and telephone number of the device administrator. These fields are optional.
Restrictions	**Hide IP Address from general users:** As an added security measure, if this feature is enabled, it keeps 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 keeps 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.



Aggregate device

1 Administrative
2 Properties
3 Connectivity

Network information

Select network: Primary

Name: net1

IP address: IP address

Access type: Generic

□ Enable Web session

□ Enable SSH session

□ Enable telnet session

□ Enable VNC session

□ Enable RDP session

□ Enable SPM (Service Processor Management)

Back | Save | Cancel

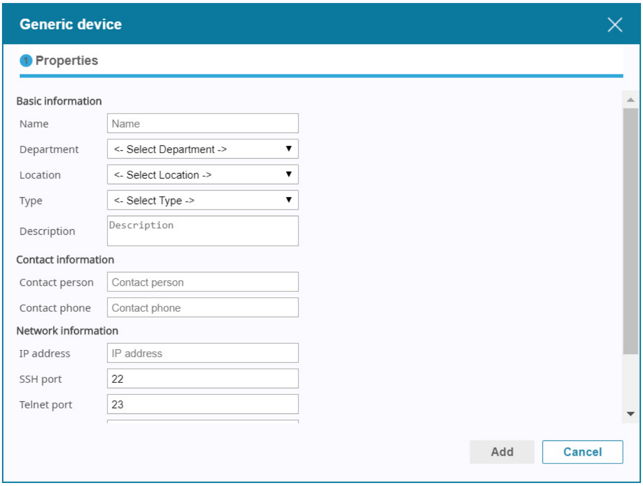
5. Fill in the fields according to the information in the table below:

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.
Sessions	Check to enable the sessions.

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

Adding a Generic Device

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



Note: See *Generic Device*, page 47, for an explanation of generic devices.

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

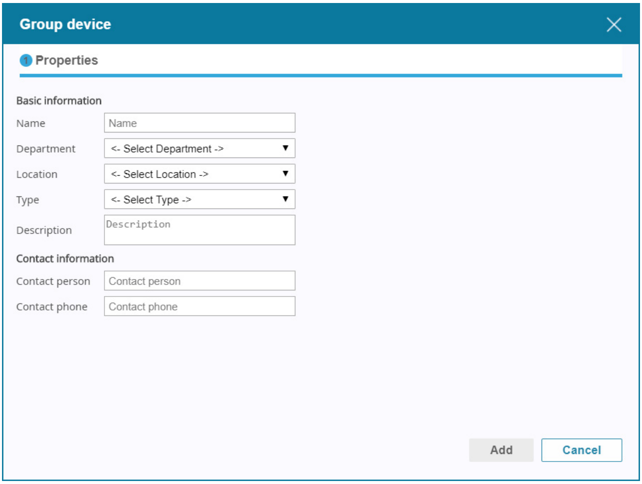
Field	Information
Basic Information	**Name:** Provide a name to identify the device. **Department:** For organizational purposes you can establish department categories (R&D, for example), and assign devices to them (see *Category Management* on page 87). If you wish to assign this device to a department, 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 87). 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	The name and telephone number of the device administrator. These fields are optional.

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:



Group device

Properties

Basic information

Name	Name
Department	<- Select Department ->
Location	<- Select Location ->
Type	<- Select Type ->
Description	Description

Contact information

Contact person	Contact person
Contact phone	Contact phone

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 87). 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 87). 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	The name and telephone number of the device administrator. These fields are optional.

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

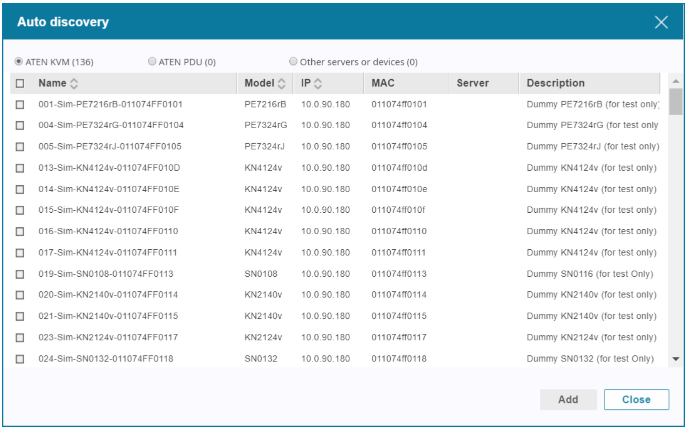
Note: 1. Refer back to *Group Device*, page 48, for an explanation of the differences between Aggregate and Group devices.

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:



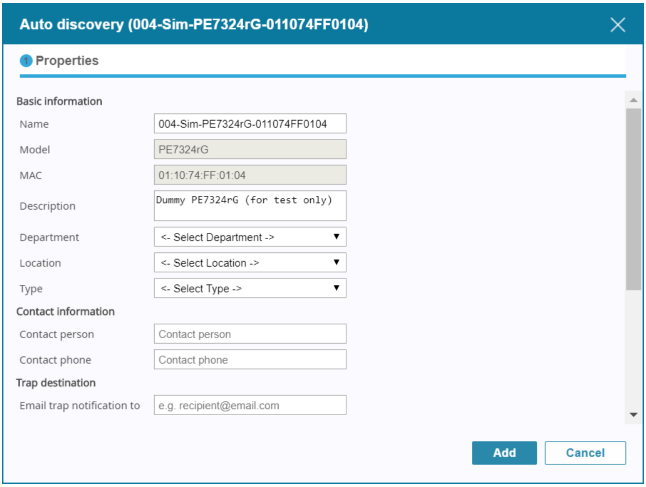
Auto discovery

● ATEN KVM (136) ○ ATEN PDU (0) ○ Other servers or devices (0)

□	Name	Model	IP	MAC	Server	Description
□	001-Sim-PE7216rB-011074FF0101	PE7216rB	10.0.90.180	011074ff0101		Dummy PE7216rB (for test only
□	004-Sim-PE7324rG-011074FF0104	PE7324rG	10.0.90.180	011074ff0104		Dummy PE7324rG (for test only
□	005-Sim-PE7324rJ-011074FF0105	PE7324rJ	10.0.90.180	011074ff0105		Dummy PE7324rJ (for test only)
□	013-Sim-KN4124v-011074FF010D	KN4124v	10.0.90.180	011074ff010d		Dummy KN4124v (for test only)
□	014-Sim-KN4124v-011074FF010E	KN4124v	10.0.90.180	011074ff010e		Dummy KN4124v (for test only)
□	015-Sim-KN4124v-011074FF010F	KN4124v	10.0.90.180	011074ff010f		Dummy KN4124v (for test only)
□	016-Sim-KN4124v-011074FF0110	KN4124v	10.0.90.180	011074ff0110		Dummy KN4124v (for test only)
□	017-Sim-KN4124v-011074FF0111	KN4124v	10.0.90.180	011074ff0111		Dummy KN4124v (for test only)
□	019-Sim-SN0108-011074FF0113	SN0108	10.0.90.180	011074ff0113		Dummy SN0116 (for test Only)
□	020-Sim-KN2140v-011074FF0114	KN2140v	10.0.90.180	011074ff0114		Dummy KN2140v (for test only)
□	021-Sim-KN2140v-011074FF0115	KN2140v	10.0.90.180	011074ff0115		Dummy KN2140v (for test only)
□	023-Sim-KN2124v-011074FF0117	KN2124v	10.0.90.180	011074ff0117		Dummy KN2124v (for test only)
□	024-Sim-SN0132-011074FF0118	SN0132	10.0.90.180	011074ff0118		Dummy SN0132 (for test Only)

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**.



Auto discovery (004-Sim-PE7324rG-011074FF0104)

Properties

Basic information

Name	004-Sim-PE7324rG-011074FF0104
Model	PE7324rG
MAC	01:10:74:FF:01:04
Description	Dummy PE7324rG (for test only)
Department	<- Select Department ->
Location	<- Select Location ->
Type	<- Select Type ->

Contact information

Contact person	Contact person
Contact phone	Contact phone

Trap destination

Email trap notification to	e.g. recipient@email.com

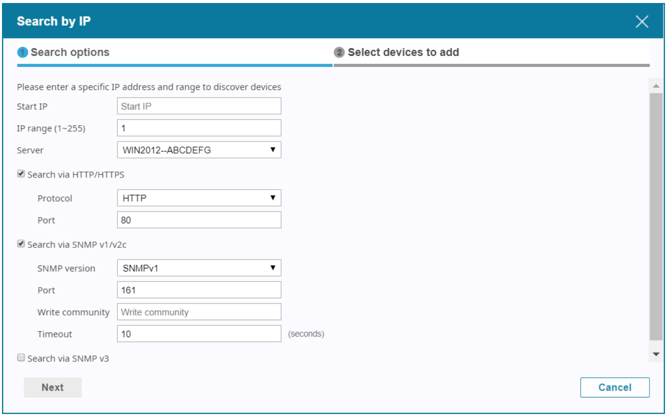
Fill in the Properties fields and click **Add**.

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:



Please enter a specific IP address and range to discover devices

Start IP: Start IP

IP range (1~255): 1

Server: WIN2012--ABCDEFG

☑ Search via HTTP/HTTPS

Protocol: HTTP

Port: 80

☑ Search via SNMP v1/v2c

SNMP version: SNMPv1

Port: 161

Write community: Write community

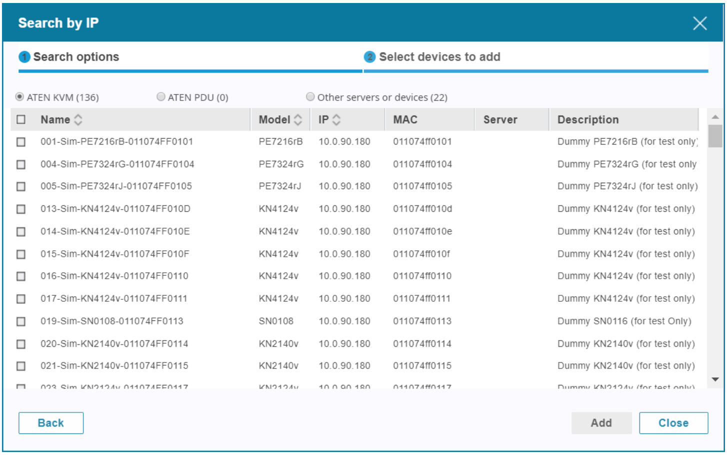
Timeout: 10 (seconds)

□ Search via SNMP v3

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 a search scope.
IP Range (1~255)	Enter a number (1~255) to set the end of a search scope.
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 what type of devices to display in the table (ATEN devices, ATEN PDUs or Other servers or devices):



Search by IP

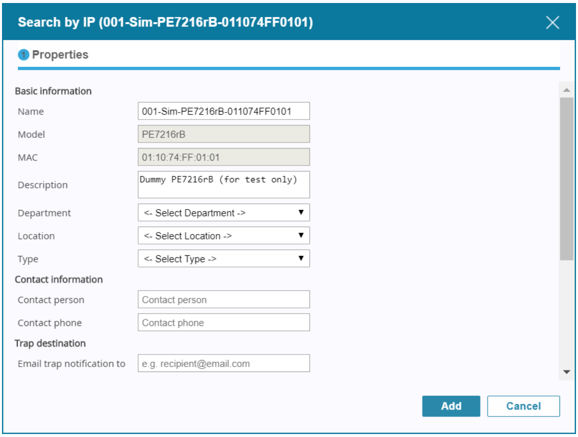
● ATEN KVM (136) ○ ATEN PDU (0) ○ Other servers or devices (22)

□	Name	Model	IP	MAC	Server	Description
□	001-Sim-PE7216rB-011074FF0101	PE7216rB	10.0.90.180	011074ff0101		Dummy PE7216rB (for test only)
□	004-Sim-PE7324rG-011074FF0104	PE7324rG	10.0.90.180	011074ff0104		Dummy PE7324rG (for test only
□	005-Sim-PE7324rJ-011074FF0105	PE7324rJ	10.0.90.180	011074ff0105		Dummy PE7324rJ (for test only)
□	013-Sim-KN4124v-011074FF010D	KN4124v	10.0.90.180	011074ff010d		Dummy KN4124v (for test only)
□	014-Sim-KN4124v-011074FF010E	KN4124v	10.0.90.180	011074ff010e		Dummy KN4124v (for test only)
□	015-Sim-KN4124v-011074FF010F	KN4124v	10.0.90.180	011074ff010f		Dummy KN4124v (for test only)
□	016-Sim-KN4124v-011074FF0110	KN4124v	10.0.90.180	011074ff0110		Dummy KN4124v (for test only)
□	017-Sim-KN4124v-011074FF0111	KN4124v	10.0.90.180	011074ff0111		Dummy KN4124v (for test only)
□	019-Sim-SN0108-011074FF0113	SN0108	10.0.90.180	011074ff0113		Dummy SN0116 (for test Only)
□	020-Sim-KN2140v-011074FF0114	KN2140v	10.0.90.180	011074ff0114		Dummy KN2140v (for test only)
□	021-Sim-KN2140v-011074FF0115	KN2140v	10.0.90.180	011074ff0115		Dummy KN2140v (for test only)
□	023-Sim-KN2124v-011074FF0117	KN2124v	10.0.90.180	011074ff0117		Dummy KN2124v (for test only)

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 checkbox of the device or server you would like to add and click **Add**.



Search by IP (001-Sim-PE7216rB-011074FF0101)

Basic information

Name	001-Sim-PE7216rB-011074FF0101
Model	PE7216rB
MAC	01:10:74:FF:01:01
Description	Dummy PE7216rB (for test only)
Department	<- Select Department -> ▾
Location	<- Select Location -> ▾
Type	<- Select Type -> ▾

Contact information

Contact person	Contact person
Contact phone	Contact phone

Trap destination

Email trap notification to	e.g. recipient@email.com

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

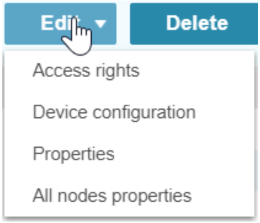
Refer to the sections above if you wish to modify any of the information fields.

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

Editing Devices

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

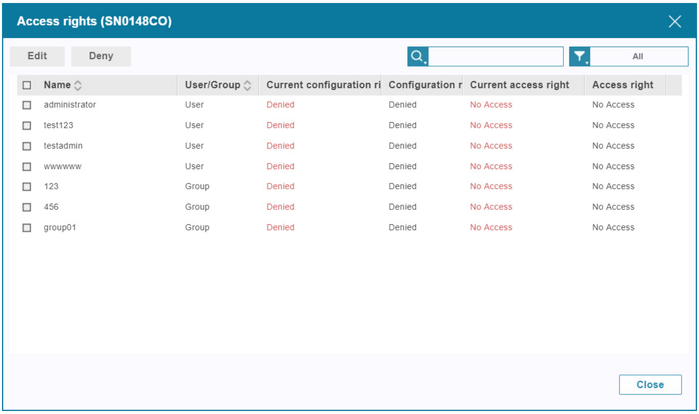
1. Check the device you wish to edit and click *Edit* for a drop-down menu:



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:



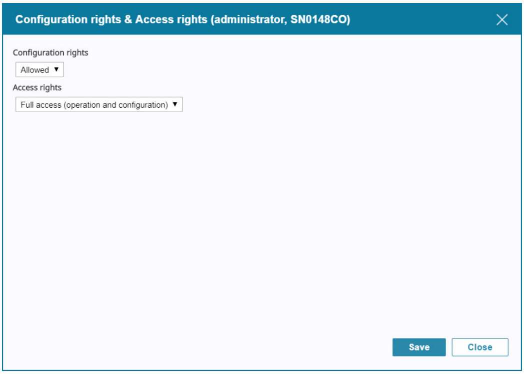
□	Name	User/Group	Current configuration ri	Configuration r	Current access right	Access right
□	administrator	User	Denied	Denied	No Access	No Access
□	test123	User	Denied	Denied	No Access	No Access
□	testadmin	User	Denied	Denied	No Access	No Access
□	wwwwww	User	Denied	Denied	No Access	No Access
□	123	Group	Denied	Denied	No Access	No Access
□	456	Group	Denied	Denied	No Access	No Access
□	group01	Group	Denied	Denied	No Access	No Access

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.

■ ATEN KVM

The options for Aten KVM devices is shown below:



Configuration rights & Access rights (administrator, SN0148CO)

Configuration rights: Allowed

Access rights: Full access (operation and configuration)

Set the configuration rights for the user or group:

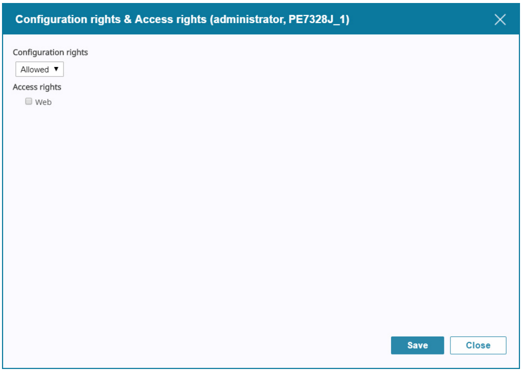
- **Allowed** – The user or group can configure the device's settings.
- **Denied** – The user or group cannot configure the device's settings.

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:



Configuration rights & Access rights (administrator, PE7328J_1)

Configuration rights: Allowed

Access rights

□ Web

Set the configuration rights for the user or group:

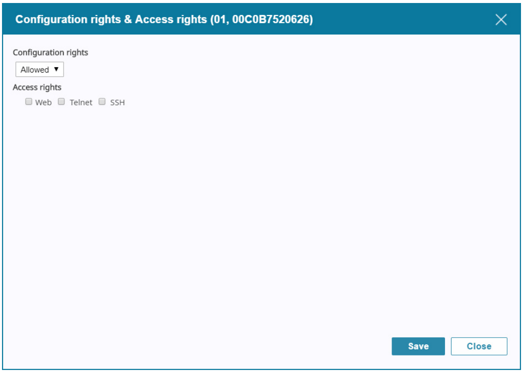
- **Allowed** – The user or group can configure the device's settings.
- **Denied** – The user or group cannot configure the device's settings.

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:



Configuration rights & Access rights (01, 00C0B7520626)

Configuration rights

Allowed ▾

Access rights

□ Web □ Telnet □ SSH

Set the configuration rights for the user or group:

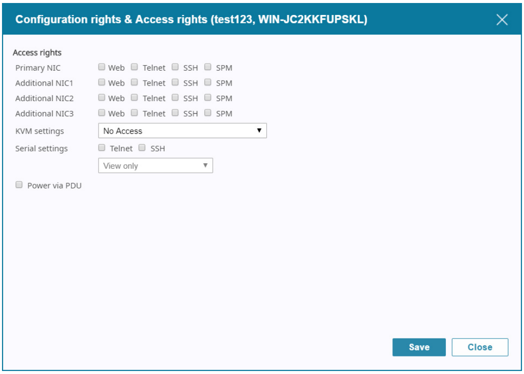
- **Allowed** – The user or group can configure the device's settings.
- **Denied** – The user or group cannot configure the device's settings.

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:



Configuration rights & Access rights (test123, WIN-JC2KKFUPSKL)

Access rights

Primary NIC □ Web □ Telnet □ SSH □ SPM

Additional NIC1 □ Web □ Telnet □ SSH □ SPM

Additional NIC2 □ Web □ Telnet □ SSH □ SPM

Additional NIC3 □ Web □ Telnet □ SSH □ SPM

KVM settings: No Access

Serial settings □ Telnet □ SSH

View only

□ Power via PDU

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

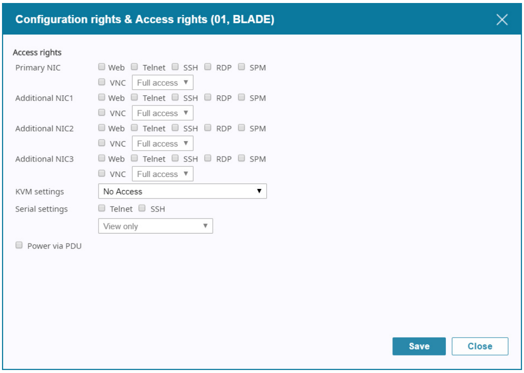
- **Primary NIC** – Specify the network protocol(s) for this NIC.
- **Additional NIC1** – Specify the network protocol(s) for this NIC
- **Additional NIC2** – Specify the network protocol(s) for this NIC.
- **Additional NIC3** – Specify the network protocol(s) for this NIC.
- **KVM settings** – Select 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:



Configuration rights & Access rights (01, BLADE)

Access rights

Primary NIC □ Web □ Telnet □ SSH □ RDP □ SPM
□ VNC Full access ▼

Additional NIC1 □ Web □ Telnet □ SSH □ RDP □ SPM
□ VNC Full access ▼

Additional NIC2 □ Web □ Telnet □ SSH □ RDP □ SPM
□ VNC Full access ▼

Additional NIC3 □ Web □ Telnet □ SSH □ RDP □ SPM
□ VNC Full access ▼

KVM settings No Access ▼

Serial settings □ Telnet □ SSH
View only ▼

□ Power via PDU

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

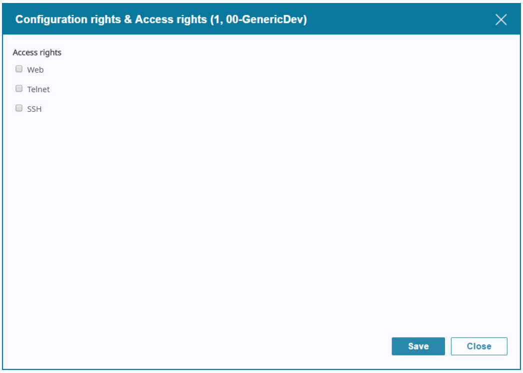
- **Primary NIC** – Specify the network protocol(s) for this NIC.
- **Additional NIC1** – Specify the network protocol(s) for this NIC
- **Additional NIC2** – Specify the network protocol(s) for this NIC.
- **Additional NIC3** – Specify the network protocol(s) for this NIC.
- **KVM settings** – Select 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.

■ Generic Device

The options for generic device is shown below:



Configuration rights & Access rights (1, 00-GenericDev)

Access rights

□ Web

□ Telnet

□ SSH

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 Configuration

To configure settings for a device, check the device checkbox and select **Device configuration**.

You will be redirected to the device’s configuration webpage.

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 Device* on page 50.

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

Follow the steps below to delete a device:

Check to select the device(s) and click **Delete**.

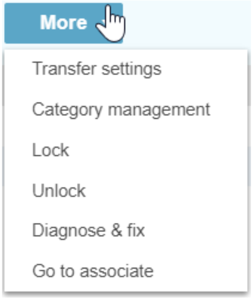
A confirmation message will pop up, click **Yes** to delete the device(s).

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:



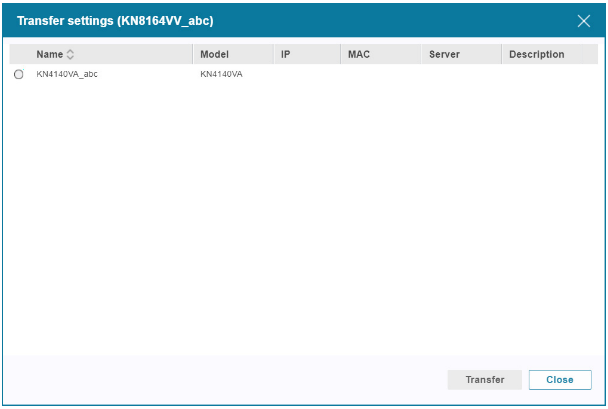
Note: You can also use the More icon ⋮ to access the More configuration options when you move your cursor over a user row.

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:



Transfer settings (KN8164VV_abc)

	Name	Model	IP	MAC	Server	Description
○	KN4140VA_abc	KN4140VA				

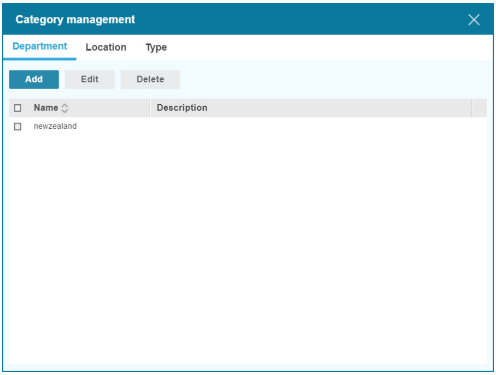
Choose a source device (e.g. device B) and click *Transfer* (bottom right-hand corner). A confirmation message will appear asking you to confirm the transfer. The CC2000 will transfer all device settings (excluding Device ID, model name and port number) and access rights of the source device (device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

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:

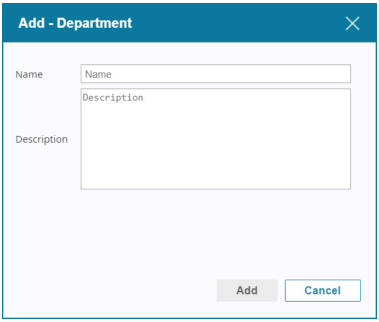
1. Click **More** and click to select **Category management**. A Category management page will pop up:



Category management

□ Name	Description
□ newzealand	

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



Add - Department

Name: Name
Description: Description

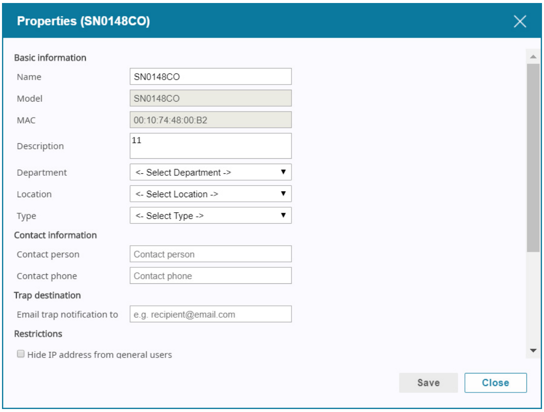
3. Fill in the Name and Description fields, and click **Add**.

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:



Properties (SN0148CO)

Basic information

Name	SN0148CO
Model	SN0148CO
MAC	00:10:74:48:00:B2
Description	11
Department	<- Select Department ->
Location	<- Select Location ->
Type	<- Select Type ->

Contact information

Contact person	Contact person
Contact phone	Contact phone

Trap destination

Email trap notification to	e.g. recipient@email.com

Restrictions

□ Hide IP address from general users

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

When physical devices are added to the CC2000 management system, their ports are locked by default – to make a port available, it must be unlocked.

Lock and **Unlock** allow you to lock and unlock all ports on the selected device. A locked port will have a lock icon 🔒 appearing in the last column of the lower screen (port) table. The unlocked ports will not have any icons.

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

Locking and unlocking individual ports are the same, except you operate in the lower screen.

Note: 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.

Operation

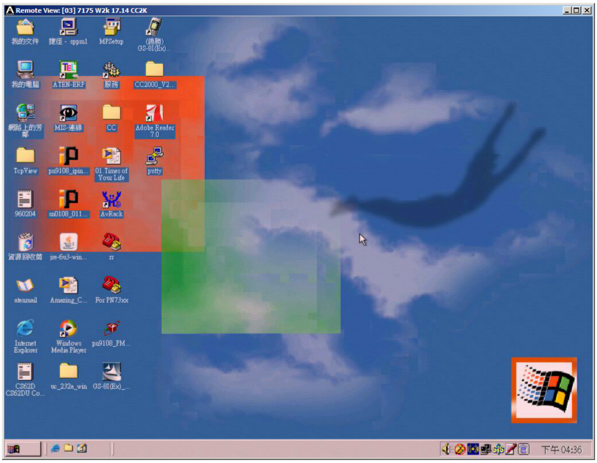
Depends on the selected device, various port operation methods are available for access and control. Click the arrow (drop-down menu) in the Operation column to select an operation method. These are explained in the following sections.

CC Viewer / KVM Viewer / SN Viewer

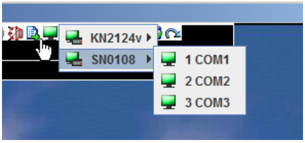
Clicking CC/KVM/SN Viewer from the drop-down menu opens viewer sessions directly to the ports of the selected device. The session opens a window with that device's port(s) on your desktop.

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:



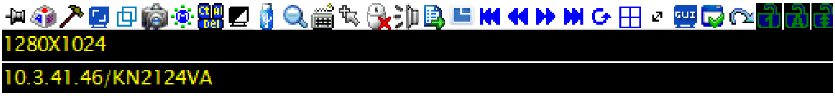
To switch ports in the viewer, open the hidden Control Panel (by hovering over the top center of the viewer window), and select the *Port List* icon. The port list choices include all the ports belonging to the device.



- 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

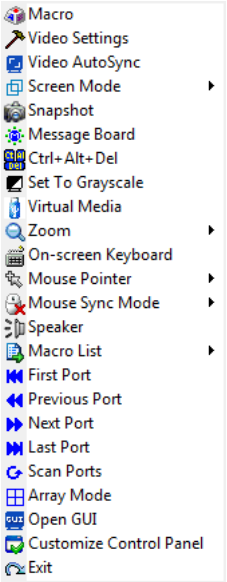
The Control Panel of the CC/KVM viewer is hidden in the upper (default) or lower center of the screen, and becomes visible when you mouse over it. The panel consists of three rows: an icon row at the top, and two text rows below it:



1280X1024

10.3.41.46/KN2124VA

- 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.

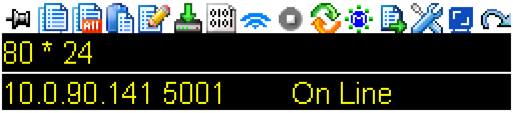
Icon	Function
📌	This is a toggle. Click to make the Control Panel persistent – i.e., it always displays on top of other screen elements. Click again to have it display normally.
🎲	Click to bring up the Macros dialog box (See the KVM device manual for more information).
🔨	Click to bring up the Video Options 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).
Ct Al Del	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.

🖱	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 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.
GUI	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).
↷	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 upper center 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:



80 * 24

10.0.90.141 5001 On Line

Control Panel Functions

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

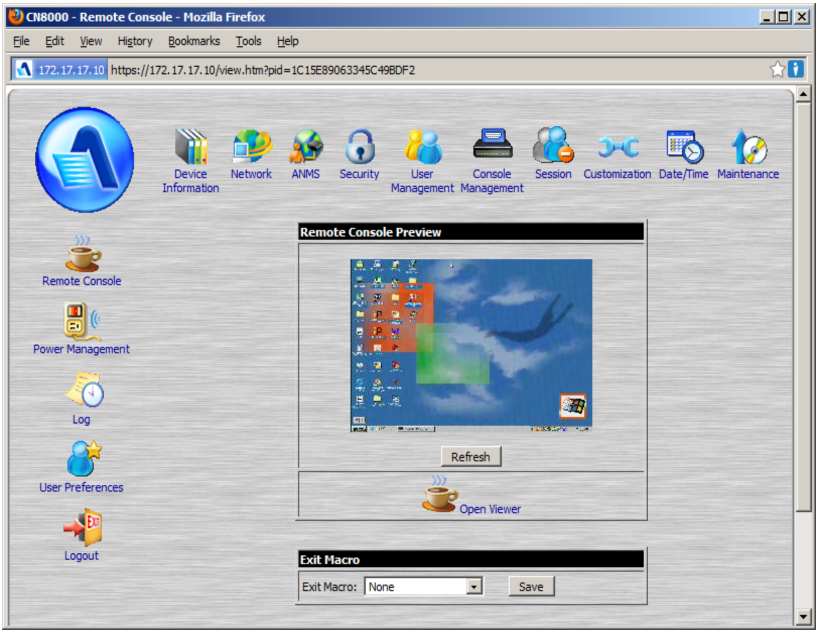
Icon	Function
📌	This is a toggle. Click to make the Control Panel appear *Always On Top* – i.e., always displays on top of the SNViewer screen. Click again to have it display in *Auto Hide* mode– allowing it to only appear when the mouse is moved over it.
📄	Use this to copy the selected text on the screen.
All	Use this to copy all text that is displayed on the screen.
📋	Use this to paste the copied text.

Icon	Function
📝	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).
0101 0101	Use this to change the page encoding (See the SN device manual for more information).
📶	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.
M	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.

Icon	Function
↷	Click to exit the viewer.

Web Access

Clicking Web Access opens a browser session for the device on your desktop just as if you had opened your browser and logged into from the URL bar:



172.17.17.10 https://172.17.17.10/view.htm?pid=1C15E89063345C49BDF2

Exit Macro: None

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.

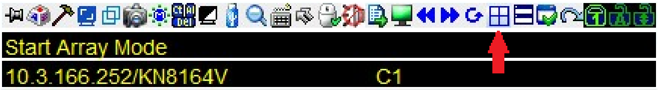
Note: The change doesn't show in the table until you leave the page and come back to it.

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

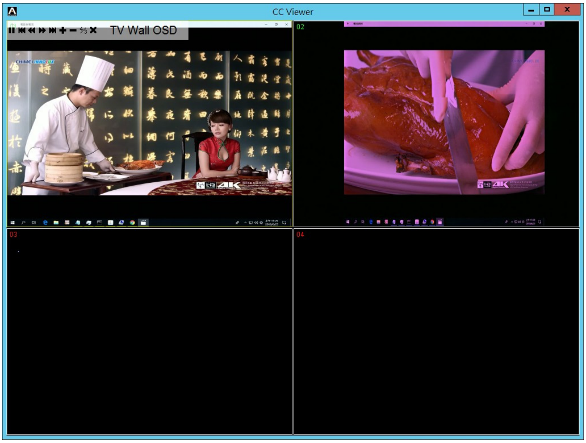
After you create a group device, you can launch panel array mode of the device by clicking the *CC Viewer* button (Operation column) and click the Start Panel Array icon in the control panel.



Start Array Mode

10.3.166.252/KN8164V C1

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

Ports

Ports and the configurations are displayed in the lower screen of the Device submenu. All the operations are the same as the device (upper screen), except that configurations are at the port level, and that it includes a **Launch Viewer** option.

Launch Viewer

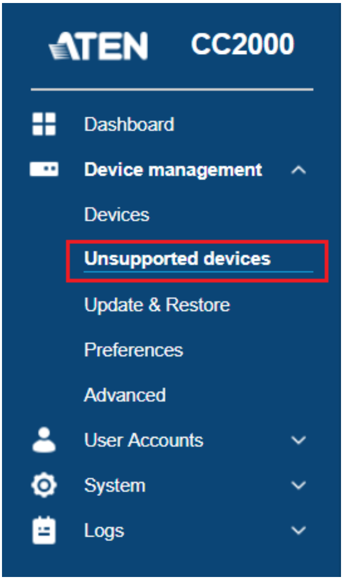
If you want to launch viewers to see the screen of the port, check the port and click **Launch Viewer**. The system will open the viewer in a new window (java or winclient).

Refer to *Operation* on page 90 for more information.

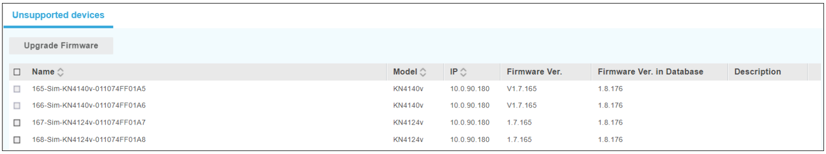
Unsupported Devices

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

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:



Unsupported devices

Upgrade Firmware

□	Name	Model	IP	Firmware Ver.	Firmware Ver. in Database	Description
□	165-Sim-KN4140v-011074FF01A5	KN4140v	10.0.90.180	V1.7.165	1.8.176	
□	166-Sim-KN4140v-011074FF01A6	KN4140v	10.0.90.180	V1.7.165	1.8.176	
□	167-Sim-KN4124v-011074FF01A7	KN4124v	10.0.90.180	1.7.165	1.8.176	
□	168-Sim-KN4124v-011074FF01A8	KN4124v	10.0.90.180	1.7.165	1.8.176	

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 104 on how to do this.

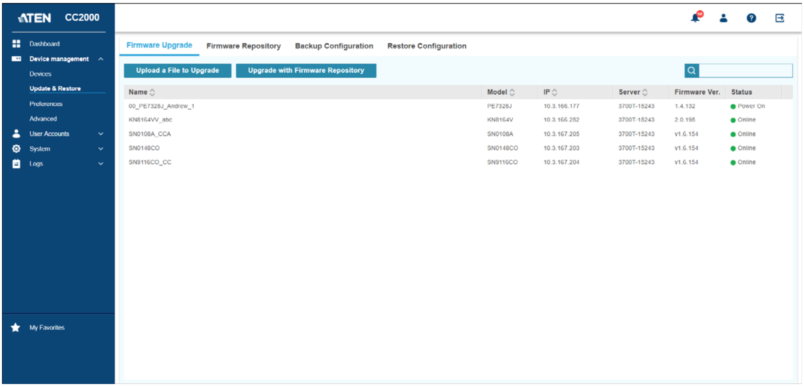
2. Once the device's firmware upgrade file is stored on the CC2000, its checkbox on this page becomes active. Check the checkbox.

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 backup files.



Name	Model	IP	Server	Firmware Ver.	Status
00_PE7328J_Andrew_1	PE7328J	10.3.166.177	3700T-15243	1.4.132	● Power On
KN8164VV_abc	KN8164V	10.3.166.252	3700T-15243	2.0.195	● Online
SN0108A_CCA	SN0108A	10.3.167.205	3700T-15243	v1.6.154	● Online
SN0148CO	SN0148CO	10.3.167.203	3700T-15243	v1.6.154	● Online
SN9116CO_CC	SN9116CO	10.3.167.204	3700T-15243	v1.6.154	● Online

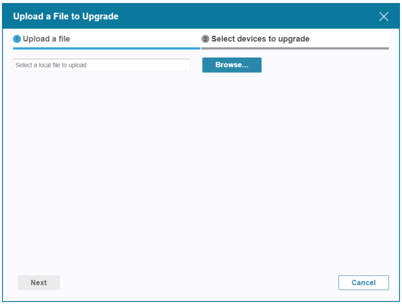
Firmware Upgrade

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

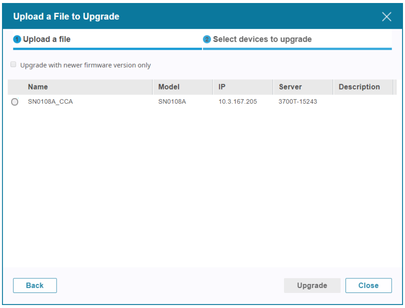
Upload a File to Upgrade

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**.



□ Upgrade with newer firmware version only

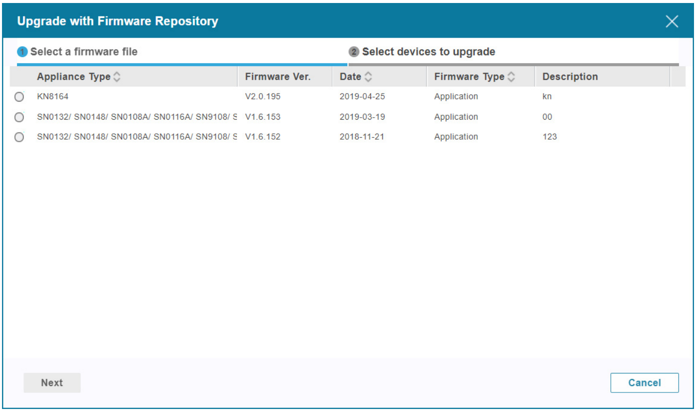
	Name	Model	IP	Server	Description
○	SN0108A_CCA	SN0108A	10.3.167.205	3700T-15243	

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 with Firmware Repository

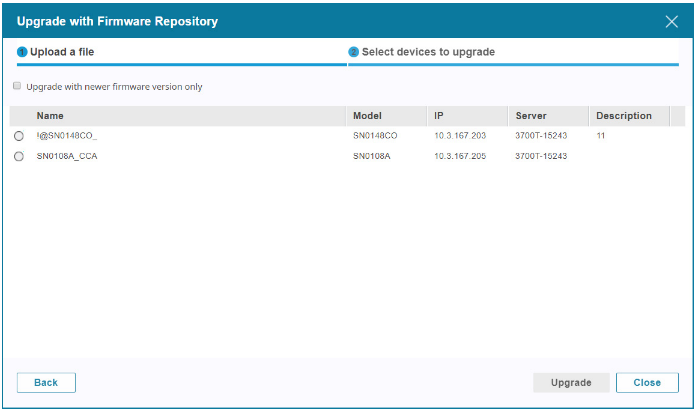
One of the ways to upgrade a device is **Upgrade with Firmware Repository**. Follow the steps below to upgrade this way:

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 104 on how to upload firmware into firmware repository.
2. Click **Upgrade with Firmware Repository**, a window will pop up.



	Appliance Type	Firmware Ver.	Date	Firmware Type	Description
○	KN8164	V2.0.195	2019-04-25	Application	kn
○	SN0132/ SN0148/ SN0108A/ SN0116A/ SN9108/ S	V1.6.153	2019-03-19	Application	00
○	SN0132/ SN0148/ SN0108A/ SN0116A/ SN9108/ S	V1.6.152	2018-11-21	Application	123

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



□ Upgrade with newer firmware version only

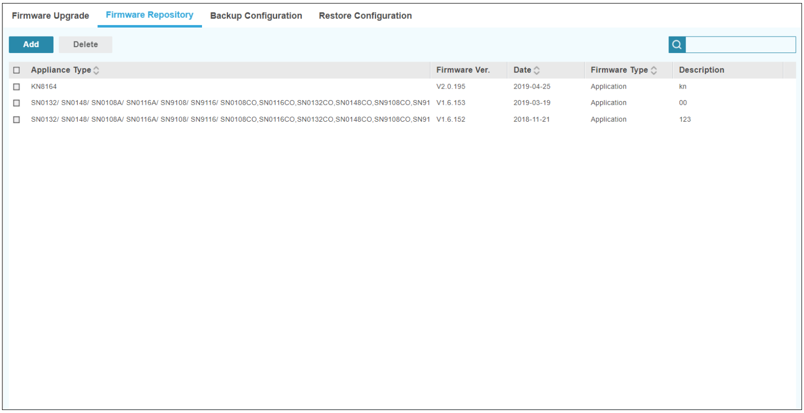
	Name	Model	IP	Server	Description
○	!@SN0148CO_	SN0148CO	10.3.167.203	3700T-15243	11
○	SN0108A_CCA	SN0108A	10.3.167.205	3700T-15243	

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:



□	Appliance Type	Firmware Ver.	Date	Firmware Type	Description
□	KN8164	V2.0.195	2019-04-25	Application	kn
□	SN0132/ SN0148/ SN0108A/ SN0116A/ SN9108/ SN9116/ SN0108CO,SN0116CO,SN0132CO,SN0148CO,SN9108CO,SN91	V1.6.153	2019-03-19	Application	00
□	SN0132/ SN0148/ SN0108A/ SN0116A/ SN9108/ SN9116/ SN0108CO,SN0116CO,SN0132CO,SN0148CO,SN9108CO,SN91	V1.6.152	2018-11-21	Application	123

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

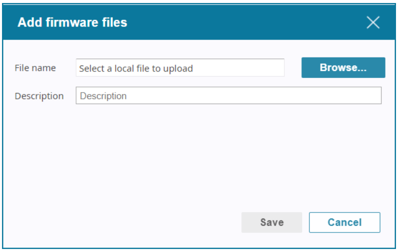
By making the latest firmware upgrade files available for distribution from this single location, you can easily perform upgrades from within the CC2000, and ensure that all the devices on your installation are operating at the same and most up-to-date firmware level.

Note: 1. Firmware upgrades can be also be performed under the Task Manager submenu. See page 171 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:



Add firmware files

File name: Select a local file to upload

Description: Description

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.

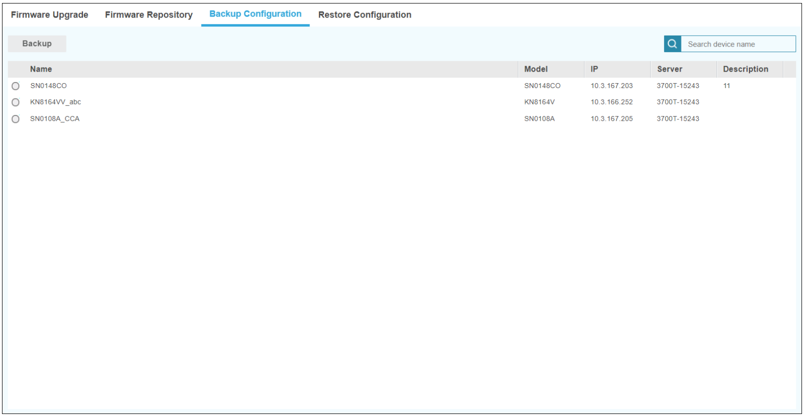
Deleting Firmware Files

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

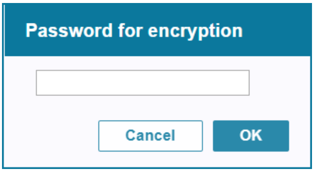
This tab will show the devices currently added to CC2000 and their information in the table.



	Name	Model	IP	Server	Description
○	SN0148CO	SN0148CO	10.3.167.203	3700T-15243	11
○	KN8164VV_abc	KN8164V	10.3.166.252	3700T-15243	
○	SN0108A_CCA	SN0108A	10.3.167.205	3700T-15243	

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

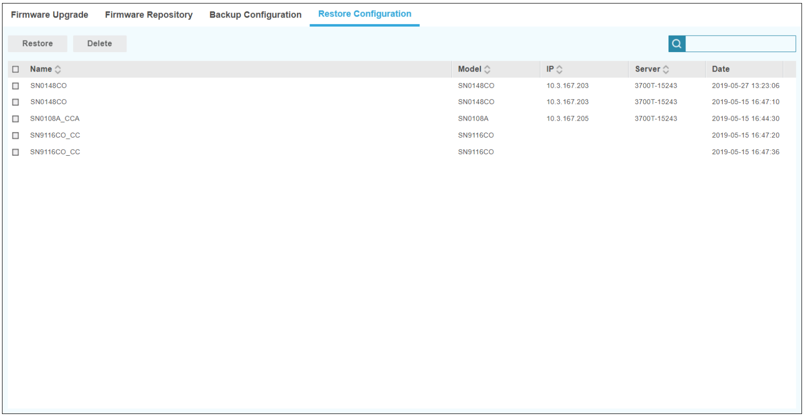
The system will ask if you would like to enter a password for encryption purpose.



Click **OK** to backup the configuration.

Restore Configuration

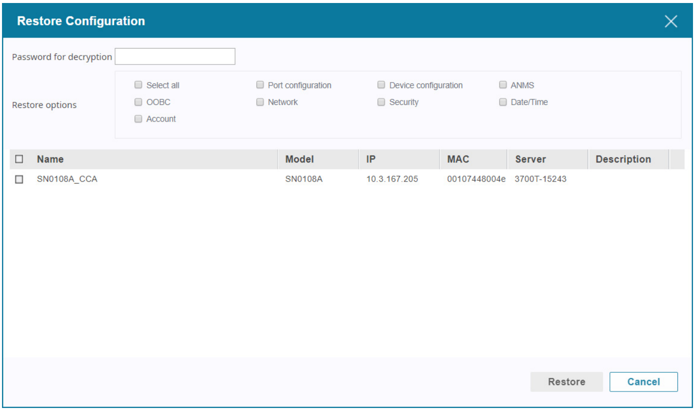
This tab will show the device configurations currently in CC2000 and their information in the table.



□	Name	Model	IP	Server	Date
□	SN0148CO	SN0148CO	10.3.167.203	3700T-15243	2019-05-27 13:23:06
□	SN0148CO	SN0148CO	10.3.167.203	3700T-15243	2019-05-15 16:47:10
□	SN0108A_CCA	SN0108A	10.3.167.205	3700T-15243	2019-05-15 16:44:30
□	SN9116CO_CC	SN9116CO			2019-05-15 16:47:20
□	SN9116CO_CC	SN9116CO			2019-05-15 16:47:36

Restore

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



Password for decryption

Restore options: □ Select all □ Port configuration □ Device configuration □ ANMS □ OOBC □ Network □ Security □ Date/Time □ Account

□	Name	Model	IP	MAC	Server	Description
□	SN0108A_CCA	SN0108A	10.3.167.205	00107448004e	3700T-15243	

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.

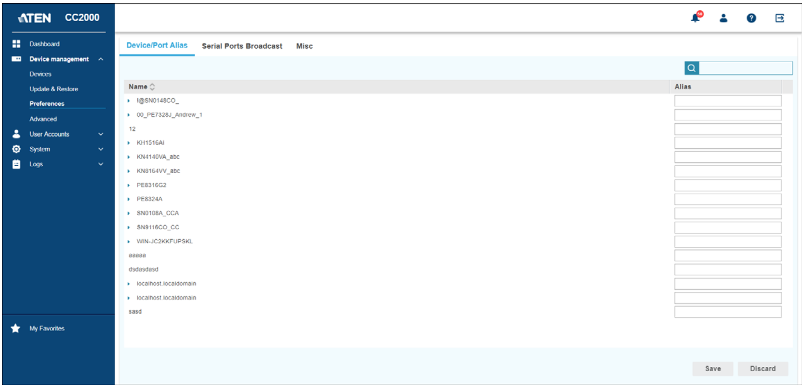
Delete

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

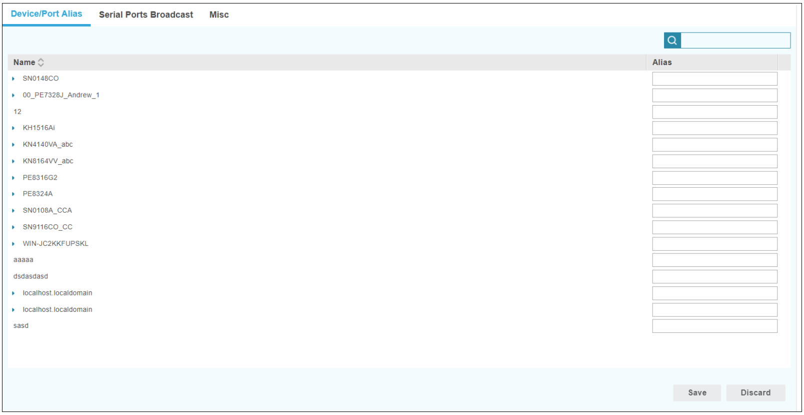
This submenu allows you to configure user preferences in different tabs.



Name	Alias
I@SN0148CO_	
00_PE7328J_Andrew_1	
12	
KH1516Ai	
KN4140VA_abc	
KN8164VV_abc	
PE8316G2	
PE8324A	
SN0108A_CCA	
SN9116CO_CC	
WIN-JC2KKFUPSKL	
aaaaa	
dsdasdasd	
localhost.localdomain	
localhost.localdomain	
sasd	

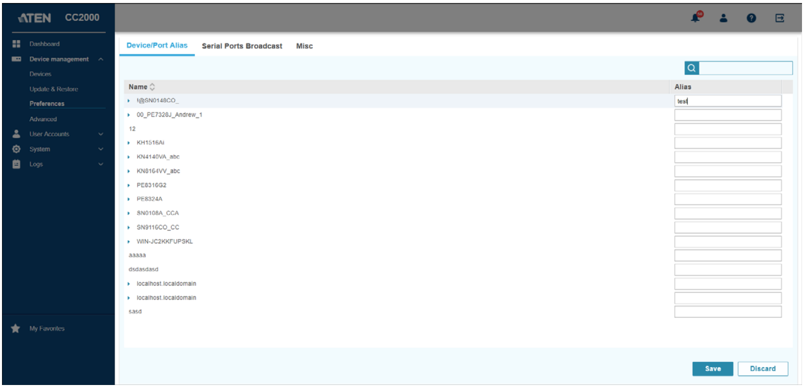
Device/Port Alias

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



Name	Alias
SN0148CO	
00_PE7328J_Andrew_1	
12	
KH1516Ai	
KN4140VA_abc	
KN8164VV_abc	
PE8316G2	
PE8324A	
SN0108A_CCA	
SN9116CO_CC	
WIN-JC2KKFUPSKL	
aaaaa	
dsdasdasd	
localhost.localdomain	
localhost.localdomain	
sasd	

- 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**.

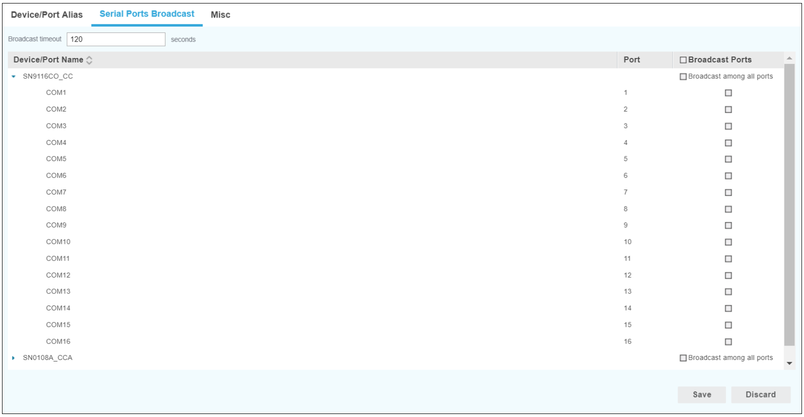


Name	Alias
!@SN0148CO_	test
00_PE7328J_Andrew_1	
12	
KH1516Ai	
KN4140VA_abc	
KN8164VV_abc	
PE8316G2	
PE8324A	
SN0108A_CCA	
SN9116CO_CC	
WIN-JC2KKFUPSKL	
aaaaa	
dsdasdasd	
localhost.localdomain	
localhost.localdomain	
sasd	

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.



Broadcast timeout 120 seconds

Device/Port Name	Port	□ Broadcast Ports
SN9116CO_CC		□ Broadcast among all ports
COM1	1	□
COM2	2	□
COM3	3	□
COM4	4	□
COM5	5	□
COM6	6	□
COM7	7	□
COM8	8	□
COM9	9	□
COM10	10	□
COM11	11	□
COM12	12	□
COM13	13	□
COM14	14	□
COM15	15	□
COM16	16	□
SN0108A_CCA		□ Broadcast among all 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.

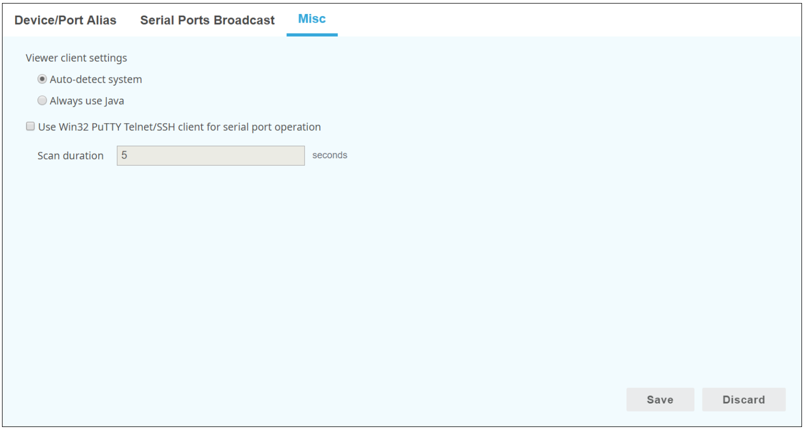
You can check **Broadcast among all ports** for a particular device to check all of its serial ports.

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.



Viewer client settings

● Auto-detect system

○ Always use Java

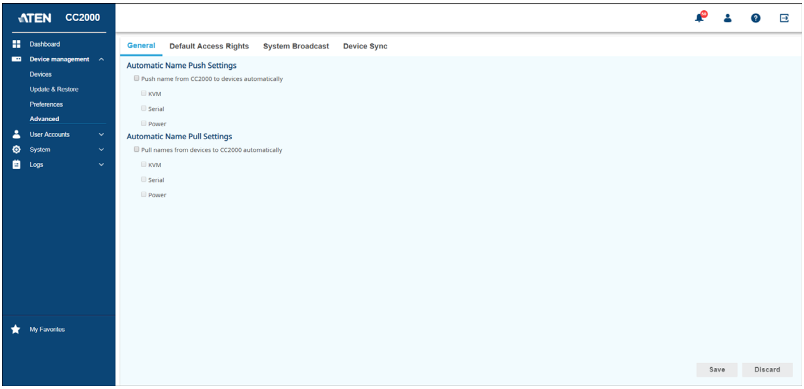
□ Use Win32 PuTTY Telnet/SSH client for serial port operation

Scan duration 5 seconds

- If you choose **Auto-detect system**, the CC2000 will check to see if you logged in with IE or with another browser. If you logged in with IE, it will open the Windows Client Viewer when you access a device or port. If you logged in with a browser other than IE, it will open the Java Client Viewer.
- 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 single 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.

Advanced

The advanced submenu includes many tabs for advanced configurations.



Automatic Name Push Settings

□ Push name from CC2000 to devices automatically

□ KVM

□ Serial

□ Power

Automatic Name Pull Settings

□ Pull names from devices to CC2000 automatically

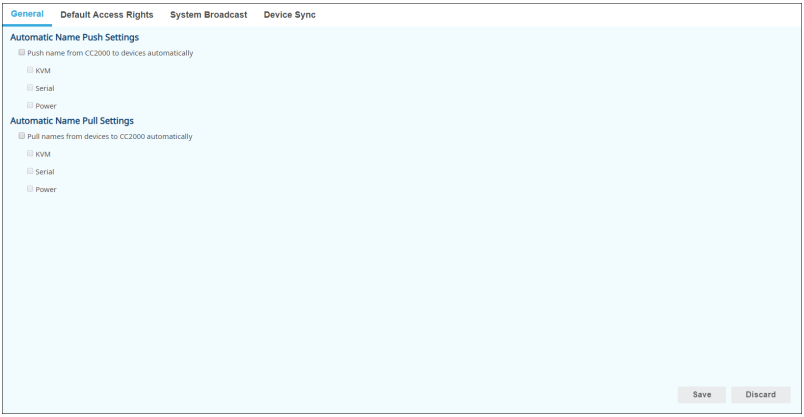
□ KVM

□ Serial

□ Power

General

The General tab is as shown below:



Automatic Name Push Settings

□ Push name from CC2000 to devices automatically

□ KVM

□ Serial

□ Power

Automatic Name Pull Settings

□ Pull names from devices to CC2000 automatically

□ KVM

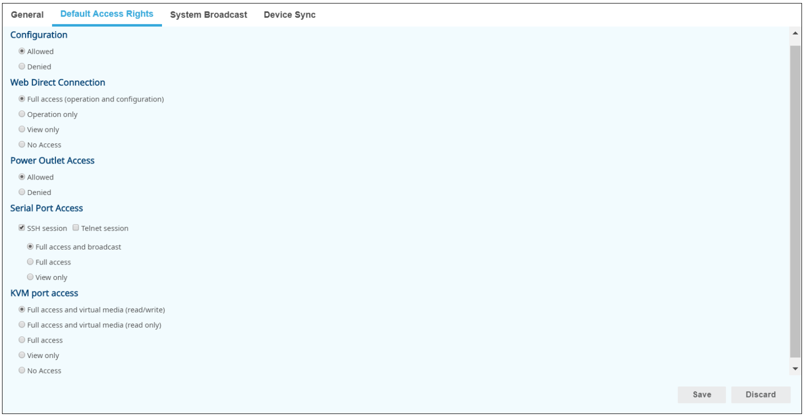
□ Serial

□ Power

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:



Configuration

- ● Allowed
- ○ Denied

Web Direct Connection

- ● Full access (operation and configuration)
- ○ Operation only
- ○ View only
- ○ No Access

Power Outlet Access

- ● Allowed
- ○ Denied

Serial Port Access

☑ SSH session ☐ Telnet session

- ● Full access and broadcast
- ○ Full access
- ○ View only

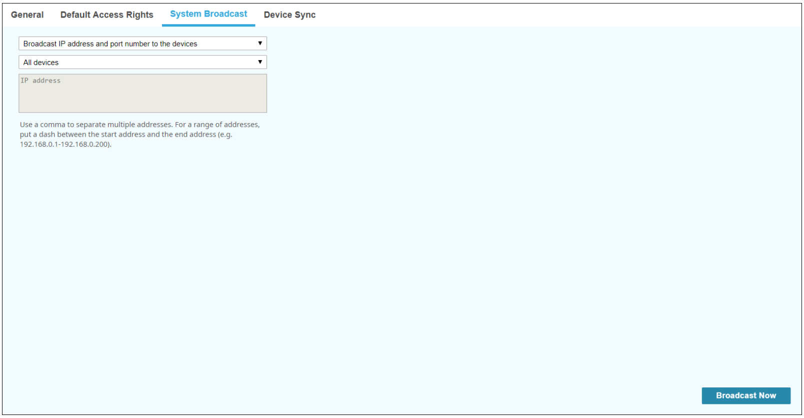
KVM port access

- ● Full access and virtual media (read/write)
- ○ Full access and virtual media (read only)
- ○ Full access
- ○ View only
- ○ No Access

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 ▾

All devices ▾

IP address

Use a comma to separate multiple addresses. For a range of addresses, put a dash between the start address and the end address (e.g. 192.168.0.1-192.168.0.200).

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 the same network segment (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.

Broadcast changed IP address and port number to the 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 the same network segment (VPN will not work)

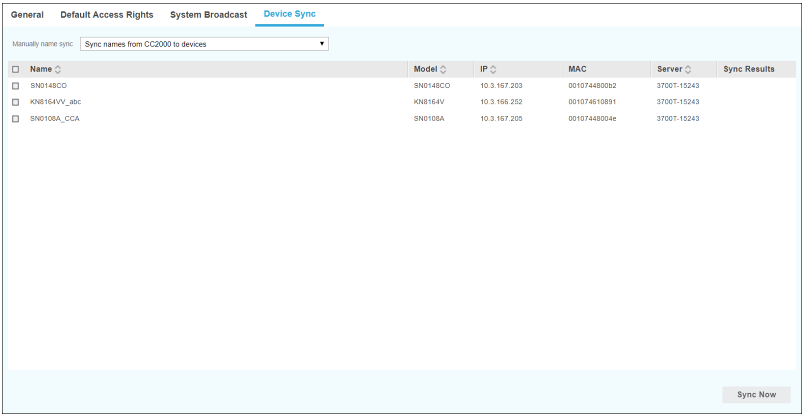
2. For heightened security, the receiving devices will only accept UDP broadcasts from the CC2000 that originally initialized them.

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

The Device Sync tab is as shown below:



Manually name sync: Sync names from CC2000 to devices ▼

□	Name	Model	IP	MAC	Server	Sync Results
□	SN0148CO	SN0148CO	10.3.167.203	0010744800b2	3700T-15243	
□	KN8164VV_abc	KN8164V	10.3.166.252	001074610891	3700T-15243	
□	SN0108A_CCA	SN0108A	10.3.167.205	00107448004e	3700T-15243	

For device name changes, use this tab to manually sync the names between the devices and the CC2000.

Select **Sync names from CC2000 to devices** or **Sync names from devices to CC2000**.

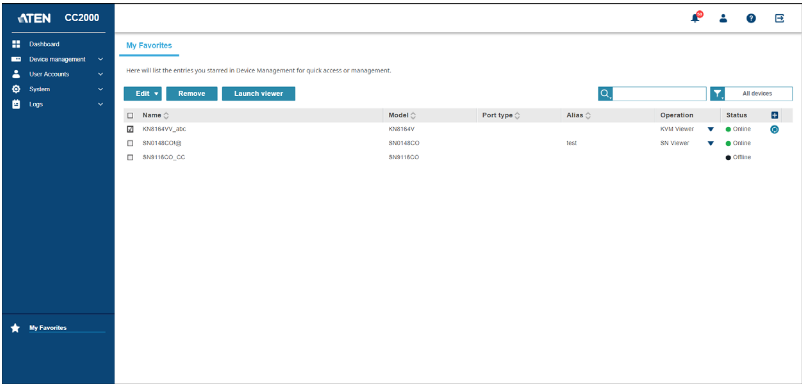
Select the device(s) you wish to sync with by checking the checkbox(es).

Click **Sync Now**.

My Favorites

The *My Favorites* page is similar to a bookmarks feature. 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:



Here will list the entries you starred in Device Management for quick access or management.

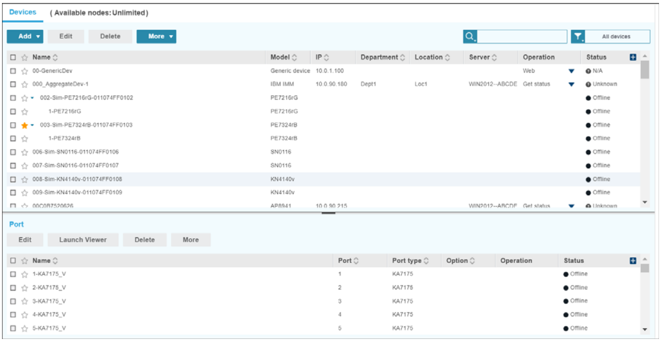
☐	Name	Model	Port type	Alias	Operation	Status
☑	KN8164VV_abc	KN8164V			KVM Viewer	● Online
☐	SN0148CO!@	SN0148CO		test	SN Viewer	● Online
☐	SN9116CO_CC	SN9116CO				● Offline

Note: *Edit* and *Launch viewer* work the way they do in the Devices submenu. Refer to *Editing Devices* on page 79 and *Operation* on page 90 for more information.

Add Favorites

Follow the steps below to add a favorite.

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



☐	☆	Name	Model	IP	Department	Location	Server	Operation	Status
☐	☆	00-GenericDev	Generic device	10.0.1.100				Web	N/A
☐	☆	000_AggregateDev-1	IBM IMM	10.0.90.180	Dept1	Loc1	WIN2012--ABCDE	Get status	Unknown
☐	☆	002-Sim-PE7216rG-011074FF0102	PE7216rG						● Offline
☐	☆	1-PE7216rG	PE7216rG						● Offline
☐	★	003-Sim-PE7324rB-011074FF0103	PE7324rB						● Offline
☐	☆	1-PE7324rB	PE7324rB						● Offline
☐	☆	006-Sim-SN0116-011074FF0106	SN0116						● Offline
☐	☆	007-Sim-SN0116-011074FF0107	SN0116						● Offline
☐	☆	008-Sim-KN4140v-011074FF0108	KN4140v						● Offline
☐	☆	009-Sim-KN4140v-011074FF0109	KN4140v						● Offline
☐	☆	00C0B7520626	AP8941	10.0.90.215			WIN2012--ABCDE	Get status	Unknown

☐	☆	Name	Port	Port type	Option	Operation	Status
☐	☆	1-KA7175_V	1	KA7175			● Offline
☐	☆	2-KA7175_V	2	KA7175			● Offline
☐	☆	3-KA7175_V	3	KA7175			● Offline
☐	☆	4-KA7175_V	4	KA7175			● Offline
☐	☆	5-KA7175_V	5	KA7175			● Offline

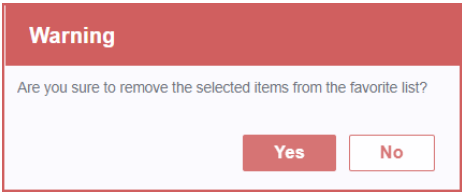
2. Find the device/port you wish to add to My Favorites in the device/port list.

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

4. The star icon will change to a 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 checkbox of the device/port and click **Remove**. The system will ask if you would like to remove the device/port, click **Yes** to continue.



Warning

Are you sure to remove the selected items from the favorite list?

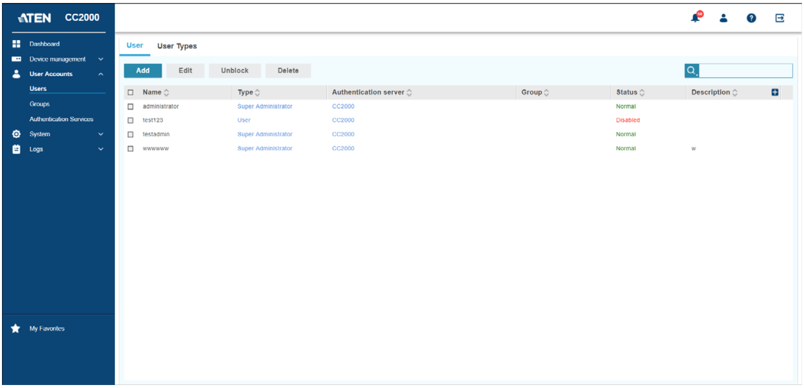
Chapter 6
User Accounts

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:



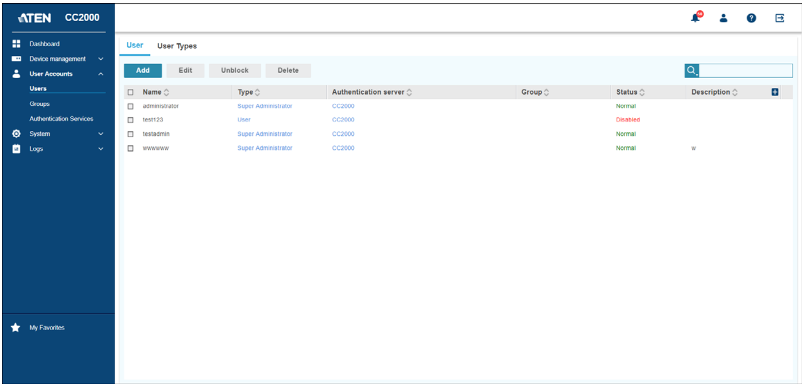
□	Name	Type	Authentication server	Group	Status	Description
□	administrator	Super Administrator	CC2000		Normal	
□	test123	User	CC2000		Disabled	
□	testadmin	Super Administrator	CC2000		Normal	
□	wwwwww	Super Administrator	CC2000		Normal	w

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.

Users

The Users submenu looks similar to the one below:



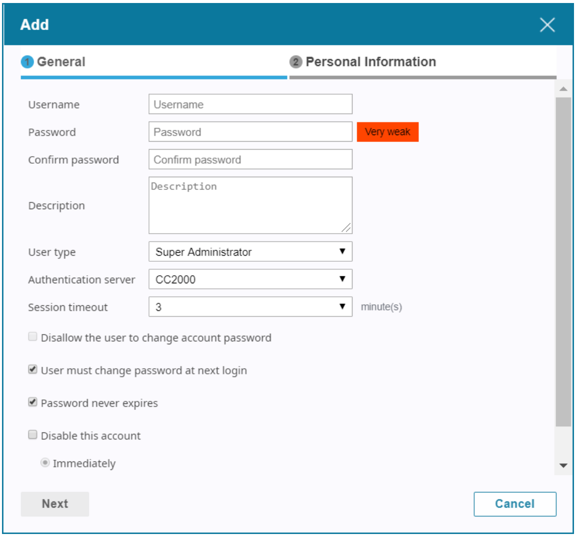
□	Name	Type	Authentication server	Group	Status	Description
□	administrator	Super Administrator	CC2000		Normal	
□	test123	User	CC2000		Disabled	
□	testadmin	Super Administrator	CC2000		Normal	
□	wwwwww	Super Administrator	CC2000		Normal	w

User

Add User

Follow the steps below to add a user:

1. Click **Add** for the page below:



Username	Username
Password	Password
Confirm password	Confirm password
Description	Description
User type	Super Administrator
Authentication server	CC2000
Session timeout	3 minute(s)

□ Disallow the user to change account password

☑ User must change password at next login

☑ Password never expires

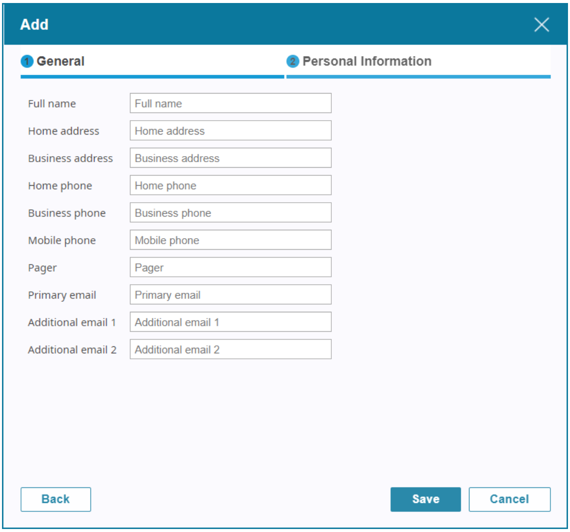
□ Disable this account

● Immediately

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

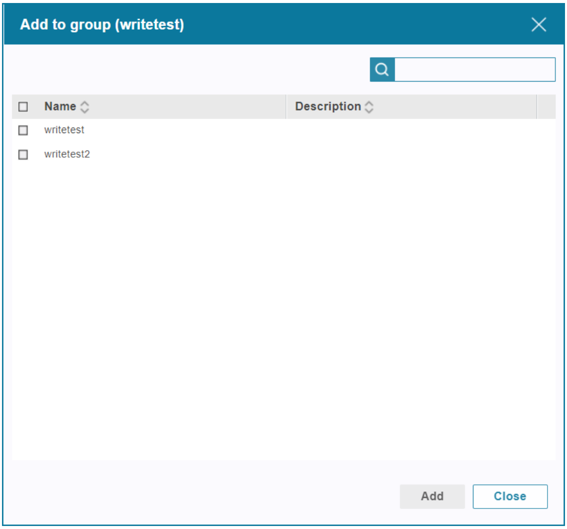
Field	Description
Username	**Internal (CC2000) Accounts:** A maximum of 32 English alphanumeric characters is allowed. The minimum number of characters is based on the CC2000's account policy settings (see *CC2000 Authentication*, page 140). **External Authentication:** The Login name should be one that 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 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. 125 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 *Add Authentication Services*, page 135, 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 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 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 pertains to Web log in sessions.
Other Information	Check the checkbox(es) for the extra policies governing this account.

3. Click **Next** for the personal information page.



The information entered here is to help identify the user only.

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



□	Name	Description
□	writetest	
□	writetest2	

5. Check the group you wish the user to be added to and click **Add**.

6. Click **Close** to complete the process.

Edit User

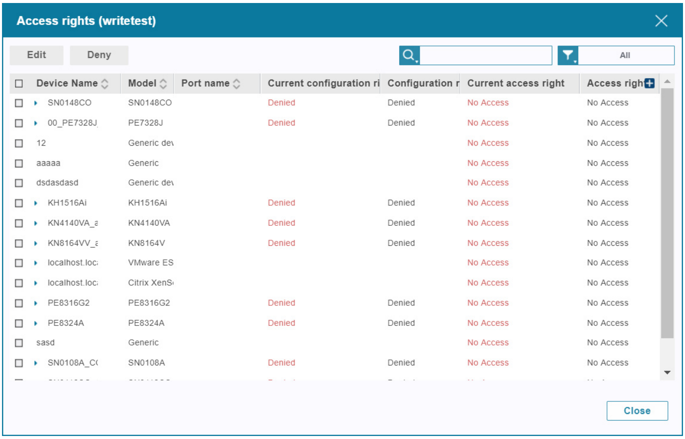
You can edit the Access Rights and the Properties of a user.

■ Edit 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:



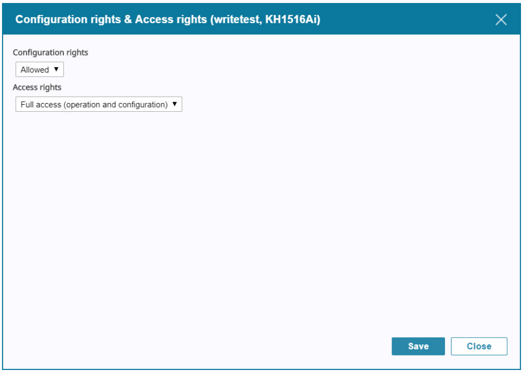
Access rights (writetest)

□	Device Name	Model	Port name	Current configuration ri	Configuration r	Current access right	Access righ
□	SN0148CO	SN0148CO		Denied	Denied	No Access	No Access
□	00_PE7328J	PE7328J		Denied	Denied	No Access	No Access
□	12	Generic de\				No Access	No Access
□	aaaaa	Generic				No Access	No Access
□	dsdasdasd	Generic de\				No Access	No Access
□	KH1516Ai	KH1516Ai		Denied	Denied	No Access	No Access
□	KN4140VA_a	KN4140VA		Denied	Denied	No Access	No Access
□	KN8164VV_a	KN8164V		Denied	Denied	No Access	No Access
□	localhost.loc	VMware ES				No Access	No Access
□	localhost.loc	Citrix XenS				No Access	No Access
□	PE8316G2	PE8316G2		Denied	Denied	No Access	No Access
□	PE8324A	PE8324A		Denied	Denied	No Access	No Access
□	sasd	Generic				No Access	No Access
□	SN0108A_C	SN0108A		Denied	Denied	No Access	No Access

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:



Configuration rights & Access rights (writetest, KH1516Ai)

Configuration rights: Allowed

Access rights: Full access (operation and configuration)

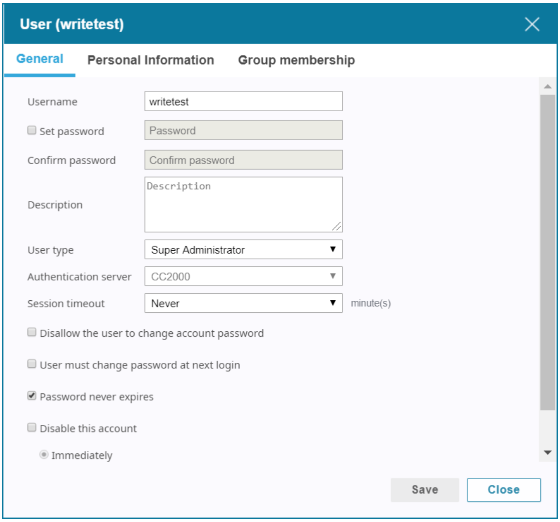
4. Refer to the information in *Access rights* on page 79 to help you edit the rights.

■ Edit 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:



Username: writetest

☐ Set password: Password

Confirm password: Confirm password

Description: Description

User type: Super Administrator

Authentication server: CC2000

Session timeout: Never minute(s)

☐ Disallow the user to change account password

☐ User must change password at next login

☑ Password never expires

☐ Disable this account

● Immediately

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

   Refer to *User* on page 120 for information about the three tabs shown here.

■ Unblock User

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

To unblock a 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: 1. 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.

2. 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 243.

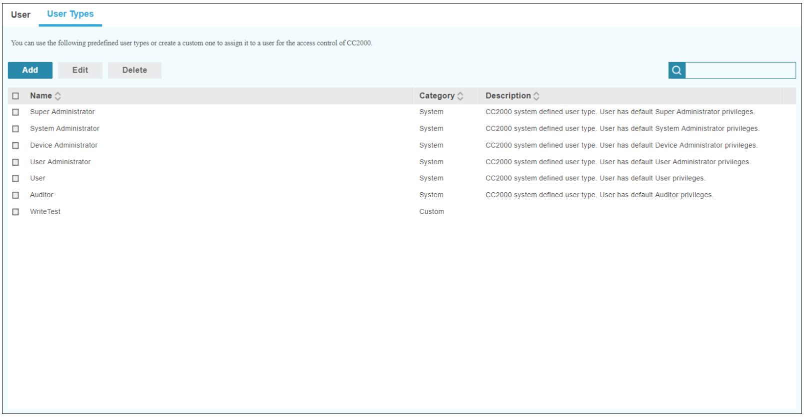
Delete User

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

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

User Types

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



You can use the following predefined user types or create a custom one to assign it to a user for the access control of CC2000.

□	Name	Category	Description
□	Super Administrator	System	CC2000 system defined user type. User has default Super Administrator privileges.
□	System Administrator	System	CC2000 system defined user type. User has default System Administrator privileges.
□	Device Administrator	System	CC2000 system defined user type. User has default Device Administrator privileges.
□	User Administrator	System	CC2000 system defined user type. User has default User Administrator privileges.
□	User	System	CC2000 system defined user type. User has default User privileges.
□	Auditor	System	CC2000 system defined user type. User has default Auditor privileges.
□	WriteTest	Custom	

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 roles performed by members of the System category are fixed. The roles associated with each type are summarized in the table below:

Assigned Roles	Super Admin	System Admin	User Admin	Device Admin	User	Auditor
System Management	√	√				◊
System tasks	√	√				◊
Authentication services	√	√	√			◊
User / Group management	√	√	√			◊
User / Group device access rights	√	√	√			◊
Device management	√	√		√		◊
Log configuration and setting	√	√	√	√		
View logs / reports	√	√	√	√		◊
Users can change their own passwords	√	√	√	√	√	√

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.
- You cannot change Super Administrators to different user types whereas System Administrators can be changed to different user types.

2. Auditor:

- Auditors can access all tabs and pages, but is restricted to *View Only* rights.
- For **Preferences**, Auditors can change his/her *Web Options* and *Password*.

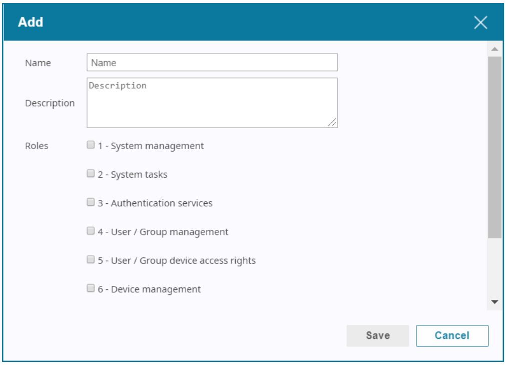
Custom User Types

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:



Name: Name

Description: Description

Roles:
- □ 1 - System management
- □ 2 - System tasks
- □ 3 - Authentication services
- □ 4 - User / Group management
- □ 5 - User / Group device access rights
- □ 6 - Device management

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

Note: 1. The Name can be the equivalent of from 2–32 English alphanumeric characters, but cannot contain the following: " ' \

2. The Description can be up to 256 Bytes.

3. Click **Save** to complete.

■ Edit 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.

Delete User Type

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

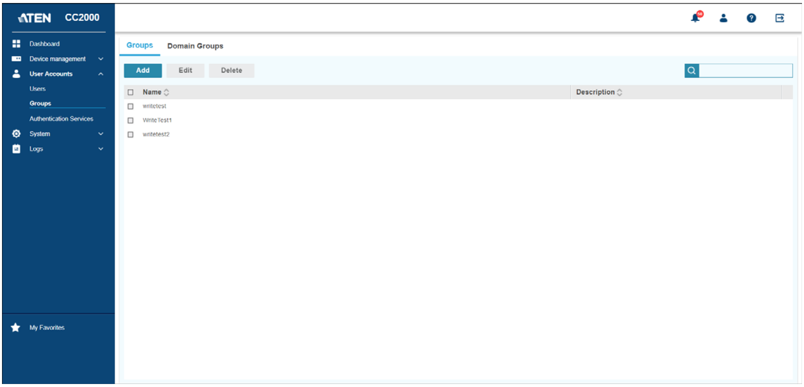
A confirmation message will pop up, click **Yes** to delete the user type(s).

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

Groups

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 need only set them once for the group, instead of having to set them for each user 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:

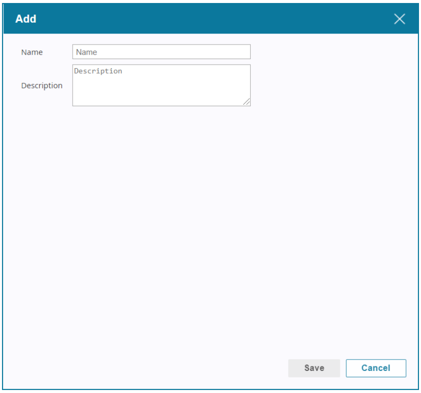


□	Name	Description
□	writetest	
□	WriteTest1	
□	writetest2	

Groups Tab

Add Group

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



Name: Name

Description: Description

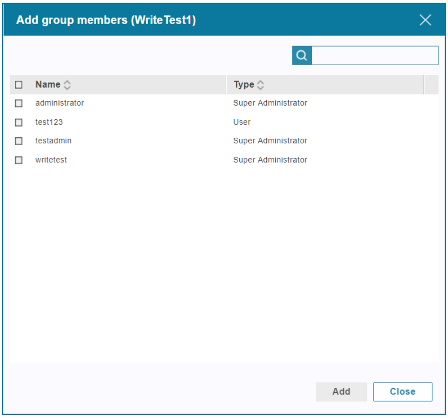
2. Enter a name and description.

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

2. The Description can be up to 256 Bytes

3. Click **Save**.

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



Add group members (WriteTest1)

□	Name	Type
□	administrator	Super Administrator
□	test123	User
□	testadmin	Super Administrator
□	writetest	Super Administrator

5. Check the users you wish to include into the group and click **Add**.

6. When you have finished adding the users, click **Close**.

Edit Group

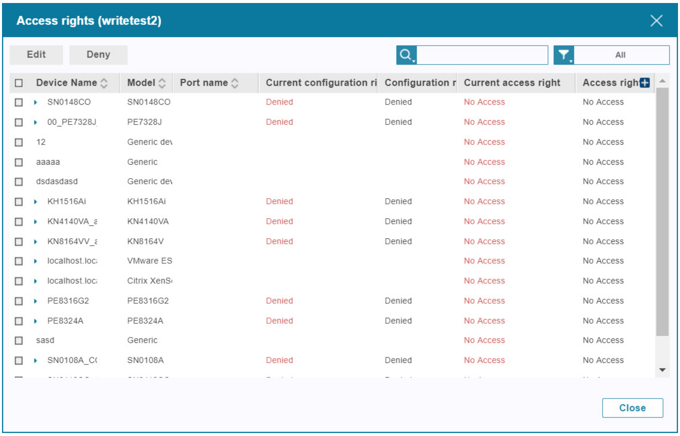
■ Edit Group Access Rights

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:



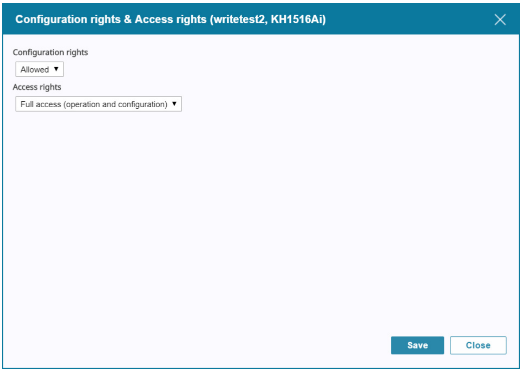
Access rights (writetest2)

□	Device Name	Model	Port name	Current configuration ri	Configuration r	Current access right	Access righ
□	▸ SN0148CO	SN0148CO		Denied	Denied	No Access	No Access
□	▸ 00_PE7328J	PE7328J		Denied	Denied	No Access	No Access
□	12	Generic de\				No Access	No Access
□	aaaaa	Generic				No Access	No Access
□	dsdasdasd	Generic de\				No Access	No Access
□	▸ KH1516Ai	KH1516Ai		Denied	Denied	No Access	No Access
□	▸ KN4140VA_a	KN4140VA		Denied	Denied	No Access	No Access
□	▸ KN8164VV_a	KN8164V		Denied	Denied	No Access	No Access
□	▸ localhost.loc	VMware ES				No Access	No Access
□	▸ localhost.loc	Citrix XenS				No Access	No Access
□	▸ PE8316G2	PE8316G2		Denied	Denied	No Access	No Access
□	▸ PE8324A	PE8324A		Denied	Denied	No Access	No Access
□	sasd	Generic				No Access	No Access
□	▸ SN0108A_C(	SN0108A		Denied	Denied	No Access	No Access

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:



Configuration rights & Access rights (writetest2, KH1516Ai)

Configuration rights: Allowed ▾

Access rights: Full access (operation and configuration) ▾

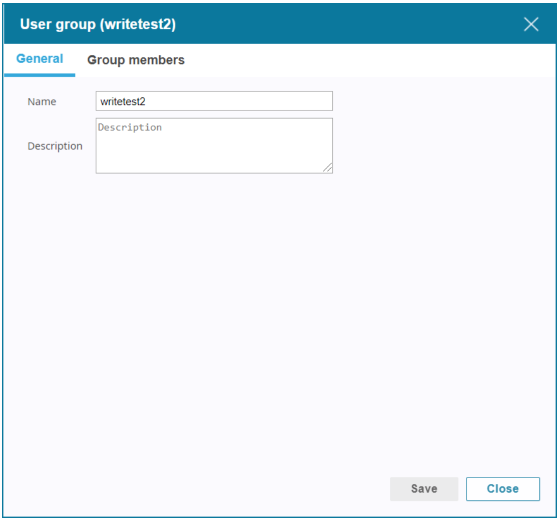
4. Refer to the information in *Access rights* on page 79 to help you edit the rights.

■ Edit 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:



User group (writetest2)

Name: writetest2

Description: Description

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

   Refer to *Add Group* on page 128 for information about the two tabs shown here.

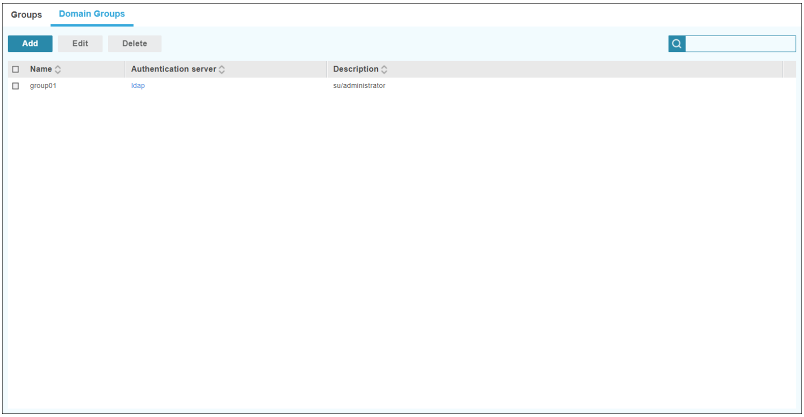
Delete Group

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

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

Domain Groups tab

The Domain Groups tab is shown below:

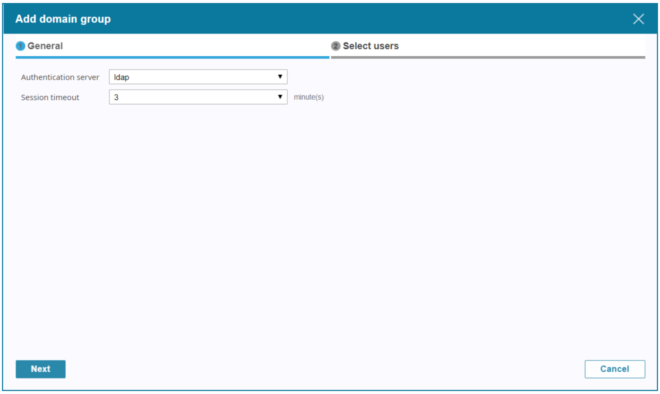


□	Name	Authentication server	Description
□	group01	ldap	su/administrator

You must have an external authentication service before you can configure this page. Refer to *Add Authentication Services* on page 135 on how to add authentication service.

Add Domain Group

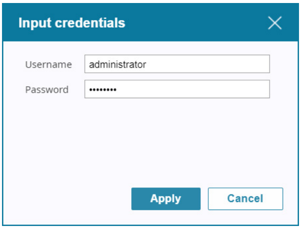
1. Click **Add** for the Add domain group pop-up window:



Authentication server: ldap

Session timeout: 3 minute(s)

2. Select the Authentication server and Session timeout by clicking and selecting from their corresponding drop-down menu.
3. Click **Next**. Where necessary, the server may prompt you for credential input. An example is shown:

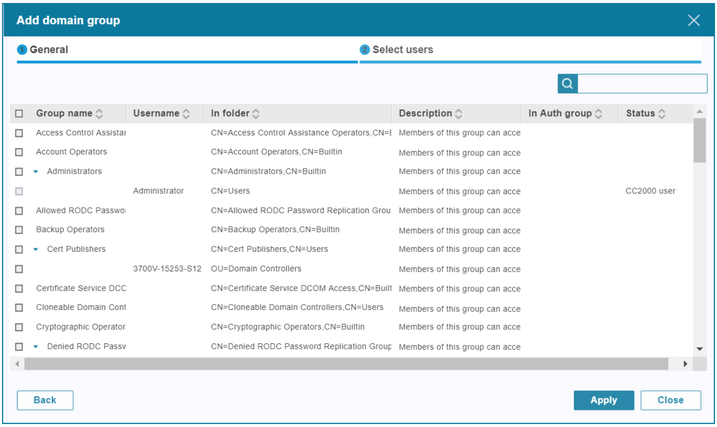


Input credentials

Username administrator

Password ••••••••

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



Add domain group

1 General 2 Select users

□	Group name	Username	In folder	Description	In Auth group	Status
□	Access Control Assistar		CN=Access Control Assistance Operators,CN=E	Members of this group can acce		
□	Account Operators		CN=Account Operators,CN=Builtin	Members of this group can acce		
□	▾ Administrators		CN=Administrators,CN=Builtin	Members of this group can acce		
□		Administrator	CN=Users	Members of this group can acce		CC2000 user
□	Allowed RODC Passwo		CN=Allowed RODC Password Replication Grou	Members of this group can acce		
□	Backup Operators		CN=Backup Operators,CN=Builtin	Members of this group can acce		
□	▾ Cert Publishers		CN=Cert Publishers,CN=Users	Members of this group can acce		
□		3700V-15253-S12	OU=Domain Controllers	Members of this group can acce		
□	Certificate Service DCC		CN=Certificate Service DCOM Access,CN=Built	Members of this group can acce		
□	Cloneable Domain Cont		CN=Cloneable Domain Controllers,CN=Users	Members of this group can acce		
□	Cryptographic Operator		CN=Cryptographic Operators,CN=Builtin	Members of this group can acce		
□	▾ Denied RODC Passv		CN=Denied RODC Password Replication Group	Members of this group can acce		

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

Authentication Services

The CC2000 provides an internal *Username / Password* authentication service. In addition, the CC2000 supports the following third party external authentication servers: Active Directory, Kerberos, LDAP, RADIUS, TACACS+ and Windows NT Domain.

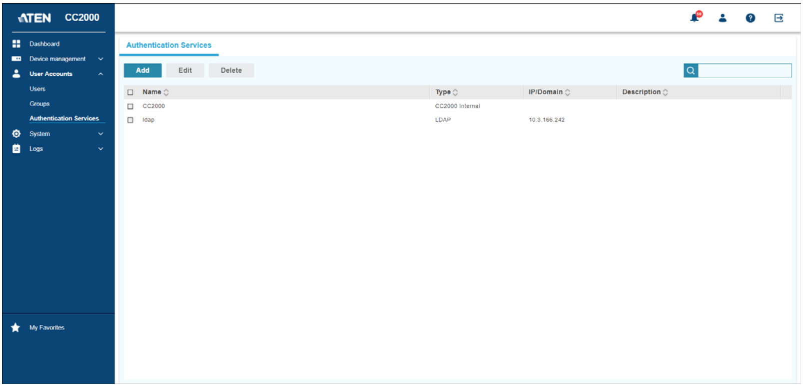
Note: 1. *Authentication* refers to determining the authenticity of the person logging in; *authorization* refers to assigning permission to use the device's various functions.

2. These external servers provide authentication services only – they do not provide authorization services. Authorization is provided through the CC2000 management system.

By adding an external authentication server to the CC2000 management system (see page 135 for details), when you add a user account, you can select the external authentication server from the list of authentication servers.

Note: 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 132, for details.

The Authentication Services submenu is shown below:

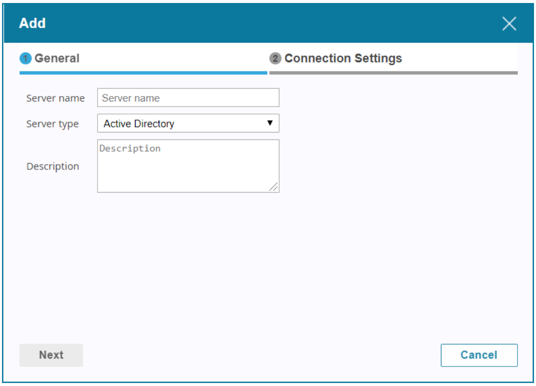


□	Name	Type	IP/Domain	Description
□	CC2000	CC2000 Internal		
□	ldap	LDAP	10.3.166.242	

Add Authentication Services

Follow the steps below to add authentication services:

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



Add

1 General — 2 Connection Settings

Server name: Server name

Server type: Active Directory

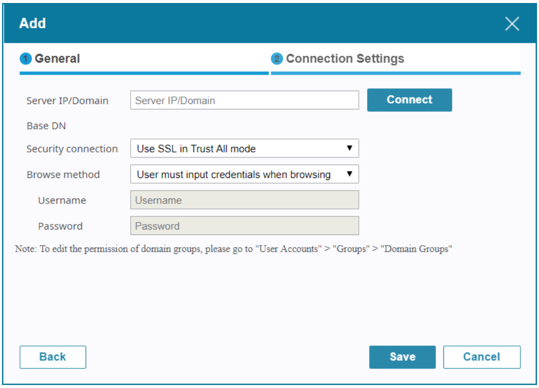
Description: Description

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

Note: 1. The Server name can be the equivalent of from 2–32 English alphanumeric characters, but cannot contain the following: **" '**

2. The Description can be up to 256 bytes.

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



Add

1 General — 2 Connection Settings

Server IP/Domain: Server IP/Domain

Base DN

Security connection: Use SSL in Trust All mode

Browse method: User must input credentials when browsing

Username: Username

Password: Password

Note: To edit the permission of domain groups, please go to "User Accounts" > "Groups" > "Domain Groups"

4. Enter information on the page. Refer to *Server Information* on page 136 for the information fields.

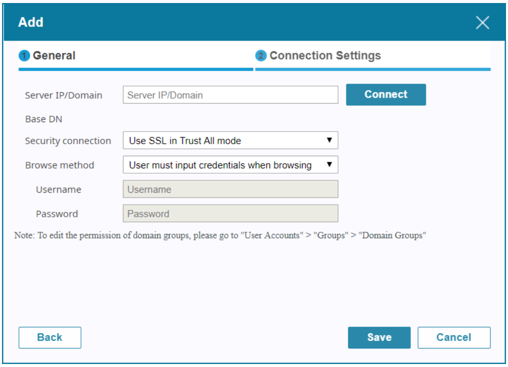
5. Enter the server IP/domain and click **Connect** to test the connection.
6. Select the Security connection and Browse method using the corresponding drop-down menu. Click **Save**.

Server Information

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

1. 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 267.
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.



Server IP/Domain: Server IP/Domain

Base DN

Security connection: Use SSL in Trust All mode

Browse method: User must input credentials when browsing

Username: Username

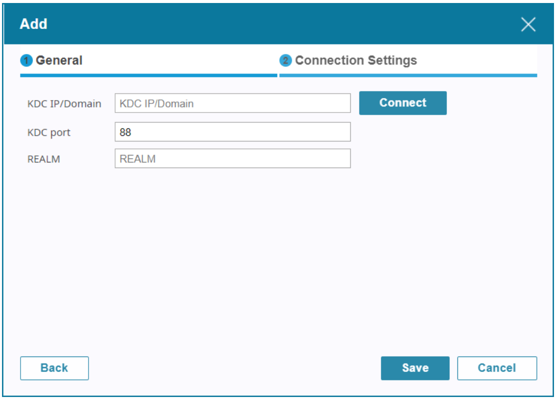
Password: Password

Note: To edit the permission of domain groups, please go to "User Accounts" > "Groups" > "Domain Groups"

2. Kerberos

Heading	Information
KDC IP/Domain	Get the IP/Domain from the Kerberos administrator.

Heading	Information
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.



KDC IP/Domain: KDC IP/Domain

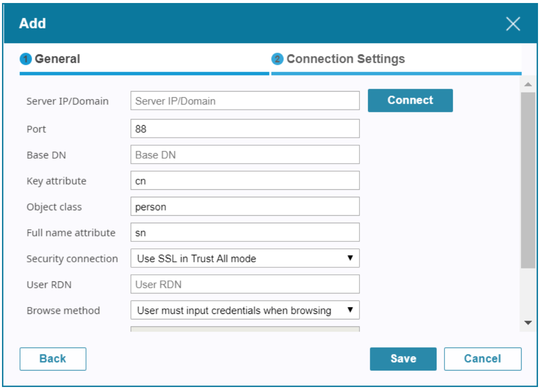
KDC port: 88

REALM: REALM

3. 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 265.
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 265.

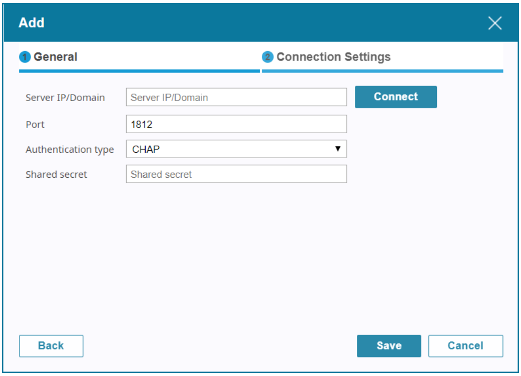
Heading	Information
Browsing Method	◆ Select *Browse with user credentials* to allow the user to browse LDAP/LDAPS using credentials configured on the server. If this is selected the user doesn't have to input his credentials each time he browses. ◆ Select *User must input credentials when browsing* to have the user input his credentials each time he browses the LDAP/LDAPS.



Server IP/Domain	Server IP/Domain
Port	88
Base DN	Base DN
Key attribute	cn
Object class	person
Full name attribute	sn
Security connection	Use SSL in Trust All mode ▼
User RDN	User RDN
Browse method	User must input credentials when browsing ▼

4. 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 268 and *TACACS+ Settings Example*, page 270.
Authentication Settings	Get the information for these fields from the service administrator. For example settings see *RADIUS Settings Example*, page 268 and *TACACS+ Settings Example*, page 270. 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.



Server IP/Domain: Server IP/Domain

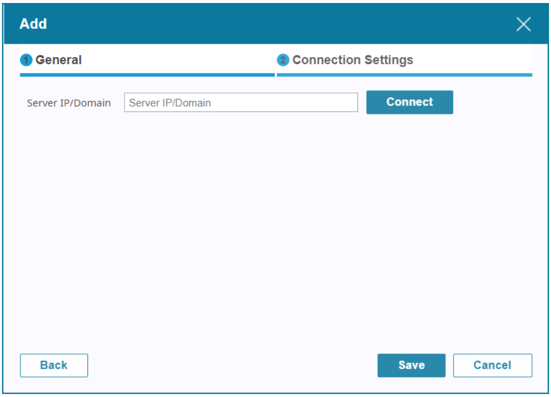
Port: 1812

Authentication type: CHAP

Shared secret: Shared secret

5. Windows NT Domain

   Get the information for the Domain Name from the service administrator. For example settings see *NT Domain Settings Example*, page 272.



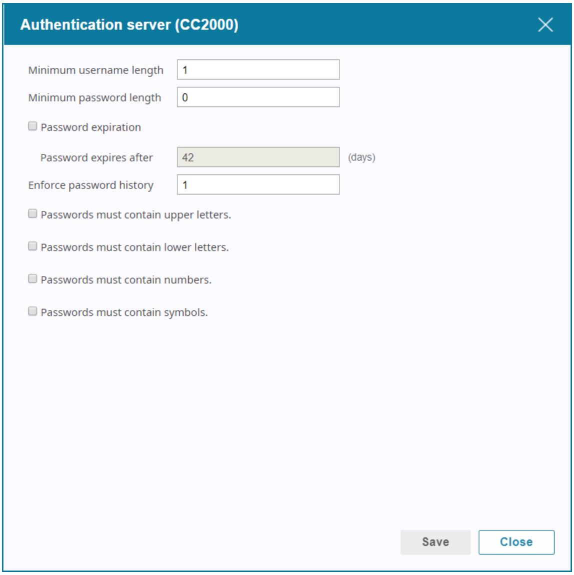
Server IP/Domain: Server IP/Domain

CC2000 Authentication

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.



Authentication server (CC2000)

Minimum username length: 1

Minimum password length: 0

□ Password expiration

Password expires after: 42 (days)

Enforce password history: 1

□ Passwords must contain upper letters.

□ Passwords must contain lower letters.

□ Passwords must contain numbers.

□ Passwords must contain symbols.

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

Minimum username length	The username length can be the equivalent of from 1–32 English alphanumeric characters. The default is 6 characters.
Minimum password length	The password length can be the equivalent of 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**.

Delete 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: 1. You can delete all deleteable servers by checking the box at the top of the column.

2. If a user account has been created on the CC2000 that uses an external authentication server, the server cannot be deleted.

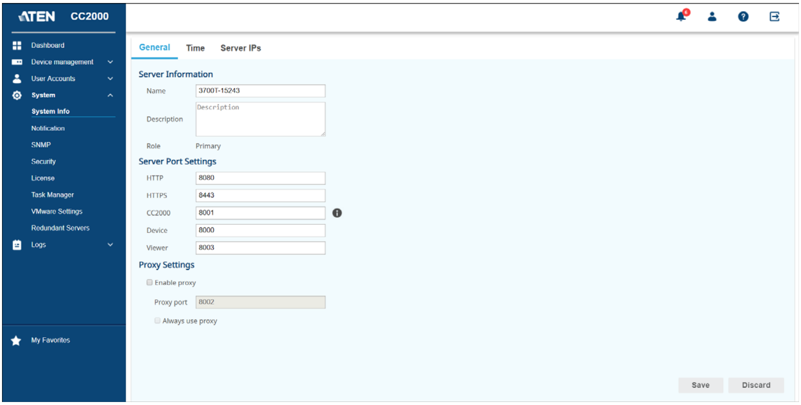
This Page Intentionally Left Blank

Chapter 7
System

Overview

A CC2000 installation is comprised of CC2000 compatible devices residing on a network segment that are connected – over-IP – to a CC2000 server that also resides on that same network segment. 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 the others are considered Secondaries. When you click the System, the CC2000 opens to the default System page, which looks similar to the screen below:



Server Information

Name: 3700T-15243
Description: Description
Role: Primary

Server Port Settings

HTTP: 8080
HTTPS: 8443
CC2000: 8001
Device: 8000
Viewer: 8003

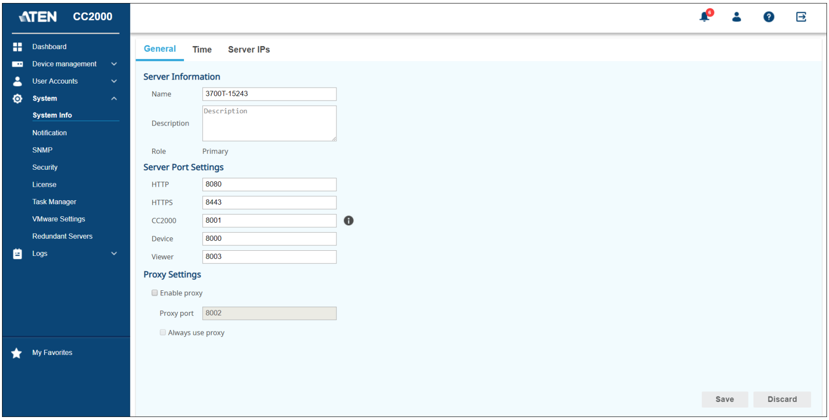
Proxy Settings

□ Enable proxy
Proxy port: 8002
□ Always use proxy

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, and it looks similar to the one below:



Server Information

Name: 3700T-15243

Description: Description

Role: Primary

Server Port Settings

HTTP: 8080

HTTPS: 8443

CC2000: 8001

Device: 8000

Viewer: 8003

Proxy Settings

□ Enable proxy

Proxy port: 8002

□ Always use proxy

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.
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.

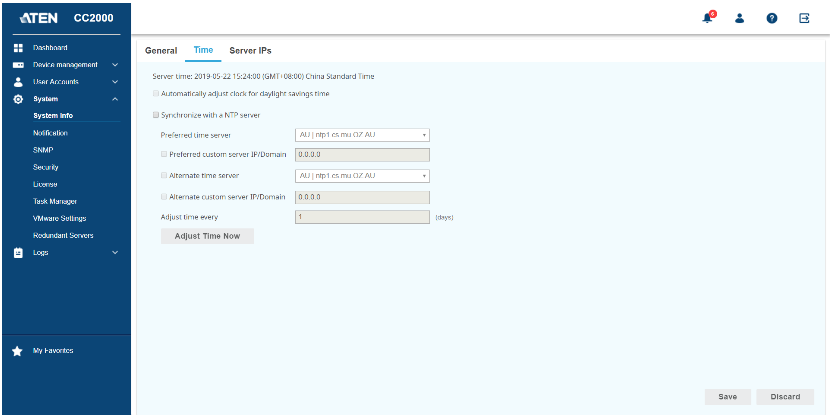
Field	Description
Viewer	The port that the CC2000 uses for the viewers to communicate with when Multiviewer is in effect. See *Launch Viewer*, page 99.
Enable proxy	If you need to use the proxy function, check this box, then specify the proxy port in the indicated field. See *CC2000 Proxy Function*, page 229.
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 synchronized the time of the server the CC2000 is installed on to a network time server.



Server time: 2019-05-22 15:24:00 (GMT+08:00) China Standard Time

□ Automatically adjust clock for daylight savings time

□ Synchronize with a NTP server

Preferred time server: AU | ntp1.cs.mu.OZ.AU

□ Preferred custom server IP/Domain: 0.0.0.0

□ Alternate time server: AU | ntp1.cs.mu.OZ.AU

□ Alternate custom server IP/Domain: 0.0.0.0

Adjust time every: 1 (days)

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:

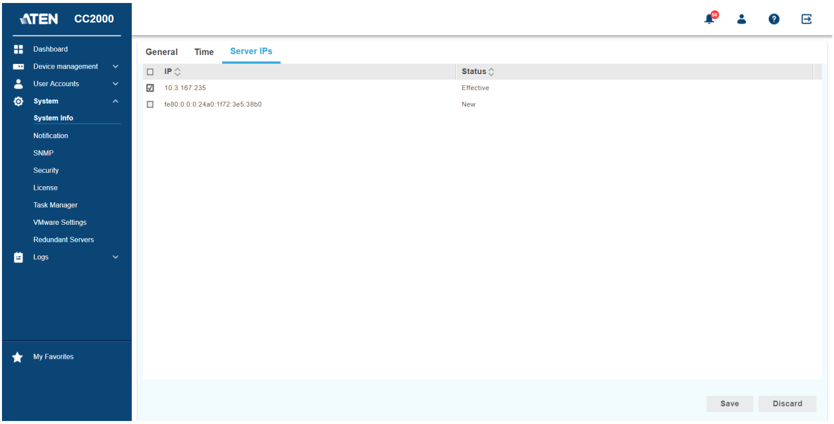
1. Check the **Synchronize with a NTP server** checkbox.
2. Use the drop-down menu **Preferred time server** to select your preferred time server, or

   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

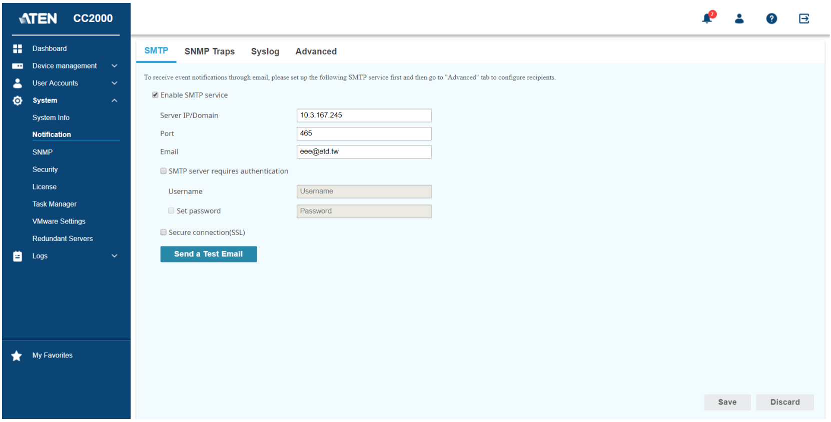
The Server IPs page shows available IP for the server that CC2000 is installed on. Check the checkbox of the IP(s) you wish to use and click **Save** to enable the server and make it Effective.



□	IP	Status
☑	10.3.167.235	Effective
□	fe80:0:0:0:24a0:1f72:3e5:38b0	New

Notification

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:



To receive event notifications through email, please set up the following SMTP service first and then go to "Advanced" tab to configure recipients.

☑ Enable SMTP service

Server IP/Domain: 10.3.167.245

Port: 465

Email: eee@etd.tw

□ SMTP server requires authentication

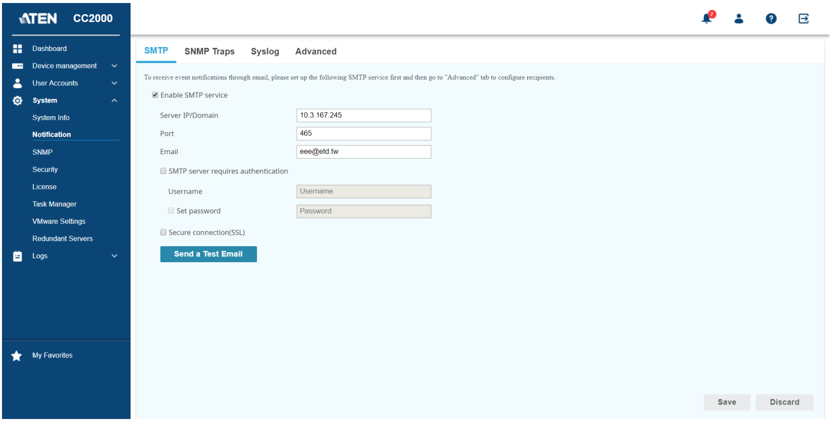
Username: Username

□ Set password: Password

□ Secure connection(SSL)

SMTP

The CC2000 can send email notification of events traps on the installation to specified users.



To receive event notifications through email, please set up the following SMTP service first and then go to "Advanced" tab to configure recipients.

☑ Enable SMTP service

Server IP/Domain: 10.3.167.245

Port: 465

Email: eee@etd.tw

□ SMTP server requires authentication

Username: Username

□ Set password: Password

□ Secure connection(SSL)

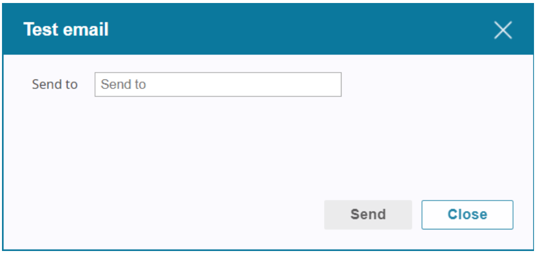
Note: Please set up the SMTP first and then go to *Advanced* tab to configure recipients, see page 151.

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:



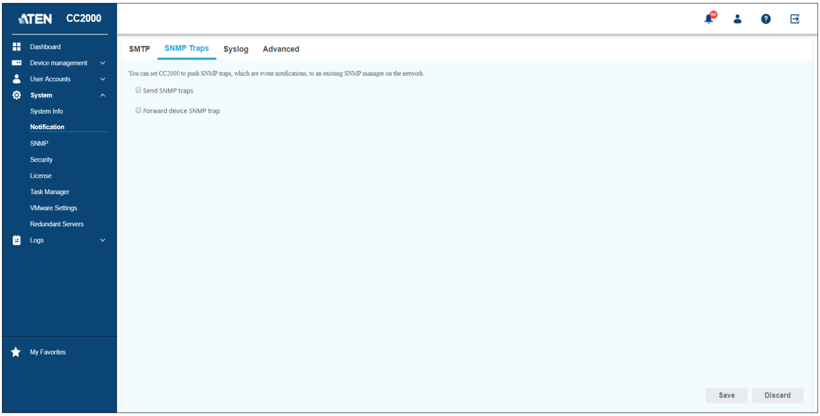
8. Key in an email address for the recipient of the test email then click **Send**. If the settings have been configured correctly, the recipient will receive the test email.

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:



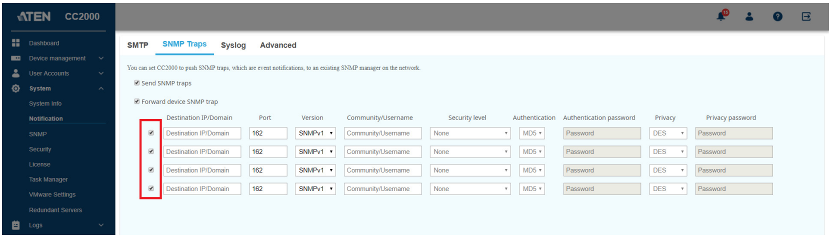
You can set CC2000 to push SNMP traps, which are event notifications, to an existing SNMP manager on the network.

□ Send SNMP traps

□ Forward device SNMP trap

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.



You can set CC2000 to push SNMP traps, which are event notifications, to an existing SNMP manager on the network.

☑ Send SNMP traps

☑ Forward device SNMP trap

	Destination IP/Domain	Port	Version	Community/Username	Security level	Authentication	Authentication password	Privacy	Privacy password
☑	Destination IP/Domain	162	SNMPv1	Community/Username	None	MD5	Password	DES	Password
☑	Destination IP/Domain	162	SNMPv1	Community/Username	None	MD5	Password	DES	Password
☑	Destination IP/Domain	162	SNMPv1	Community/Username	None	MD5	Password	DES	Password
☑	Destination IP/Domain	162	SNMPv1	Community/Username	None	MD5	Password	DES	Password

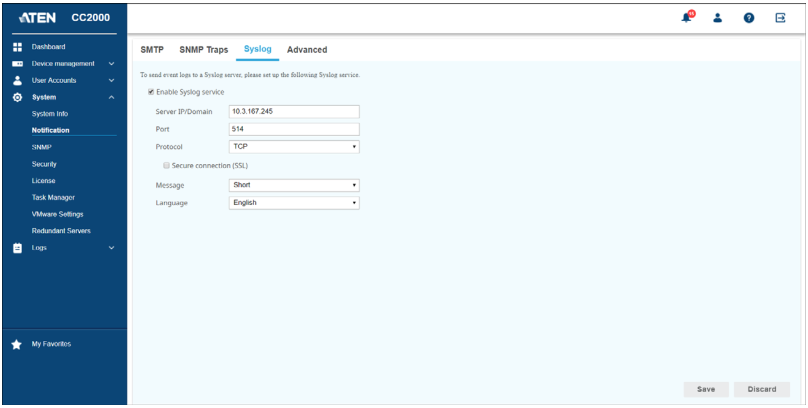
4. Key in the IP address(es) in the **Destination IP/Domain** field and the service port number(s) in the **Port** field of the manager computer(s) to be notified of SNMP trap events. The valid port range is 1–65535. The default port number is 162.

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 send event logs to a Syslog server, please set up the following Syslog service.

☑ Enable Syslog service

Server IP/Domain: 10.3.167.245

Port: 514

Protocol: TCP

□ Secure connection (SSL)

Message: Short

Language: English

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).

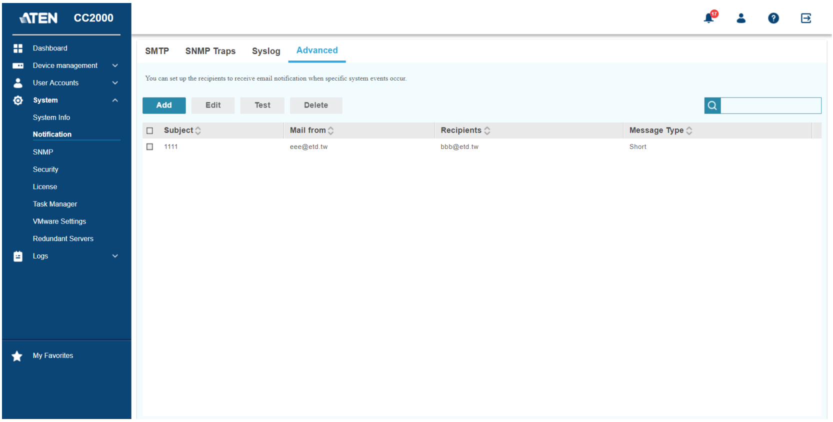
4. Use the drop-down menu **Message** to select whether to log a short message or a full message.

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 specified users of specified events that occurred on the CC2000. When you select Advanced, a page similar to the one below appears:



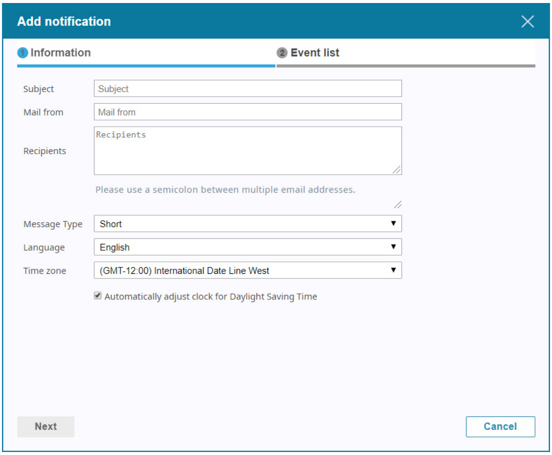
You can set up the recipients to receive email notification when specific system events occur.

□	Subject	Mail from	Recipients	Message Type
□	1111	eee@etd.tw	bbb@etd.tw	Short

Adding Notification Settings

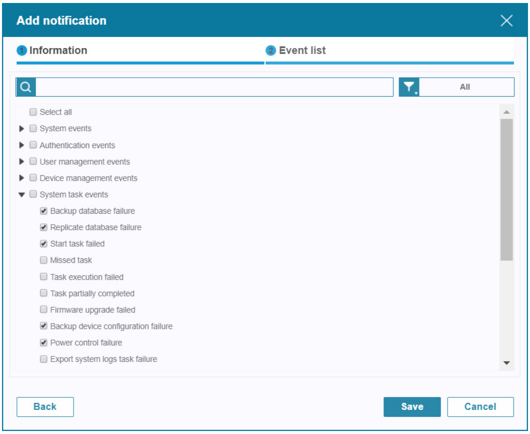
There are four buttons in the Advanced page: Add, Edit, Test, and Delete. Follow the instructions below to add users and specify the events they will receive notification of.

1. Click **Add** for the Add notification page:



Subject: Subject
Mail from: Mail from
Recipients: Recipients
Please use a semicolon between multiple email addresses.
Message Type: Short
Language: English
Time zone: (GMT-12:00) International Date Line West
☑ Automatically adjust clock for Daylight Saving Time

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.



- □ Select all
- ▶ □ System events
- ▶ □ Authentication events
- ▶ □ User management events
- ▶ □ Device management events
- ▼ □ System task events
  - ☑ Backup database failure
  - ☑ Replicate database failure
  - ☑ Start task failed
  - □ Missed task
  - □ Task execution failed
  - □ Task partially completed
  - □ Firmware upgrade failed
  - ☑ Backup device configuration failure
  - ☑ Power control failure
  - □ Export system logs task failure

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 147 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.

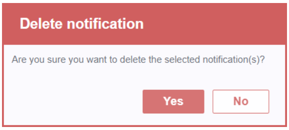
Testing Event Notifications

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.

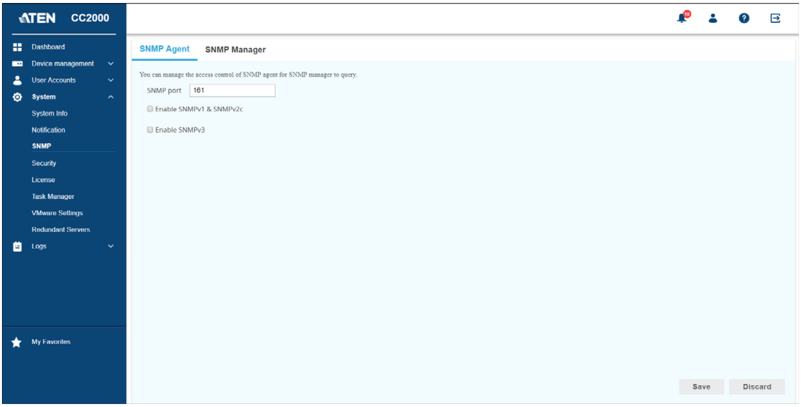


Delete notification

Are you sure you want to delete the selected notification(s)?

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:



You can manage the access control of SNMP agent for SNMP manager to query.

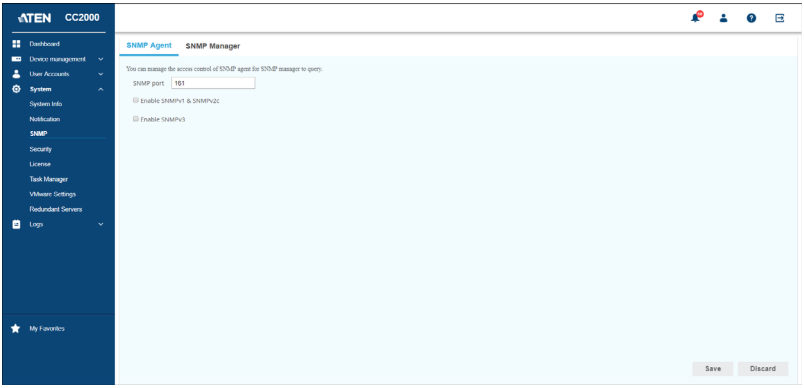
SNMP port 161

□ Enable SNMPv1 & SNMPv2c

□ Enable SNMPv3

SNMP Agent

The SNMP Agent page lets you set the CC2000's agents and control access for SNMP trap events as detailed below:



You can manage the access control of SNMP agent for SNMP manager to query.

SNMP port 161

□ Enable SNMPv1 & SNMPv2c

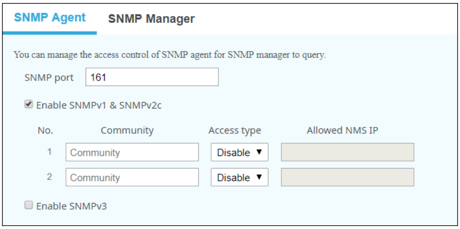
□ Enable SNMPv3

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.



You can manage the access control of SNMP agent for SNMP manager to query.

SNMP port 161

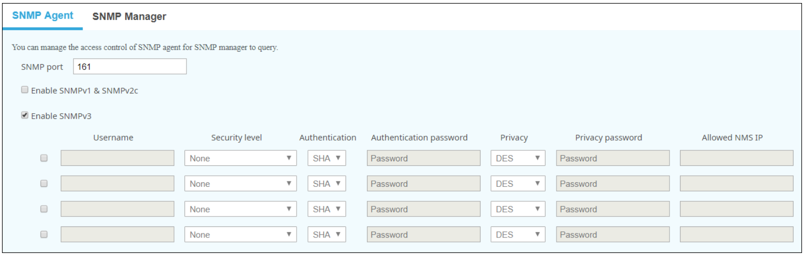
☑ Enable SNMPv1 & SNMPv2c

No.	Community	Access type	Allowed NMS IP
1	Community	Disable ▼	
2	Community	Disable ▼	

□ Enable SNMPv3

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.



You can manage the access control of SNMP agent for SNMP manager to query.

SNMP port 161

□ Enable SNMPv1 & SNMPv2c

☑ Enable SNMPv3

	Username	Security level	Authentication	Authentication password	Privacy	Privacy password	Allowed NMS IP
□		None ▼	SHA ▼	Password	DES ▼	Password	
□		None ▼	SHA ▼	Password	DES ▼	Password	
□		None ▼	SHA ▼	Password	DES ▼	Password	
□		None ▼	SHA ▼	Password	DES ▼	Password	

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.

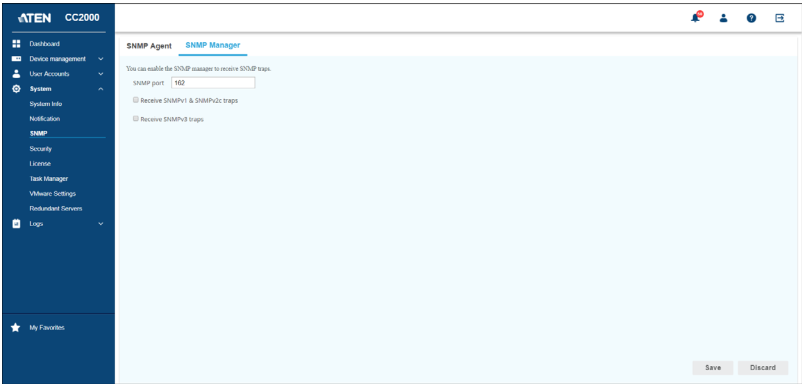
8. Key in the allowed NMS IP address that correspond to each of the profiles in the Allowed NMS IP field.

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:



You can enable the SNMP manager to receive SNMP traps.

SNMP port 162

□ Receive SNMPv1 & SNMPv2c traps

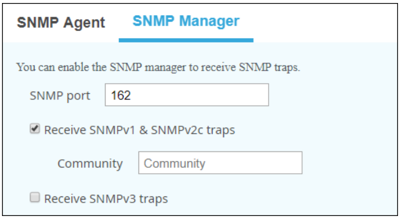
□ Receive SNMPv3 traps

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.



You can enable the SNMP manager to receive SNMP traps.

SNMP port 162

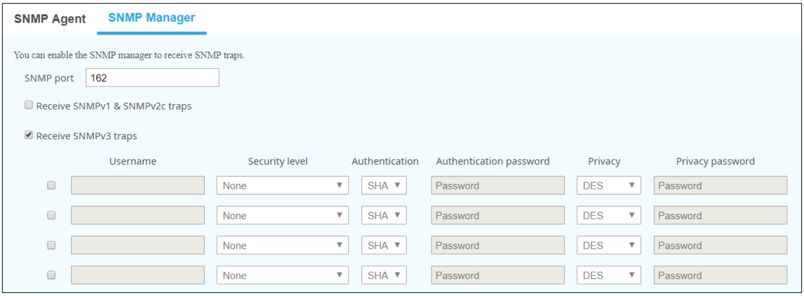
☑ Receive SNMPv1 & SNMPv2c traps

Community Community

□ Receive SNMPv3 traps

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.



You can enable the SNMP manager to receive SNMP traps.

SNMP port 162

□ Receive SNMPv1 & SNMPv2c traps

☑ Receive SNMPv3 traps

	Username	Security level	Authentication	Authentication password	Privacy	Privacy password
□		None ▼	SHA ▼	Password	DES ▼	Password
□		None ▼	SHA ▼	Password	DES ▼	Password
□		None ▼	SHA ▼	Password	DES ▼	Password
□		None ▼	SHA ▼	Password	DES ▼	Password

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.

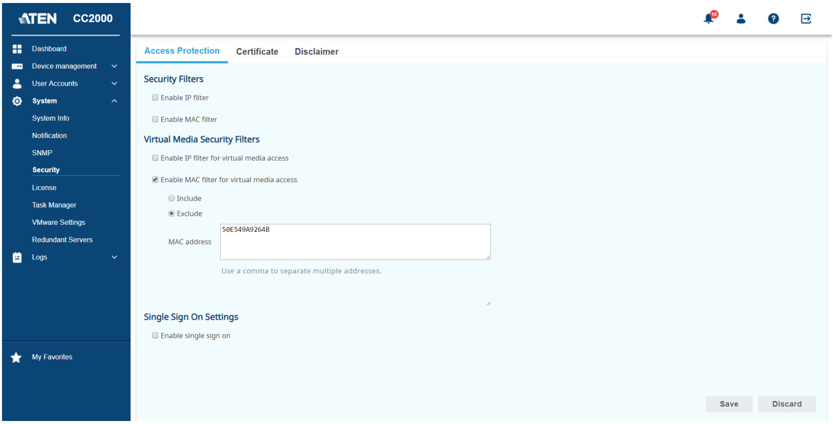
7. Select the **Privacy** protocols and key in the privacy password(s) in the Privacy password field.

8. Click **Save** to save your settings.

Note: Make sure all the fields are filled in correctly so the system can successfully save your configurations.

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:



Security Filters

□ Enable IP filter

□ Enable MAC filter

Virtual Media Security Filters

□ Enable IP filter for virtual media access

☑ Enable MAC filter for virtual media access

○ Include

● Exclude

MAC address: 50E549A9264B

Use a comma to separate multiple addresses.

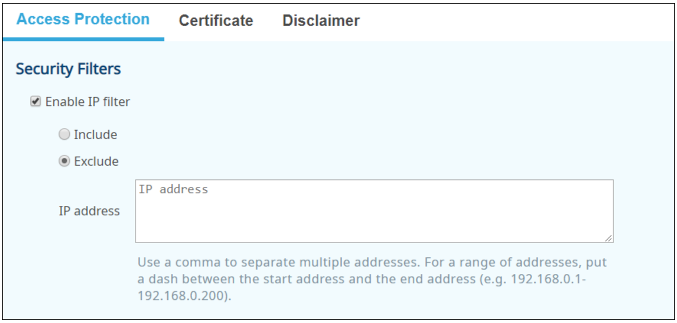
Single Sign On Settings

□ Enable single sign on

Access Protection

IP Filtering

IP filtering controls access to the CC2000 based on the IP addresses of the computers attempting to connect to it.



Security Filters

☑ Enable IP filter

○ Include

● Exclude

IP address: IP address

Use a comma to separate multiple addresses. For a range of addresses, put a dash between the start address and the end address (e.g. 192.168.0.1-192.168.0.200).

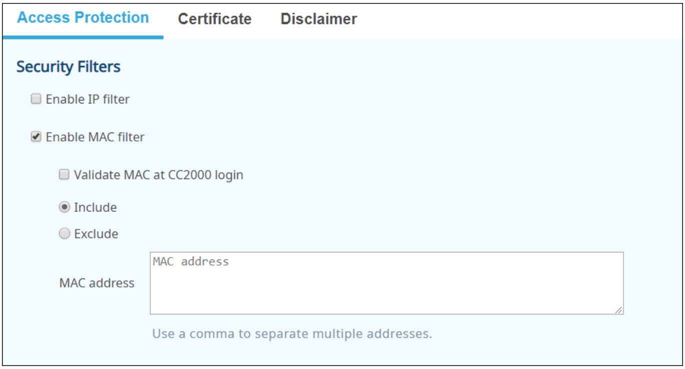
- To enable IP filtering, check the **Enable IP filter** checkbox.
  - If the **Include** button is selected, all the addresses specified in the Address List are allowed access while all others are denied access.

- 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.



Security Filters

□ Enable IP filter

☑ Enable MAC filter

□ Validate MAC at CC2000 login

● Include

○ Exclude

MAC address: MAC address

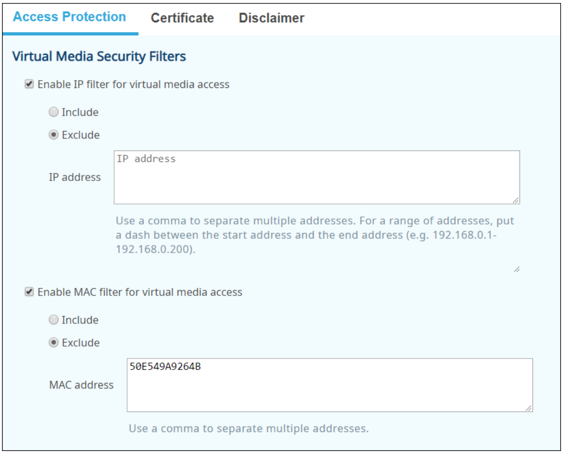
Use a comma to separate multiple addresses.

- 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.



Virtual Media Security Filters

☑ Enable IP filter for virtual media access

○ Include

● Exclude

IP address: IP address

Use a comma to separate multiple addresses. For a range of addresses, put a dash between the start address and the end address (e.g. 192.168.0.1-192.168.0.200).

☑ Enable MAC filter for virtual media access

○ Include

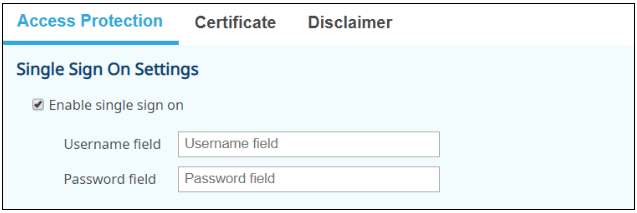
● Exclude

MAC address: 50E549A9264B

Use a comma to separate multiple addresses.

- 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 159 or *MAC Filtering*, page 160.
- Click **Save** to save your settings.

Single Sign On Settings



Single Sign On Settings

☑ Enable single sign on

Username field: Username field

Password field: Password field

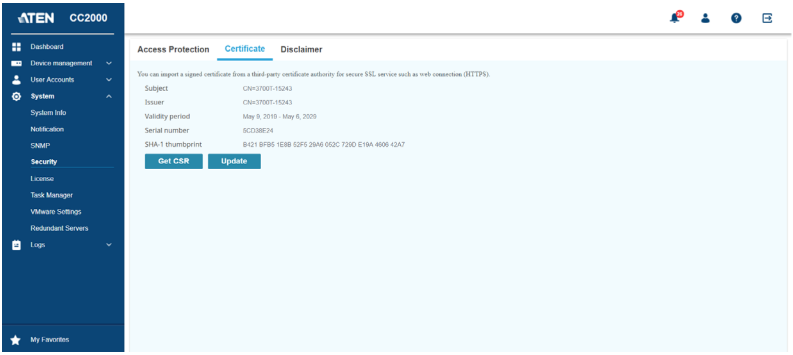
If **Single Sign On Settings** is enabled, it will allow users from another web application to log in CC2000 automatically through a form-based authentication. To integrate, please refer to *SSO HTML Sample Codes* on page 281.

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:



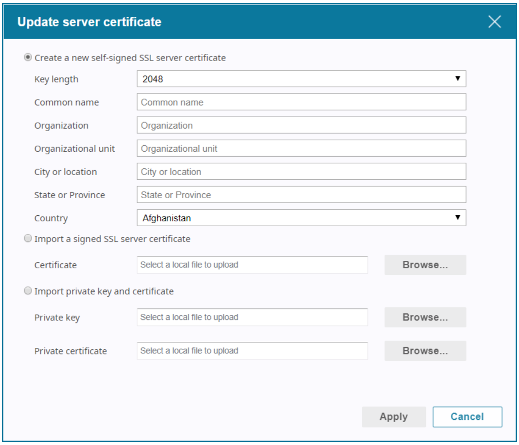
You can import a signed certificate from a third-party certificate authority for secure SSL service such as web connection (HTTPS).

Subject	CN=3700T-15243
Issuer	CN=3700T-15243
Validity period	May 9, 2019 - May 6, 2029
Serial number	5CD38E24
SHA-1 thumbprint	B421 BFB5 1E8B 52F5 29A6 052C 729D E19A 4606 42A7

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:



Update server certificate

● Create a new self-signed SSL server certificate

Key length: 2048

Common name: Common name

Organization: Organization

Organizational unit: Organizational unit

City or location: City or location

State or Province: State or Province

Country: Afghanistan

○ Import a signed SSL server certificate

Certificate: Select a local file to upload — Browse...

○ Import private key and certificate

Private key: Select a local file to upload — Browse...

Private certificate: Select a local file to upload — Browse...

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.

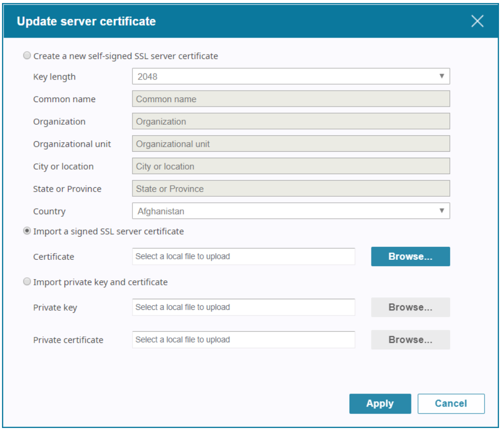
   At this point you are brought back to the beginning of the login sequence where you must go through the procedure of accepting the security certificate and logging in.

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.



Update server certificate

○ Create a new self-signed SSL server certificate

Key length: 2048

Common name: Common name

Organization: Organization

Organizational unit: Organizational unit

City or location: City or location

State or Province: State or Province

Country: Afghanistan

● Import a signed SSL server certificate

Certificate: Select a local file to upload

○ Import private key and certificate

Private key: Select a local file to upload

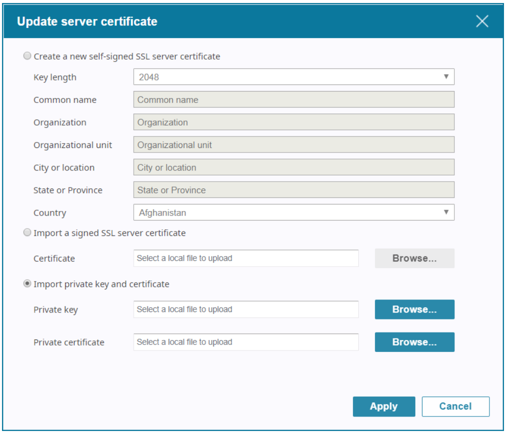
Private certificate: Select a local file to upload

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.



Update server certificate

○ Create a new self-signed SSL server certificate

Key length: 2048

Common name: Common name

Organization: Organization

Organizational unit: Organizational unit

City or location: City or location

State or Province: State or Province

Country: Afghanistan

○ Import a signed SSL server certificate

Certificate: Select a local file to upload

● Import private key and certificate

Private key: Select a local file to upload

Private certificate: Select a local file to upload

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 239 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.

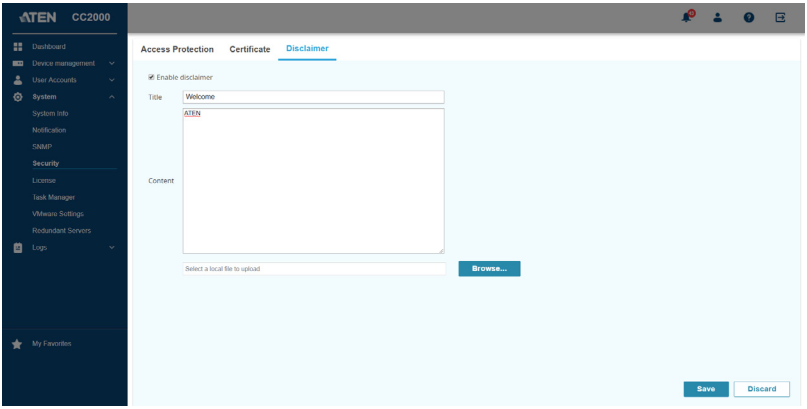
3. Click **Browse** on the right of **Private certificate**, locate your certificate file and select it.
4. Click **Apply** at the bottom-right of the panel.

Note: Both the private encryption key and the signed certificate must be imported at the same time.

Disclaimer

A disclaimer notice can be setup on the CC2000 server for users to accept when he/she logs into CC2000.

To setup a disclaimer, check the Enable disclaimer checkbox, enter the title and content of the disclaimer and click **Save**.



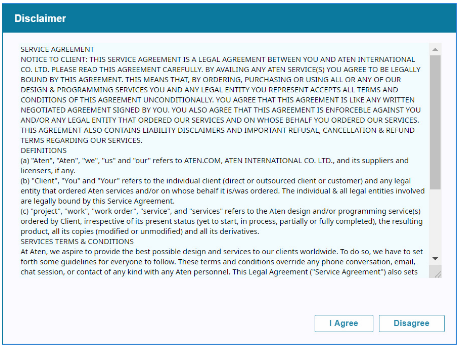
☑ Enable disclaimer

Title: Welcome

Content: ATEN

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:

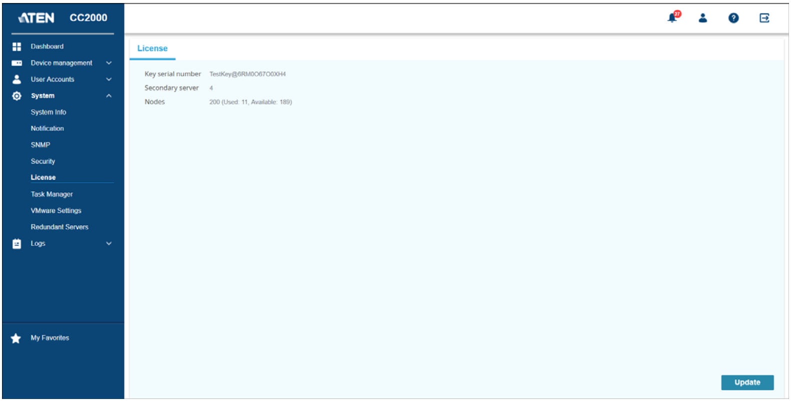

Disclaimer

SERVICE AGREEMENT
NOTICE TO CLIENT: THIS SERVICE AGREEMENT IS A LEGAL AGREEMENT BETWEEN YOU AND ATEN INTERNATIONAL CO. LTD. PLEASE READ THIS AGREEMENT CAREFULLY. BY AVAILING ANY ATEN SERVICE(S) YOU AGREE TO BE LEGALLY BOUND BY THIS AGREEMENT. THIS MEANS THAT, BY ORDERING, PURCHASING OR USING ALL OR ANY OF OUR DESIGN & PROGRAMMING SERVICES YOU AND ANY LEGAL ENTITY YOU REPRESENT ACCEPTS ALL TERMS AND CONDITIONS OF THIS AGREEMENT UNCONDITIONALLY. YOU AGREE THAT THIS AGREEMENT IS LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU. YOU ALSO AGREE THAT THIS AGREEMENT IS ENFORCEBLE AGAINST YOU AND/OR ANY LEGAL ENTITY THAT ORDERED OUR SERVICES AND ON WHOSE BEHALF YOU ORDERED OUR SERVICES. THIS AGREEMENT ALSO CONTAINS LIABILITY DISCLAIMERS AND IMPORTANT REFUSAL, CANCELLATION & REFUND TERMS REGARDING OUR SERVICES.
DEFINITIONS
(a) "Aten", "Aten", "we", "us" and "our" refers to ATEN.COM, ATEN INTERNATIONAL CO. LTD., and its suppliers and licensers, if any.
(b) "Client", "You" and "Your" refers to the individual client (direct or outsourced client or customer) and any legal entity that ordered Aten services and/or on whose behalf it is/was ordered. The individual & all legal entities involved are legally bound by this Service Agreement.
(c) "project", "work", "work order", "service", and "services" refers to the Aten design and/or programming service(s) ordered by Client, irrespective of its present status (yet to start, in process, partially or fully completed), the resulting product, all its copies (modified or unmodified) and all its derivatives.
SERVICES TERMS & CONDITIONS
At Aten, we aspire to provide the best possible design and services to our clients worldwide. To do so, we have to set forth some guidelines for everyone to follow. These terms and conditions override any phone conversation, email, chat session, or contact of any kind with any Aten personnel. This Legal Agreement ("Service Agreement") also sets

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 nodes), you must upgrade the license.

When you select **License** from the System menu, a page similar to the one below appears:



Key serial number TestKey@6RM0O67O0XH4
Secondary server 4
Nodes 200 (Used: 11, Available: 189)

The meanings of the page items are described in the table below:

Item	Description
Key serial number	The serial number of the license key. **Note:** This is different from the software serial number that you used when installing the CC2000 server. The license serial number can be found on the key.
Secondary server	The total number of Secondary server on the installation (up to 31 units – depending on the license purchase).
Nodes	The total number of nodes permitted on the installation according to the license purchase. **Note:** The number of nodes that can be licensed is unlimited – it depends on the license purchase.

Updating the License

To update the license:

1. Contact your dealer to obtain a license key for the number of Secondaries and nodes you want to be able to access.
2. Insert the license key into a USB port on your Primary server.

3. Click **Update** at the bottom-right of the License panel.

Note: 1. Once the update has completed, it is no longer necessary to keep the key plugged into the USB port. Remove the key and place it somewhere safe, since you will need it for future updates.

2. 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.

3. 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.

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 190).

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 created for management (see *Preliminary Procedures*, page 44).

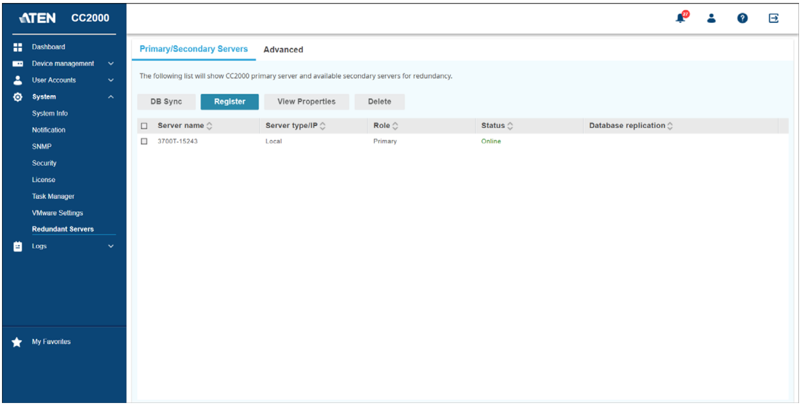
When devices are added to the CC2000 management system the default configuration is for them to be locked. Although their configuration information is stored by the CC2000, they cannot be managed.

Locked ports can be unlocked either by selecting a physical port and unlocking it by clicking the **Unlock** button (see *Locking / Unlocking Devices*, page 88), or by making the port part of an aggregate device (see *Adding an Aggregate Device*, page 68).

If all the licenses are in use, only if a currently unlocked port is locked, or if an aggregate device is deleted – thereby freeing up the license it was using – can a locked port (or new aggregate device) use that license to become unlocked and be capable of being managed by the CC2000 management system.

License Conflict

If there are two Primaries on the same network segment that have been upgraded with the same license key, a license conflict will occur. The Browser GUI of the CC2000 server that was the second one to be installed, will open to a page that looks similar to the one below:



The following list will show CC2000 primary server and available secondary servers for redundancy.

□	Server name	Server type/IP	Role	Status	Database replication
□	3700T-15243	Local	Primary	Online	

To confirm that a conflict has occurred, click the **Logs** tab. A sentence like the following will appear in the log file: A license violation has been detected at Primary server. Remote CC server (IP: [the conflicting servers’ IP]).

If this occurs there are a number of ways to resolve the conflict:

1. On one of the two Primaries: either shut it down, or stop service, or disconnect it from the network, or uninstall the CC2000.
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 one of the CC2000 servers.

Task Manager

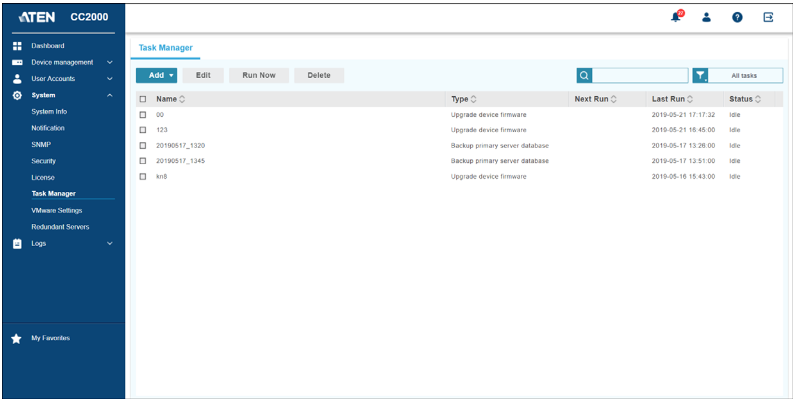
The **Task Manager** menu offers four configuration choices: **Add**, **Edit**, **Run Now**, and **Delete**. This page allows authorized administrators to perform a number of system maintenance tasks. The tasks that can be performed are determined by the user’s type, and the authorization options that 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 243, for details.

- Power control a device
- Auto upgrade with 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, a screen similar to the one below appears:



□	Name	Type	Next Run	Last Run	Status
□	00	Upgrade device firmware		2019-05-21 17:17:32	Idle
□	123	Upgrade device firmware		2019-05-21 16:45:00	Idle
□	20190517_1320	Backup primary server database		2019-05-17 13:26:00	Idle
□	20190517_1345	Backup primary server database		2019-05-17 13:51:00	Idle
□	kn8	Upgrade device firmware		2019-05-16 15:43:00	Idle

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 its database on the Primary it is connected to (see *Replicate Database*, page 187).

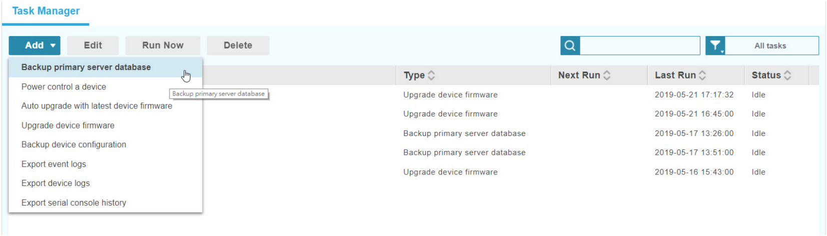
The **Task Manager** table lists all the tasks that have been configured. The meanings of each headings are explained in the table below:

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

Add

To add a task, do the following:

1. Click **Add** a list of task choices:


Task Manager
Add
Edit
Run Now
Delete
All tasks
Backup primary server database
Power control a device
Auto upgrade with latest device firmware
Upgrade device firmware
Backup device configuration
Export event logs
Export device logs
Export serial console history
Backup primary server database

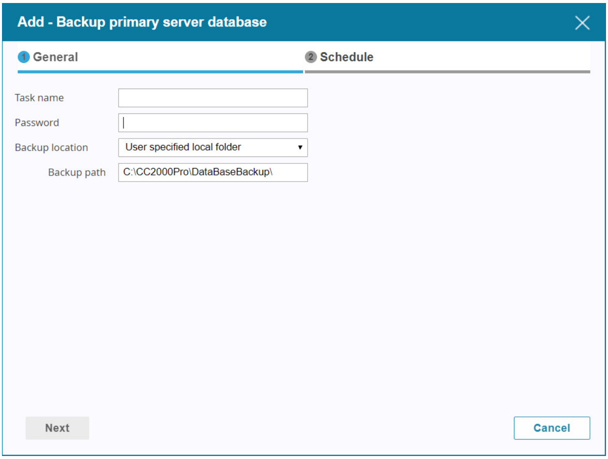
Type	Next Run	Last Run	Status
Upgrade device firmware		2019-05-21 17:17:32	Idle
Upgrade device firmware		2019-05-21 16:45:00	Idle
Backup primary server database		2019-05-17 13:26:00	Idle
Backup primary server database		2019-05-17 13:51:00	Idle
Upgrade device firmware		2019-05-16 15:43:00	Idle

2. Click to select the task you want to add. A pop-up window appears and the content depends on the selected task.

While each of the tasks is different, for the most part the procedures involved in setting them up are similar. The following examples take you through the various task procedures you will encounter.

Backup Primary Server Database

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



Add - Backup primary server database

Task name
Password
Backup location: User specified local folder
Backup path: C:\CC2000Pro\DataBaseBackup\

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

Note: 1. This task is only available on the Primary server.

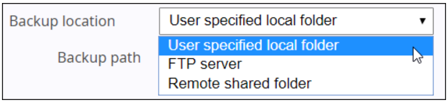
2. The password is required. If you set one, make a note of it and store it in a safe place. You will need it when restoring the database. (If you don't set a password you can restore the database without one.) See *Restore*, page 243, for information on restoring the database.

3. The password cannot exceed the equivalent of 32 English alphanumeric characters.

4. The extension of the backup file is cbk (`*.cbk`).

---

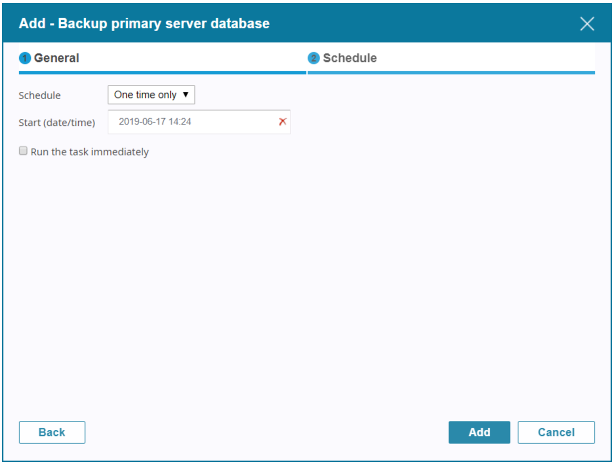
2. Select the **Backup location** where you want to store the backup file in. There are three options to choose from, **User specified local folder**, **FTP server**, and **Remote shared folder**.



- The default setting is for the backup file to be stored in a local directory based on the directory that the CC2000 was installed in. For example, `C:\CC2000\DataBaseBackup`.

- Fill in the rest of the fields if you choose FTP server or Remote shared folder.

3. When you have filled in the all the informations, click **Next** for the Schedule page.

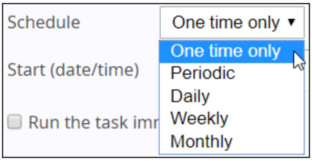


Schedule: One time only ▼

Start (date/time): 2019-06-17 14:24

□ Run the task immediately

4. Use the drop-down menu Schedule to see a list of available choices.

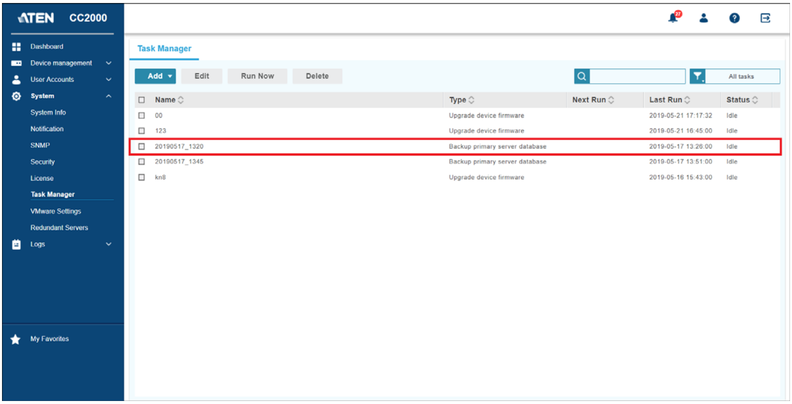


Depending on what you select for the Schedule, further scheduling choices may appear. For examples, if you choose One time only, the Start (date/time) appears. If you choose Periodic, the Optional period field appears.

Note: If you set a time in the schedule for the backup to take place (Monthly, for example), but you want it to start with 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 will have passed by the time you save your changes. Which means that 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.

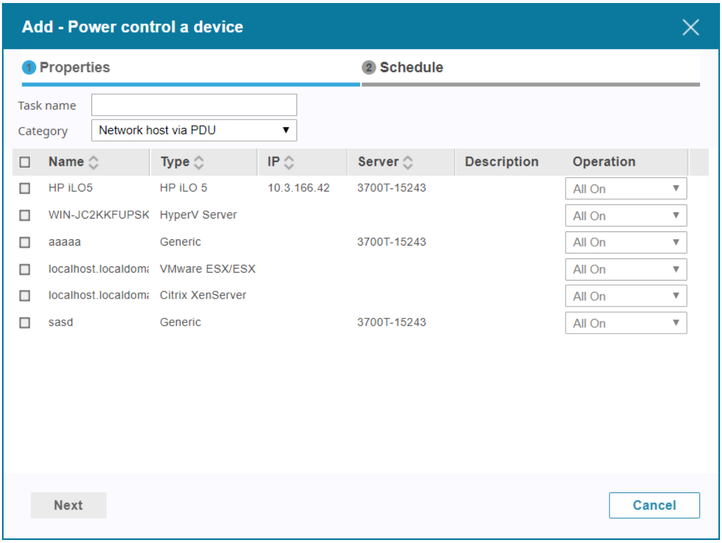


☐	Name	Type	Next Run	Last Run	Status
☐	00	Upgrade device firmware		2019-05-21 17:17:32	Idle
☐	123	Upgrade device firmware		2019-05-21 16:45:00	Idle
☐	20190517_1320	Backup primary server database		2019-05-17 13:26:00	Idle
☐	20190517_1345	Backup primary server database		2019-05-17 13:51:00	Idle
☐	kn8	Upgrade device firmware		2019-05-16 15:43:00	Idle

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.



Task name

Category: Network host via PDU

☐	Name	Type	IP	Server	Description	Operation
☐	HP iLO5	HP iLO 5	10.3.166.42	3700T-15243		All On
☐	WIN-JC2KKFUPSK	HyperV Server				All On
☐	aaaaa	Generic		3700T-15243		All On
☐	localhost.localdom:	VMware ESX/ESX				All On
☐	localhost.localdom:	Citrix XenServer				All On
☐	sasd	Generic		3700T-15243		All On

1. Provide a name for the task.

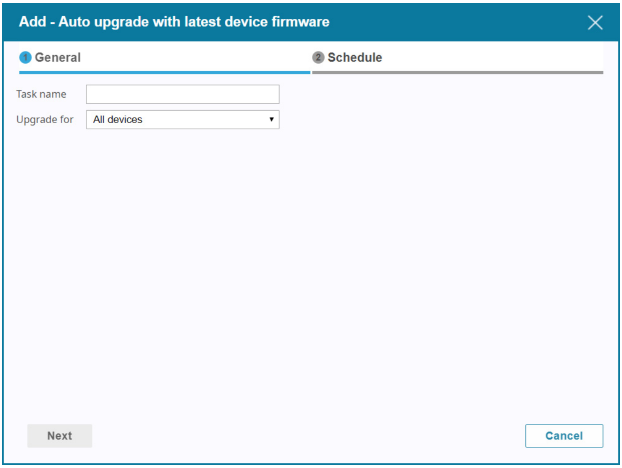
2. Choose to turn on or off for the selected device as a whole, or on a port-by-port basis by clicking and selecting from the Category drop-down menu.
3. Check the checkbox of the target devices or ports you want to control, or check the checkbox in front of Name at the top of the column to select all of them.
4. Select whether to turn the ports On or Off in the Operation column.
5. Click **Next** for the Schedule page.
6. Make your schedule choices in the Schedule page.

Note: Refer to *Backup Primary Server Database* on page 173 as the schedule page is similar.

7. Click **Add** to finish setting up the task.

Auto upgrade with latest device firmware

This task allows you to schedule auto device firmware upgrade with the newest available firmware.



Add - Auto upgrade with latest device firmware

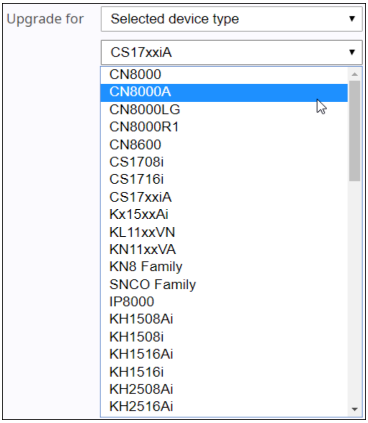
Task name:

Upgrade for: All devices

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.

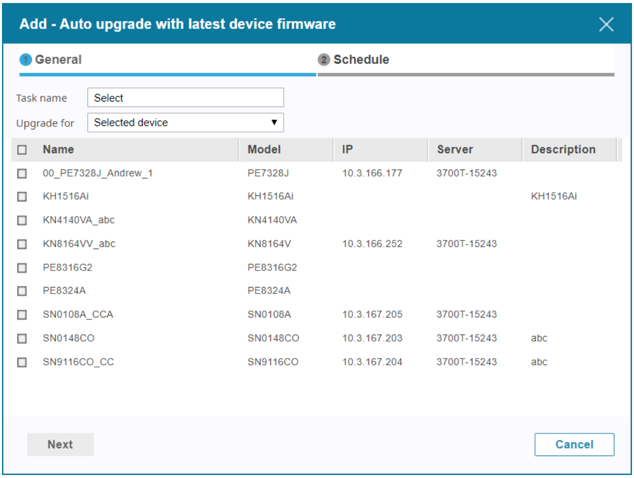


Upgrade for: Selected device type ▾

CS17xxiA ▾

   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.



Add - Auto upgrade with latest device firmware

Task name: Select

Upgrade for: Selected device ▾

□	Name	Model	IP	Server	Description
□	00_PE7328J_Andrew_1	PE7328J	10.3.166.177	3700T-15243	
□	KH1516Ai	KH1516Ai			KH1516Ai
□	KN4140VA_abc	KN4140VA			
□	KN8164VV_abc	KN8164V	10.3.166.252	3700T-15243	
□	PE8316G2	PE8316G2			
□	PE8324A	PE8324A			
□	SN0108A_CCA	SN0108A	10.3.167.205	3700T-15243	
□	SN0148CO	SN0148CO	10.3.167.203	3700T-15243	abc
□	SN9116CO_CC	SN9116CO	10.3.167.204	3700T-15243	abc

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

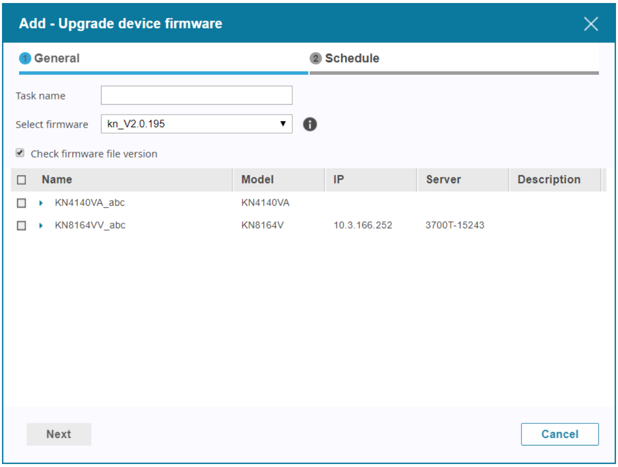
5. Make your schedule choices in the Schedule page.

Note: Refer to *Backup Primary Server Database* on page 173 as the schedule page is similar.

6. 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.



Task name

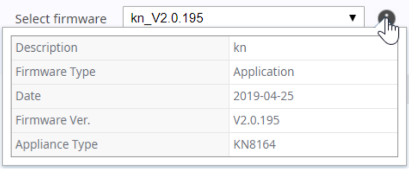
Select firmware: kn_V2.0.195

☑ Check firmware file version

□	Name	Model	IP	Server	Description
□	KN4140VA_abc	KN4140VA			
□	KN8164VV_abc	KN8164V	10.3.166.252	3700T-15243	

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:



Select firmware: kn_V2.0.195

Description	kn
Firmware Type	Application
Date	2019-04-25
Firmware Ver.	V2.0.195
Appliance Type	KN8164

3. Selecting a firmware file will display all the devices available for firmware upgrade in the table below.

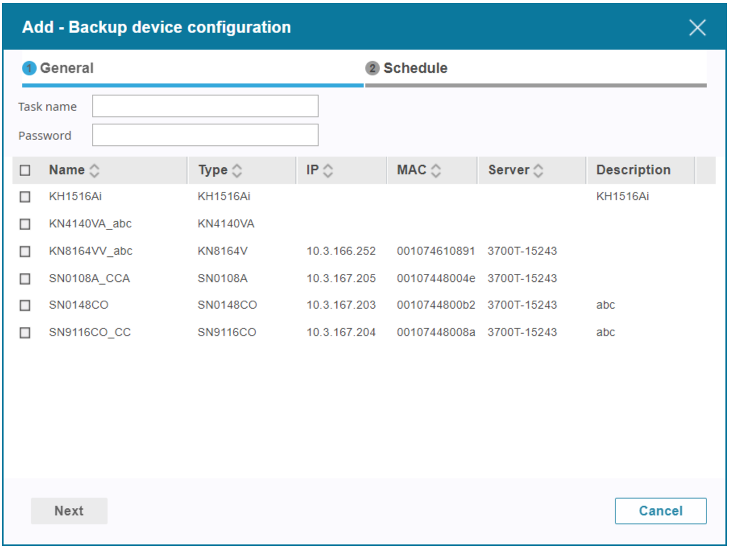
4. Check the checkbox(es) of the device you wish to upgrade and click **Next**.
5. When finished, click **Next** for the Schedule page.
6. Make your schedule choices in the Schedule page.

Note: Refer to *Backup Primary Server Database* on page 173 as the schedule page is similar.

7. When finished, click **Add** to add the task.

Backup Device Configuration

When you choose the Backup device configuration task, the following page appears:



Task name

Password

□	Name	Type	IP	MAC	Server	Description
□	KH1516Ai	KH1516Ai				KH1516Ai
□	KN4140VA_abc	KN4140VA				
□	KN8164VV_abc	KN8164V	10.3.166.252	001074610891	3700T-15243	
□	SN0108A_CCA	SN0108A	10.3.167.205	00107448004e	3700T-15243	
□	SN0148CO	SN0148CO	10.3.167.203	0010744800b2	3700T-15243	abc
□	SN9116CO_CC	SN9116CO	10.3.167.204	00107448008a	3700T-15243	abc

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

Note: Make a note of the password and store it in a safe place. You will need it when restoring the configuration. See *Restore Configuration*, page 107 for restoration details.

2. In the Device list, check the checkbox of the name of the device(s) you want to back up.
3. When finished, click **Next** for the Schedule page.

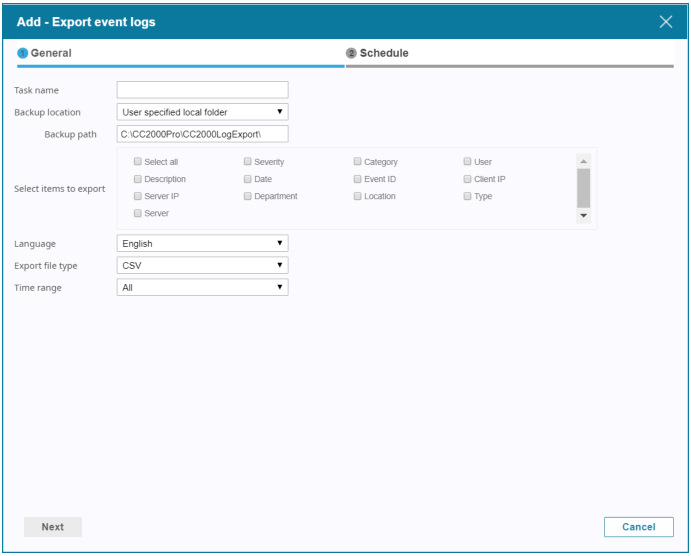
4. Make your schedule choices in the Schedule page.

Note: Refer to *Backup Primary Server Database* on page 173 as the schedule page is similar.

5. When finished, click **Add** to add the task.

Export Event Logs

When you choose the Export event logs task, the following page appears:



Task name

Backup location: User specified local folder

Backup path: C:\CC2000Pro\CC2000LogExport\

Select items to export:
□ Select all □ Severity □ Category □ User
□ Description □ Date □ Event ID □ Client IP
□ Server IP □ Department □ Location □ Type
□ Server

Language: English

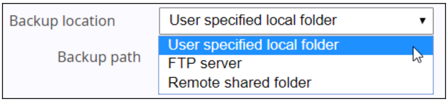
Export file type: CSV

Time range: All

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 a server's records you must look at its particular file. You can identify the file by means of the Task name you gave it.

2. Select the **Backup location** where you want to store the backup file in. There are three options to choose from, **User specified local folder**, **FTP server**, and **Remote shared folder**.



- The default setting is for the backup file to be stored in a local directory based on the directory that the CC2000 was installed in. For example, `C:\CC2000\DataBaseBackup`.
- 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 an 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), key a password into the Password field that comes up.

Note: Make a note of the password – you will need it to import the file.

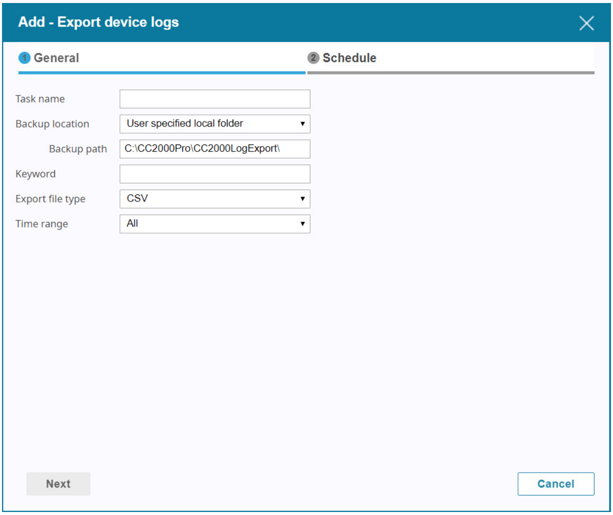
6. In the Time range drop-down menu, there are three options.
   - **All**: Exports all the records in the database.
   - **Since the last time task run**: Exports all the records of tasks since the last time they were ran.
   - **Select time range**: Export records for a particular time and period, set the time parameters with the From and To fields.
7. When finished, click **Next** for the Schedule page.
8. Make your schedule choices in the Schedule page.

Note: Refer to *Backup Primary Server Database* on page 173 as the schedule page is similar.

9. When finished, click **Add** to add the task.

Export Device Logs

The CC2000 also acts as a log server for all ATEN/Altusen devices where CC2000 records the system events that take place on the devices in a database. This task allows you to export the recordings of the device database as a file. When you choose the Export device logs task, the following page appears:



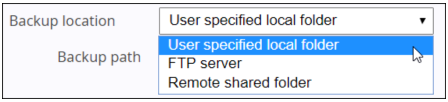
Add - Export device logs

Task name:
Backup location: User specified local folder
Backup path: C:\CC2000Pro\CC2000LogExport\
Keyword:
Export file type: CSV
Time range: All

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 the records you must go to each server to look at its particular file.

2. Select the **Backup location** where you want to store the backup file in. There are three options to choose from, **User specified local folder**, **FTP server**, and **Remote shared folder**.



Backup location: User specified local folder

- The default setting is for the backup file to be stored in a local directory based on the directory that the CC2000 was installed in. For example, `C:\CC2000\DataBaseBackup`.
- 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), key a password into the Password field that comes up.

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 the records in the database.
   - **Since the last time task run**: Exports all the records of tasks since the last time they were ran.
   - **Include**: Export records for a particular time period, set the time parameters with the From and To fields.
   - **Exclude**: Export all records but exclude the records in the time period specified here. Set the time parameters in the From and To fields.
6. When finished, click **Next** for the Schedule page.
7. Make your schedule choices in the Schedule page.

Note: Refer to *Backup Primary Server Database* on page 173 as the schedule page is similar.

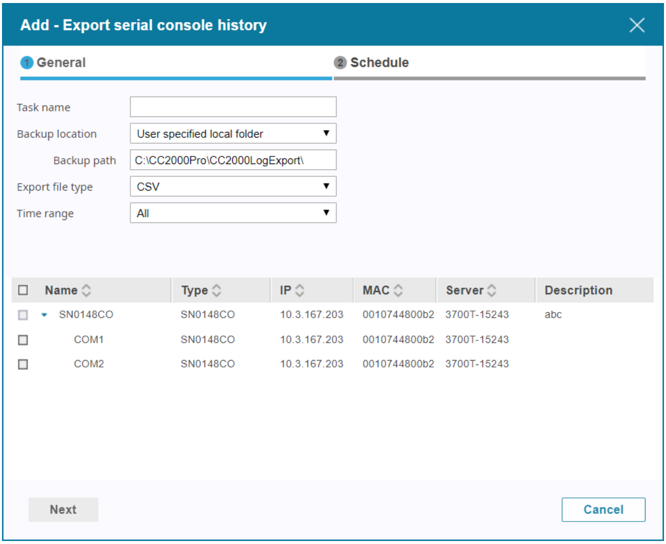
8. When finished, click **Add** to add the task.
9. When you have finished with this page, click **Next** at the bottom-left of the panel for the Schedule page.
10. Make your schedule choices in the Schedule page that comes up.

    Note: The schedule choices are similar to the ones described for the *Backup Primary server database* task.

11. When you have finished making your schedule choices, click **Add**.

Export serial console history

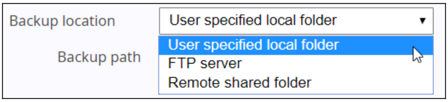
The CC2000 keeps a record of all user sessions that take place (see page 197). This function lets you save the serial console history of each device and export as a file(s). When you choose the Export serial console history task, the following page appears:



Task name:
Backup location: User specified local folder
Backup path: C:\CC2000Pro\CC2000LogExport\
Export file type: CSV
Time range: All

□	Name	Type	IP	MAC	Server	Description
□	▾ SN0148CO	SN0148CO	10.3.167.203	0010744800b2	3700T-15243	abc
□	COM1	SN0148CO	10.3.167.203	0010744800b2	3700T-15243	
□	COM2	SN0148CO	10.3.167.203	0010744800b2	3700T-15243	

1. Provide a name for the task.
2. Select the **Backup location** where you want to store the backup file in. There are three options to choose from, **User specified local folder**, **FTP server**, and **Remote shared folder**.



Backup location: User specified local folder
Backup path

- The default setting is for the backup file to be stored in a local directory based on the directory that the CC2000 was installed in. For example, `C:\CC2000\DataBaseBackup`.
- 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), key a password into the Password field that comes up.

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 the records in the database.
   - **Include**: Export records for a particular time period, set the time parameters with the From and To fields.
   - **Exclude**: Export all records but exclude the records in the time period specified here. Set the time parameters in the From and To fields.
5. For the device list, check the checkbox of the desired device(s), or check the checkbox in front of Name at the top of the column to select all of them.

Note: If you prefer to only export the serial console history for selected ports, instead of clicking the device's checkbox, click the arrowhead in front of the device's name to expand the port list and click to select the ports.

6. When finished, click **Next** for the Schedule page.
7. Make your schedule choices in the Schedule page.

Note: Refer to *Backup Primary Server Database* on page 173 as the schedule page is similar.

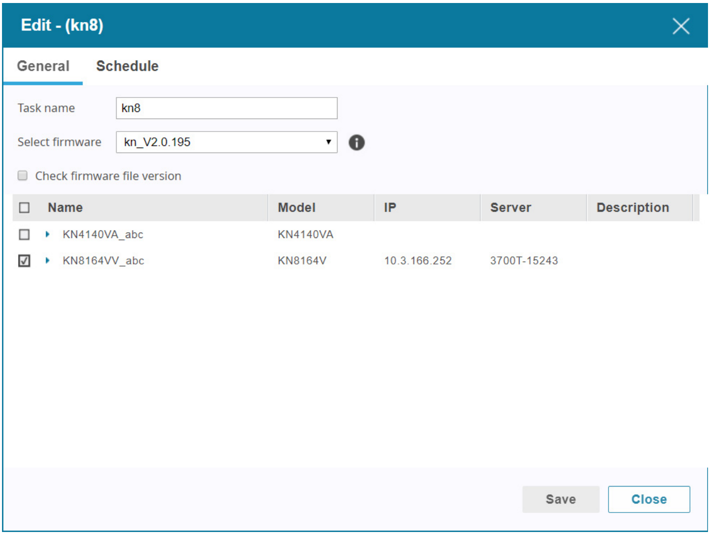
8. When finished, click **Add** to add the task.

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 example is shown:



Task name: kn8

Select firmware: kn_V2.0.195

□ Check firmware file version

□	Name	Model	IP	Server	Description
□	KN4140VA_abc	KN4140VA			
☑	KN8164VV_abc	KN8164V	10.3.166.252	3700T-15243	

For the different tasks and the editable parameters, refer to *Add* on page 172 for more information.

After editing the parameters, click **Save** to finish.

Run Now

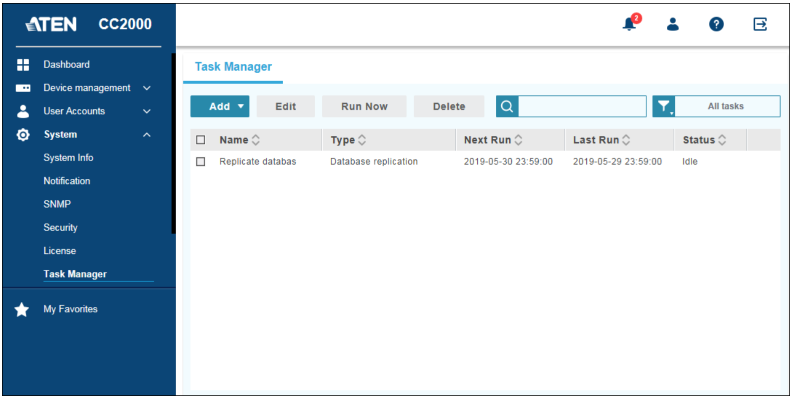
Use **Run Now** to immediately execute the task. Check the checkbox of the task and click **Run Now**.

Deleting a Task

Use **Delete** to delete a 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:



□	Name	Type	Next Run	Last Run	Status
□	Replicate databas	Database replication	2019-05-30 23:59:00	2019-05-29 23:59:00	Idle

When you check the checkbox Replicate Database and click Edit, the Edit page comes up. The procedures are similar to the ones described for the Editing a task. Refer back to page 186 for details, if necessary.

Note: 1. Each CC2000 server maintains its own individual database of the accounts, logs, devices, and access rights that are configured on it. By replicating, it sends all that information 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.

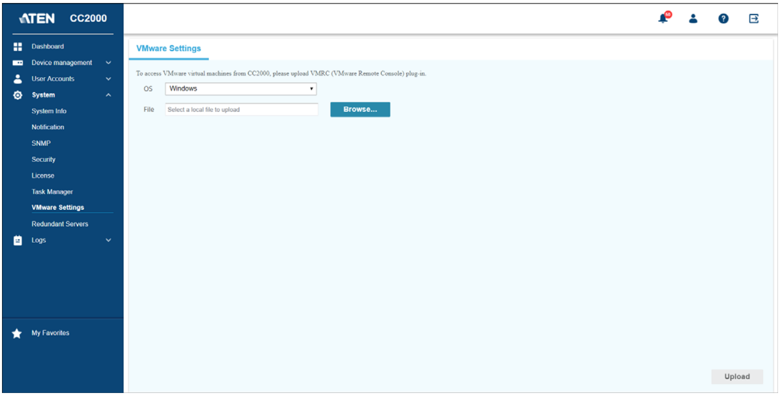
3. The default is for the database to be automatically replicated once a day at 00:00. You can use this page to change the replication schedule, but be aware that setting the replication schedule to too small of a time interval can adversely influence system performance. If you set the schedule to too 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 within 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 access VMware virtual machines from CC2000, please upload VMRC (VMware Remote Console) plug-in.

OS: Windows

File: Select a local file to upload

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 in step one.
4. Click the **Upload** button.

Installing Xterm

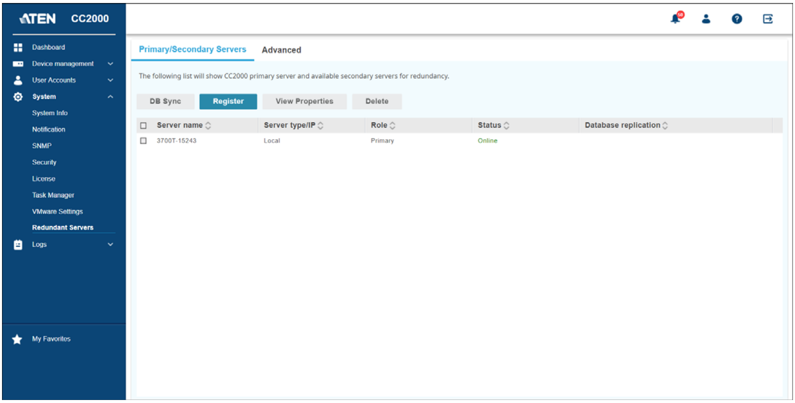
If the operating system of the port you are accessing is running Ubuntu 18.04_x64, CentOS 7.5_x64, or Debian 9.5_x64, you must install Xterm to run VMRC properly.

On terminal, run 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**. The default Redundant Servers page is **Primary/Secondary Servers**, and it looks similar to the one below:



The following list will show CC2000 primary server and available secondary servers for redundancy.

□	Server name	Server type/IP	Role	Status	Database replication
□	3700T-15243	Local	Primary	Online	

Primary/Secondary Servers

The Interactive Display Panel provides a table listing the CC2000 servers, along with some basic information about them. A green online in the status means that the server is currently accessible. A red offline in the status means that it is not currently accessible.

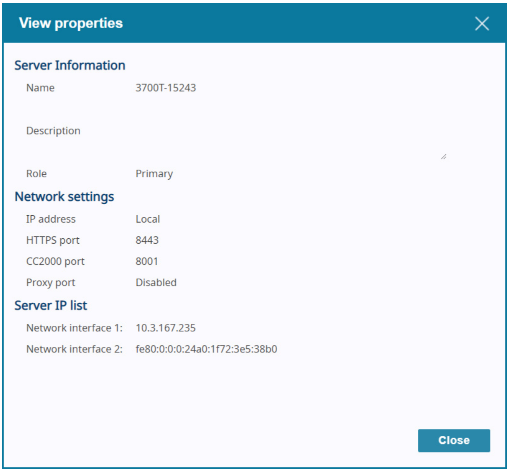
The definitions of the Server table headings are given below:

Heading	Meaning
Server Name	The name given to the server when it was installed.
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 on line. **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 CC2000 to register with the Primary becomes the substitute Primary). 2. The substitute Primary performs the Primary's role in regard to providing centralized management control – it cannot be used to add or delete devices; it can not 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**.



View properties

Server Information

Name 3700T-15243

Description

Role Primary

Network settings

IP address Local

HTTPS port 8443

CC2000 port 8001

Proxy port Disabled

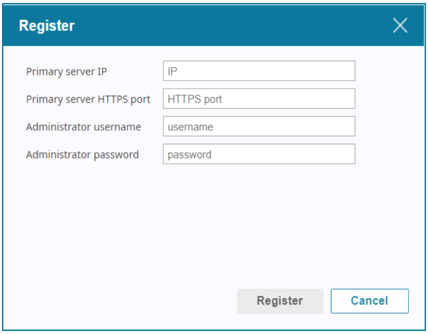
Server IP list

Network interface 1: 10.3.167.235

Network interface 2: fe80:0:0:0:24a0:1f72:3e5:38b0

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.

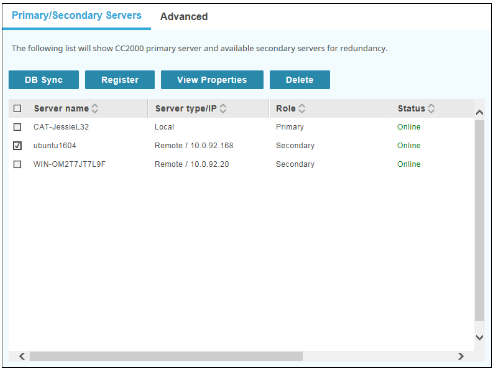
Note: 1. For the *Administrator username* and *Administrator password* fields, you must use a valid Super Administrator’s or System Administrator’s username and password.

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 almost all 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



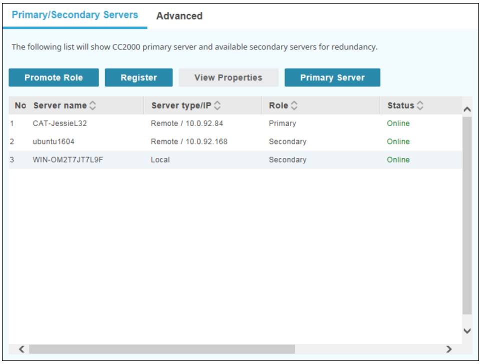
The following list will show CC2000 primary server and available secondary servers for redundancy.

□	Server name	Server type/IP	Role	Status
□	CAT-JessieL32	Local	Primary	Online
☑	ubuntu1604	Remote / 10.0.92.168	Secondary	Online
□	WIN-OM2T7JT7L9F	Remote / 10.0.92.20	Secondary	Online

To delete a secondary server(s), check the checkbox of the secondary server(s) and click **Delete**.

To synchronize primary server database to a secondary server(s), check the secondary server(s) and click **DB Sync**.

Secondary Server View



The following list will show CC2000 primary server and available secondary servers for redundancy.

No	Server name	Server type/IP	Role	Status
1	CAT-JessieL32	Remote / 10.0.92.84	Primary	Online
2	ubuntu1604	Remote / 10.0.92.168	Secondary	Online
3	WIN-OM2T7JT7L9F	Local	Secondary	Online

■ 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 that all CC2000 servers on the installation 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 193, 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 on line. See *Register* on page 191 for details.

■ Primary Server

This function is used under the following conditions:

- 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 key in the new IP address and/or port settings (of the Primary Server) and click **Save**.

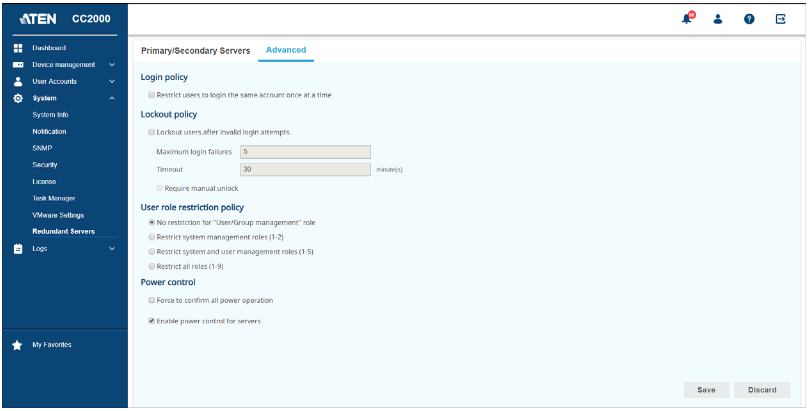
Note: 1. Since the IP address change is made at the OS level (not the CC2000 service level), the CC2000 system is unaware of the change. Therefore Primary can't change this information on the Secondaries automatically. It must be done manually on all Secondaries.

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 on line.

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

□ Restrict users to login the same account once at a time

Lockout policy

□ Lockout users after invalid login attempts.

Maximum login failures: 5

Timeout: 30 minute(s)

□ Require manual unlock

User role restriction policy

● No restriction for "User/Group management" role

○ Restrict system management roles (1-2)

○ Restrict system and user management roles (1-5)

○ Restrict all roles (1-9)

Power control

□ Force to confirm all power operation

☑ Enable power control for servers

Login policy

Check the Restrict users to login in the same account once a 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 be able 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 to enable the lockout function. 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 *Unblock User*, page 124, 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 126.

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 the connected devices regardless of the setting on the outlet.

Enabling Enable power control for servers, means if the third-party servers that supports power control, is allowed to perform power controls. Otherwise, the related power control will be removed from the menu.

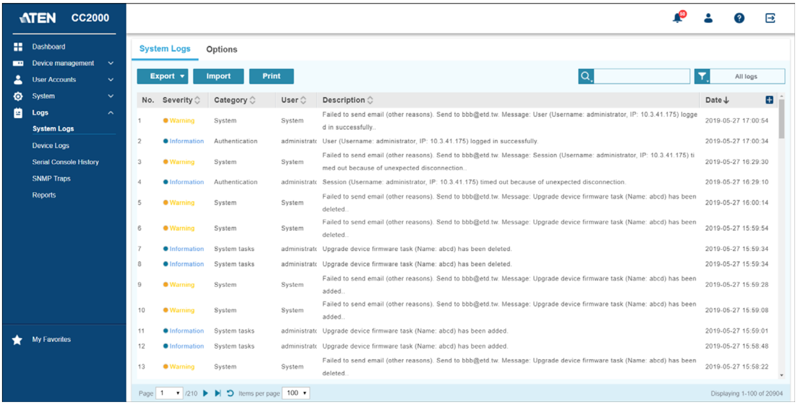
This Page Intentionally Left Blank

Chapter 8
Logs

Overview

The CC2000 keeps an extensive record of all the transactions that take place on its installation. The Logs page provides a powerful array of filters and functions that allow you to view and export the log file data, as well as be informed by email of specified events as they occur.

When you click the Logs menu, the CC2000 directs you to the System Logs page which looks similar to the page:



No.	Severity	Category	User	Description	Date
1	● Warning	System	System	Failed to send email (other reasons). Send to bbb@etd.tw. Message: User (Username: administrator, IP: 10.3.41.175) logged in successfully..	2019-05-27 17:00:54
2	● Information	Authentication	administratc	User (Username: administrator, IP: 10.3.41.175) logged in successfully.	2019-05-27 17:00:34
3	● Warning	System	System	Failed to send email (other reasons). Send to bbb@etd.tw. Message: Session (Username: administrator, IP: 10.3.41.175) timed out because of unexpected disconnection..	2019-05-27 16:29:30
4	● Information	Authentication	administratc	Session (Username: administrator, IP: 10.3.41.175) timed out because of unexpected disconnection.	2019-05-27 16:29:10
5	● Warning	System	System	Failed to send email (other reasons). Send to bbb@etd.tw. Message: Upgrade device firmware task (Name: abcd) has been deleted..	2019-05-27 16:00:14
6	● Warning	System	System	Failed to send email (other reasons). Send to bbb@etd.tw. Message: Upgrade device firmware task (Name: abcd) has been deleted..	2019-05-27 15:59:54
7	● Information	System tasks	administratc	Upgrade device firmware task (Name: abcd) has been deleted.	2019-05-27 15:59:34
8	● Information	System tasks	administratc	Upgrade device firmware task (Name: abcd) has been deleted.	2019-05-27 15:59:34
9	● Warning	System	System	Failed to send email (other reasons). Send to bbb@etd.tw. Message: Upgrade device firmware task (Name: abcd) has been added..	2019-05-27 15:59:28
10	● Warning	System	System	Failed to send email (other reasons). Send to bbb@etd.tw. Message: Upgrade device firmware task (Name: abcd) has been added..	2019-05-27 15:59:08
11	● Information	System tasks	administratc	Upgrade device firmware task (Name: abcd) has been added.	2019-05-27 15:59:01
12	● Information	System tasks	administratc	Upgrade device firmware task (Name: abcd) has been added.	2019-05-27 15:58:48
13	● Warning	System	System	Failed to send email (other reasons). Send to bbb@etd.tw. Message: Upgrade device firmware task (Name: abcd) has been deleted..	2019-05-27 15:58:22

Page 1 /210 Items per page 100

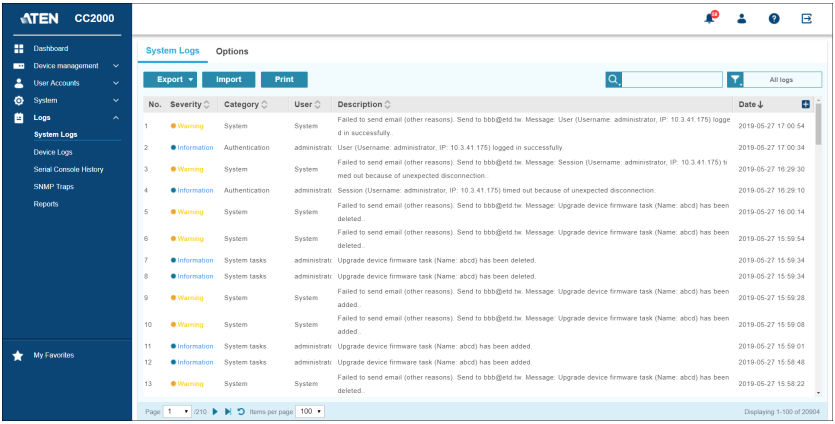
Displaying 1-100 of 20904

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:



No.	Severity	Category	User	Description	Date
1	● Warning	System	System	Failed to send email (other reasons). Send to bbb@etd.tw. Message: User (Username: administrator, IP: 10.3.41.175) logged in successfully..	2019-05-27 17:00:54
2	● Information	Authentication	administratc	User (Username: administrator, IP: 10.3.41.175) logged in successfully.	2019-05-27 17:00:34
3	● Warning	System	System	Failed to send email (other reasons). Send to bbb@etd.tw. Message: Session (Username: administrator, IP: 10.3.41.175) timed out because of unexpected disconnection..	2019-05-27 16:29:30
4	● Information	Authentication	administratc	Session (Username: administrator, IP: 10.3.41.175) timed out because of unexpected disconnection.	2019-05-27 16:29:10
5	● Warning	System	System	Failed to send email (other reasons). Send to bbb@etd.tw. Message: Upgrade device firmware task (Name: abcd) has been deleted..	2019-05-27 16:00:14
6	● Warning	System	System	Failed to send email (other reasons). Send to bbb@etd.tw. Message: Upgrade device firmware task (Name: abcd) has been deleted..	2019-05-27 15:59:54
7	● Information	System tasks	administratc	Upgrade device firmware task (Name: abcd) has been deleted.	2019-05-27 15:59:34
8	● Information	System tasks	administratc	Upgrade device firmware task (Name: abcd) has been deleted.	2019-05-27 15:59:34
9	● Warning	System	System	Failed to send email (other reasons). Send to bbb@etd.tw. Message: Upgrade device firmware task (Name: abcd) has been added..	2019-05-27 15:59:28
10	● Warning	System	System	Failed to send email (other reasons). Send to bbb@etd.tw. Message: Upgrade device firmware task (Name: abcd) has been added..	2019-05-27 15:59:08
11	● Information	System tasks	administratc	Upgrade device firmware task (Name: abcd) has been added.	2019-05-27 15:59:01
12	● Information	System tasks	administratc	Upgrade device firmware task (Name: abcd) has been added.	2019-05-27 15:58:48
13	● Warning	System	System	Failed to send email (other reasons). Send to bbb@etd.tw. Message: Upgrade device firmware task (Name: abcd) has been deleted..	2019-05-27 15:58:22

Page 1 /210 Items per page 100 Displaying 1-100 of 20904

- The default layout shows information concerning all of the events that have taken place on all the logs 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 the logged event records of current system logs page.

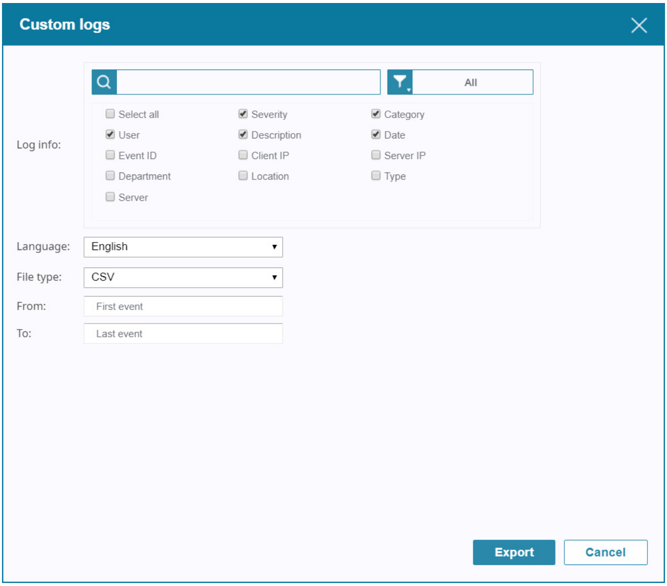
Note: The amount of logs downloaded for Logs in current page is determined by Items per page drop-down menu.

■ All logs

Select **All logs** to automatically download all of the logged event records from the system logs.

■ Custom logs

The Custom Logs page is used to save specified logged event records to a file. When you click **Custom logs**, a page similar to the one below appears:



Custom logs

Log info:

□ Select all	☑ Severity	☑ Category
☑ User	☑ Description	☑ Date
□ Event ID	□ Client IP	□ Server IP
□ Department	□ Location	□ Type
□ Server		

Language: English

File type: CSV

From: First event

To: Last event

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 as default.

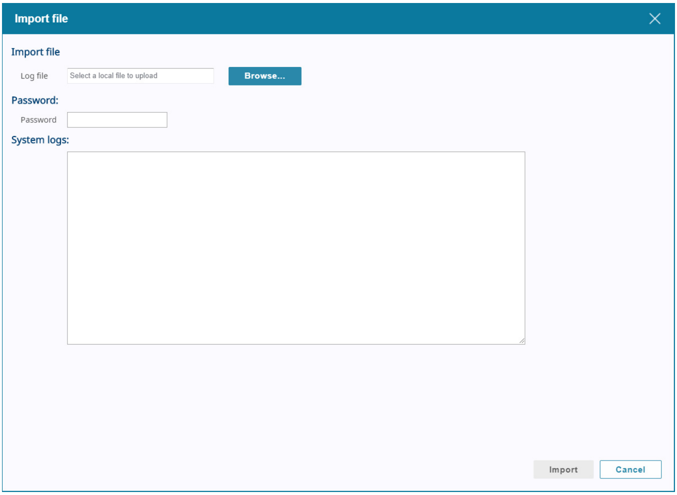
2. Use the drop-down menu **Language** for a list of languages offered if you prefer a different language, English is default. Select and confirm to have the file exported in the language that your set to.
3. Use the drop-down menu **File type** to select your preferred export file type. If you choose one of the encryption options (Encrypt file with AES or Encrypt file with DES), key a password into the Password field that comes up.

Note: Make a note of the password – you will need it to import the file.

4. Set the time parameters with the **From** and **To** fields to export logged event records for 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:

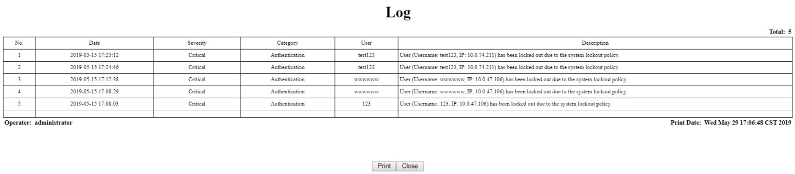
1. Either key in the full path to the file in the **Log file** field, or click **Browse** to navigate to it.
2. If the file has been encrypted, key the password that was used when it was created into the **Password** field.
3. Click **Import** at the bottom-right of the panel.

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

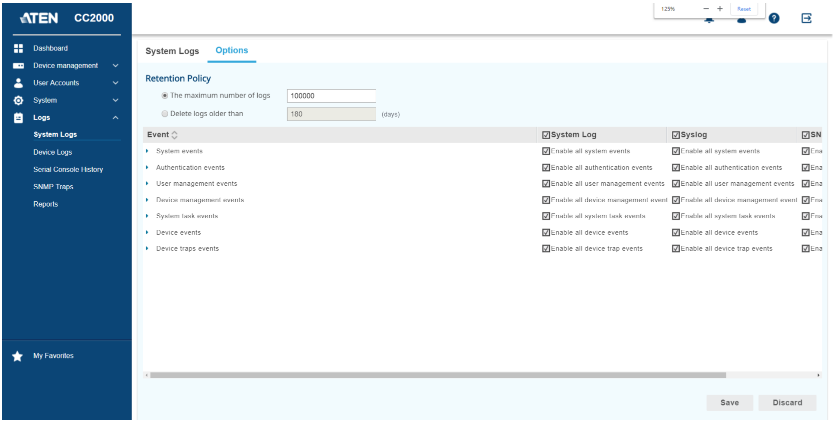
No.	Date	Severity	Category	User	Description
1	2019-05-15 17:25:12	Critical	Authentication	test123	User (Username: test123, IP: 10.0.74.211) has been locked out due to the system lockout policy.
2	2019-05-15 17:24:46	Critical	Authentication	test123	User (Username: test123, IP: 10.0.74.211) has been locked 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.

Operater: administrator

Print Date: Wed May 29 17:06:48 CST 2019

Options

The Options page gives you control over system log file’s Retention Policy. When you select Options, a page similar to the one below appears:



Retention Policy

● The maximum number of logs 100000

○ Delete logs older than 180 (days)

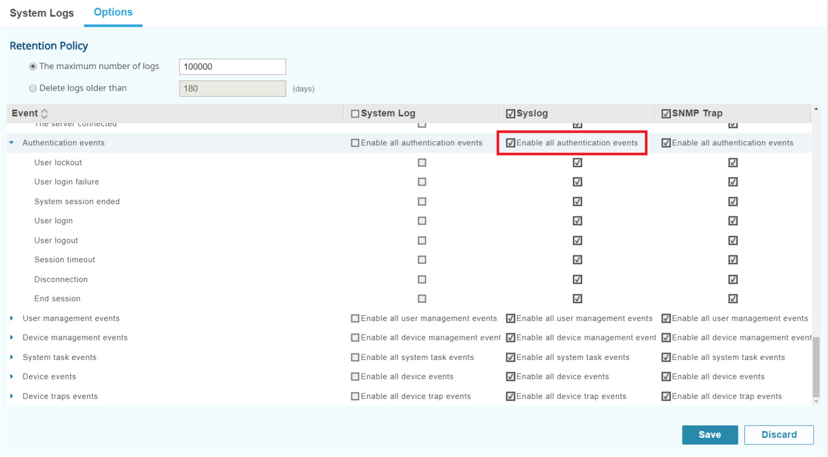
Event	☑System Log	☑Syslog	☑SN
System events	☑Enable all system events	☑Enable all system events	☑Ena
Authentication events	☑Enable all authentication events	☑Enable all authentication events	☑Ena
User management events	☑Enable all user management events	☑Enable all user management events	☑Ena
Device management events	☑Enable all device management event	☑Enable all device management event	☑Ena
System task events	☑Enable all system task events	☑Enable all system task events	☑Ena
Device events	☑Enable all device events	☑Enable all device events	☑Ena
Device traps events	☑Enable all device trap events	☑Enable all device trap events	☑Ena

To control your 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 days basis.

Note:
- When the number of days and records is reached, events are discarded on a "first in first out" basis.
- The valid range for number of logs is from 10000 - 1,000,000 logs.
- The valid range for number of days is from 30 - 1096 days.

2. For Event, it lets you select which events you want to track, and whether to record them in the System Log, Syslog, SNMP Trap, or all. Check the checkbox of the event name 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. Below is an example.



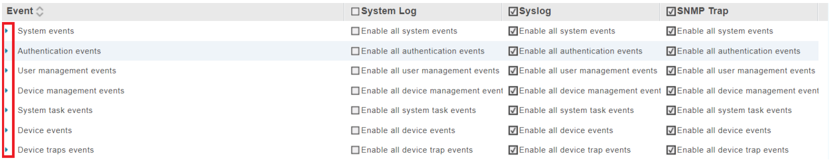
Retention Policy

● The maximum number of logs 100000

○ Delete logs older than 180 (days)

Event	□System Log	☑Syslog	☑SNMP Trap
The server connected	□	☑	☑
Authentication events	□Enable all authentication events	☑Enable all authentication events	☑Enable all authentication events
User lockout	□	☑	☑
User login failure	□	☑	☑
System session ended	□	☑	☑
User login	□	☑	☑
User logout	□	☑	☑
Session timeout	□	☑	☑
Disconnection	□	☑	☑
End session	□	☑	☑
User management events	□Enable all user management events	☑Enable all user management events	☑Enable all user management events
Device management events	□Enable all device management event	☑Enable all device management event	☑Enable all device management event
System task events	□Enable all system task events	☑Enable all system task events	☑Enable all system task events
Device events	□Enable all device events	☑Enable all device events	☑Enable all device events
Device traps events	□Enable all device trap events	☑Enable all device trap events	☑Enable all device trap events

   - 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.



Event ⇕	☐System Log	☑Syslog	☑SNMP Trap
▸ System events	☐Enable all system events	☑Enable all system events	☑Enable all system events
▸ Authentication events	☐Enable all authentication events	☑Enable all authentication events	☑Enable all authentication events
▸ User management events	☐Enable all user management events	☑Enable all user management events	☑Enable all user management events
▸ Device management events	☐Enable all device management event	☑Enable all device management event	☑Enable all device management event
▸ System task events	☐Enable all system task events	☑Enable all system task events	☑Enable all system task events
▸ Device events	☐Enable all device events	☑Enable all device events	☑Enable all device events
▸ Device traps events	☐Enable all device trap events	☑Enable all device trap events	☑Enable all device trap events

3. When you have finished with this page, click **Save** at the bottom-right of the panel.

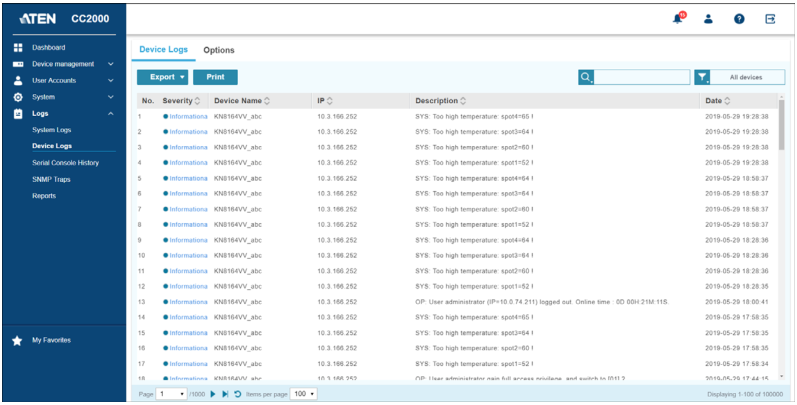
Device Logs

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:



No.	Severity	Device Name	IP	Description	Date
1	● Informationa	KN8164VV_abc	10.3.166.252	SYS: Too high temperature: spot4=65 !	2019-05-29 19:28:38
2	● Informationa	KN8164VV_abc	10.3.166.252	SYS: Too high temperature: spot3=64 !	2019-05-29 19:28:38
3	● Informationa	KN8164VV_abc	10.3.166.252	SYS: Too high temperature: spot2=60 !	2019-05-29 19:28:38
4	● Informationa	KN8164VV_abc	10.3.166.252	SYS: Too high temperature: spot1=52 !	2019-05-29 19:28:38
5	● Informationa	KN8164VV_abc	10.3.166.252	SYS: Too high temperature: spot4=64 !	2019-05-29 18:58:37
6	● Informationa	KN8164VV_abc	10.3.166.252	SYS: Too high temperature: spot3=64 !	2019-05-29 18:58:37
7	● Informationa	KN8164VV_abc	10.3.166.252	SYS: Too high temperature: spot2=60 !	2019-05-29 18:58:37
8	● Informationa	KN8164VV_abc	10.3.166.252	SYS: Too high temperature: spot1=52 !	2019-05-29 18:58:37
9	● Informationa	KN8164VV_abc	10.3.166.252	SYS: Too high temperature: spot4=64 !	2019-05-29 18:28:36
10	● Informationa	KN8164VV_abc	10.3.166.252	SYS: Too high temperature: spot3=64 !	2019-05-29 18:28:36
11	● Informationa	KN8164VV_abc	10.3.166.252	SYS: Too high temperature: spot2=60 !	2019-05-29 18:28:36
12	● Informationa	KN8164VV_abc	10.3.166.252	SYS: Too high temperature: spot1=52 !	2019-05-29 18:28:35
13	● Informationa	KN8164VV_abc	10.3.166.252	OP: User administrator (IP=10.0.74.211) logged out. Online time : 0D 00H:21M:11S.	2019-05-29 18:00:41
14	● Informationa	KN8164VV_abc	10.3.166.252	SYS: Too high temperature: spot4=65 !	2019-05-29 17:58:35
15	● Informationa	KN8164VV_abc	10.3.166.252	SYS: Too high temperature: spot3=64 !	2019-05-29 17:58:35
16	● Informationa	KN8164VV_abc	10.3.166.252	SYS: Too high temperature: spot2=60 !	2019-05-29 17:58:35
17	● Informationa	KN8164VV_abc	10.3.166.252	SYS: Too high temperature: spot1=52 !	2019-05-29 17:58:34
18	● Informationa	KN8164VV_abc	10.3.166.252	OP: User administrator gain full access privilege, and switch to [01] 2	2019-05-29 17:44:15

Displaying 1-100 of 100000

- 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 submenus, Logs in current page, and All logs.

■ Logs in current page

Select **Logs in current page** to automatically download all the logged event records of current system logs page.

Note: The amount of logs downloaded for Logs in current page is determined by Items per page drop-down menu.

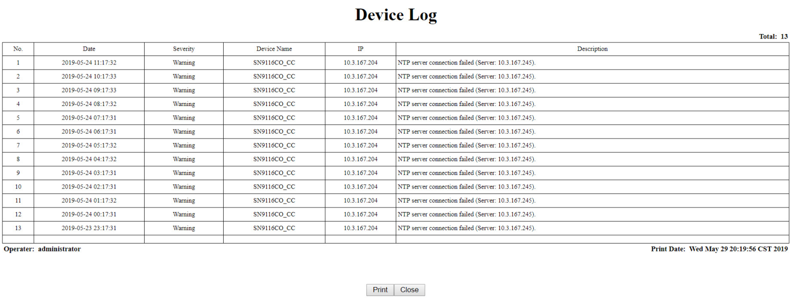
■ All logs

Select **All logs** to automatically download all of the logged event records from the system 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

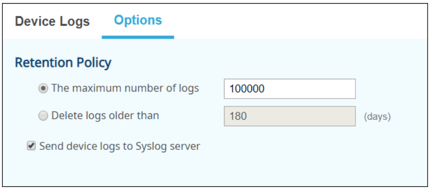
No.	Date	Severity	Device Name	IP	Description
1	2019-05-24 11:17:32	Warning	SN9116CO_CC	10.3.167.204	NTP server connection failed (Server: 10.3.167.245).
2	2019-05-24 10:17:33	Warning	SN9116CO_CC	10.3.167.204	NTP server connection failed (Server: 10.3.167.245).
3	2019-05-24 09:17:33	Warning	SN9116CO_CC	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

Options

The Options page gives you control over device log file's Retention Policy. When you select Options, a page similar to the one below appears:



Retention Policy

● The maximum number of logs 100000

○ Delete logs older than 180 (days)

☑ Send device logs to Syslog server

To control your 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 days basis.

Note:
- When the number of days and records is reached, events are discarded on a "first in first out" basis.
- The valid range for number of logs is from 10000 - 1,000,000 logs.
- The valid range for number of days is from 30 - 1096 days.

2. Check the checkbox of the **Send device logs to Syslog server** to enable Syslog function. When enabled, the CC2000 will send Device logs to Syslog server.

Note: CC2000 sets enable Send device logs to Syslog as default.

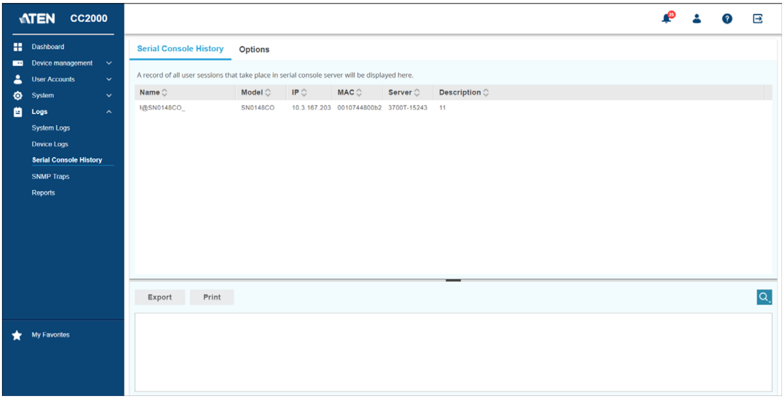
3. When you have finished with this page, click **Save** at the bottom-right of the page.

Serial Console History

The CC2000 keeps a record of all user sessions that take place in serial console server and display them. 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:



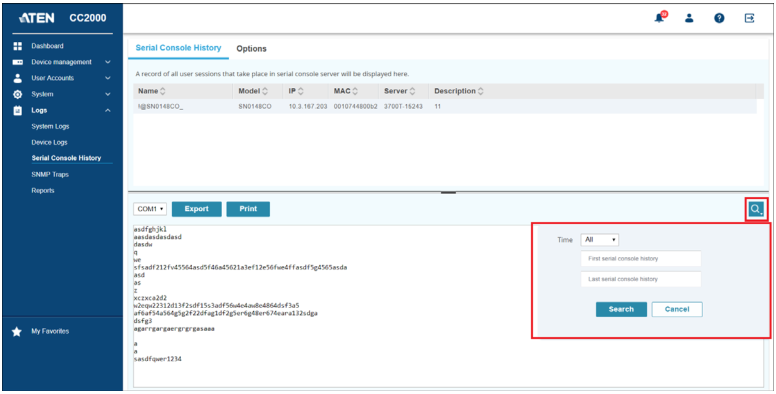
A record of all user sessions that take place in serial console server will be displayed here.

Name	Model	IP	MAC	Server	Description
l@SN0148CO_	SN0148CO	10.3.167.203	0010744800b2	3700T-15243	11

- 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 the Serial Console History records, do the following:

1. Click to choose a Model first then click the search icon, a page similar to the one below appears:



A record of all user sessions that take place in serial console server will be displayed here.

Name	Model	IP	MAC	Server	Description
!@SN0148CO_	SN0148CO	10.3.167.203	0010744800b2	3700T-15243	11

COM1

```
asdfghjkl
aasdasdasdasd
dasdw
q
we
sfsadf212fv45564asd5f46a45621a3ef12e56fwe4ffasdf5g4565asda
asd
as
z
xczxca2d2
w2eqw22312d13f2sdf15s3adf56w4e4aw8e4864dsf3a5
af6af54a564g5g2f22dfag1df2g5er6g48er674eara132sdga
dsfg3
agarrgargaergrgrgasaaa

a
a
sasdfqwer1234
```

Time: All

First serial console history

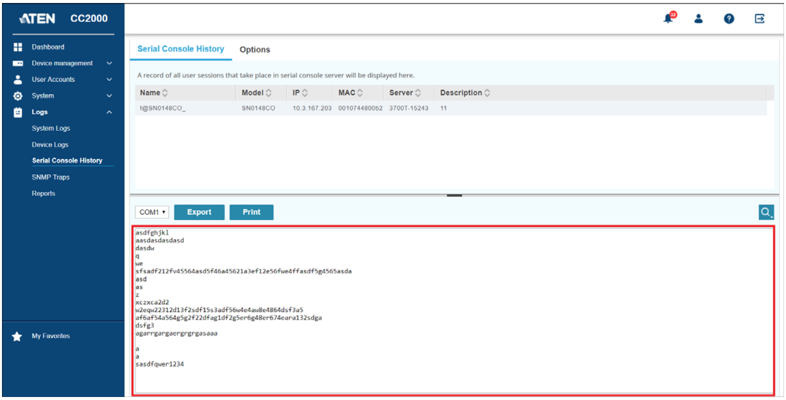
Last serial console history

2. Use the drop-down menu **Time** to select one of the three options from All, Exclude, and Include. To search records for a particular time period, select either the **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 all the records that exists in the database.
- Select **Include** to search all the records that fall within the specified time range.
- Select **Exclude** to search all the 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.



A record of all user sessions that take place in serial console server will be displayed here.

Name	Model	IP	MAC	Server	Description
l@SN0148CO_	SN0148CO	10.3.167.203	0010744800b2	3700T-15243	11

```
asdfghjkl
aasdasdasdasd
dasdw
q
we
sfsadf212fv45564asd5f46a45621a3ef12e56fwe4ffasdf5g4565asda
asd
as
z
xczxca2d2
w2eqw22312d13f2sdf15s3adf56w4e4aw8e4864dsf3a5
af6af54a564g5g2f22dfag1df2g5er6g48er674eara132sdga
dsfg3
agarrgargaergrgrgasaaa

a
a
sasdfqwer1234
```

Export

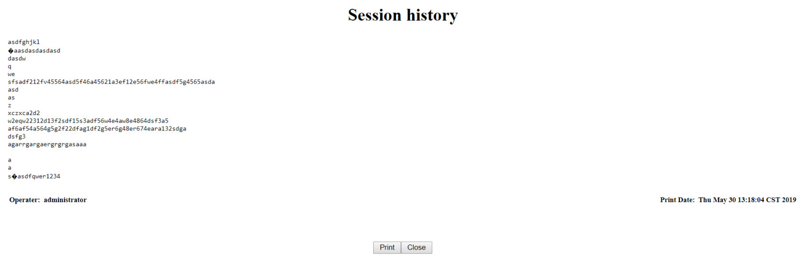
To Export the Serial Console History, do the following:

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.



Session history

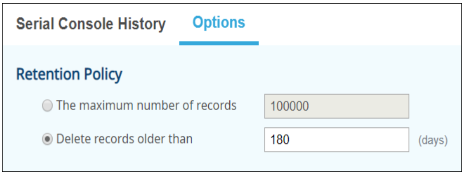
```
asdfghjkl
�aasdasdasdasd
dasdw
q
we
sfsadf212fv45564asd5f46a45621a3ef12e56fwe4ffasdf5g4565asda
asd
as
z
xczxca2d2
w2eqw22312d13f2sdf15s3adf56w4e4aw8e4864dsf3a5
af6af54a564g5g2f22dfag1df2g5er6g48er674eara132sdga
dsfg3
agarrgargaergrgrgasaaa

a
a
s�asdfqwer1234
```

Operater: administrator

Print Date: Thu May 30 13:18:04 CST 2019

Options

The Options page gives you control over serial console history's Retention Policy. When you select Options, a page similar to the one below appears:



Retention Policy

○ The maximum number of records 100000

● Delete records older than 180 (days)

To control your 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 days basis.

Note:
- When the number of days and records is reached, events are discarded on a "first in first out" basis.
- The valid range for number of records is from 10000 - 1,000,000 serial console history records.
- The valid range for number of days is from 30 - 1096 days.

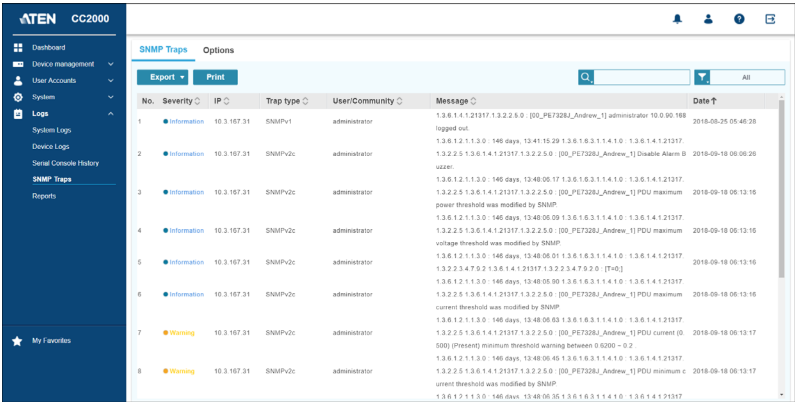
2. When you have finished with this page, click **Save** at the bottom-right of the page.

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, and it looks similar to the one below:



No.	Severity	IP	Trap type	User/Community	Message	Date
1	● Information	10.3.167.31	SNMPv1	administrator	1.3.6.1.4.1.21317.1.3.2.2.5.0 : [00_PE7328J_Andrew_1] administrator 10.0.90.168 logged out.	2018-08-25 05:46:28
2	● Information	10.3.167.31	SNMPv2c	administrator	1.3.6.1.2.1.1.3.0 : 146 days, 13:41:15.29 1.3.6.1.6.3.1.1.4.1.0 : 1.3.6.1.4.1.21317.1.3.2.2.5 1.3.6.1.4.1.21317.1.3.2.2.5.0 : [00_PE7328J_Andrew_1] Disable Alarm Buzzer.	2018-09-18 06:06:26
3	● 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 : 1.3.6.1.4.1.21317.1.3.2.2.5 1.3.6.1.4.1.21317.1.3.2.2.5.0 : [00_PE7328J_Andrew_1] PDU maximum power threshold was modified by SNMP.	2018-09-18 06:13:16
4	● 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 : 1.3.6.1.4.1.21317.1.3.2.2.5 1.3.6.1.4.1.21317.1.3.2.2.5.0 : [00_PE7328J_Andrew_1] PDU maximum voltage threshold was modified by SNMP.	2018-09-18 06:13:16
5	● 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 : 1.3.6.1.4.1.21317.1.3.2.2.3.4.7.9.2 1.3.6.1.4.1.21317.1.3.2.2.3.4.7.9.2.0 : [T=0;]	2018-09-18 06:13:16
6	● 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 : 1.3.6.1.4.1.21317.1.3.2.2.5 1.3.6.1.4.1.21317.1.3.2.2.5.0 : [00_PE7328J_Andrew_1] PDU maximum current threshold was modified by SNMP.	2018-09-18 06:13:16
7	● 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 : 1.3.6.1.4.1.21317.1.3.2.2.5 1.3.6.1.4.1.21317.1.3.2.2.5.0 : [00_PE7328J_Andrew_1] PDU current (0.500) (Present) minimum threshold warning between 0.6200 ~ 0.2 .	2018-09-18 06:13:17
8	● 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 : 1.3.6.1.4.1.21317.1.3.2.2.5 1.3.6.1.4.1.21317.1.3.2.2.5.0 : [00_PE7328J_Andrew_1] PDU minimum current threshold was modified by SNMP.	2018-09-18 06:13:17
					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 : 1.3.6.1.4.1.21317.	

- The default layout shows all of the SNMP traps 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 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 the SNMP trap records of current SNMP Traps page.

Note: The amount of traps downloaded in current page is determined by Items per page drop-down menu.

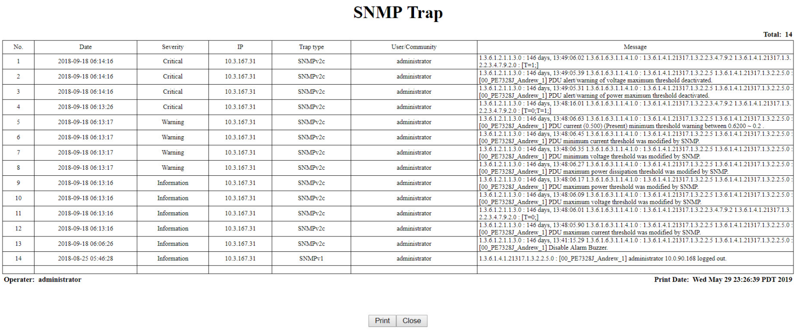
■ All SNMP traps

Select **All SNMP traps** to automatically download all of the SNMP trap records from the SNMP Traps.

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

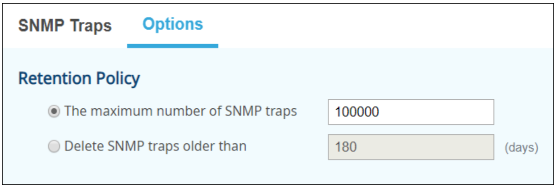
No.	Date	Severity	IP	Trap type	User/Community	Message
1	2018-09-18 06:14:16	Critical	10.3.167.31	SNMPv2c	administrator	1.3.6.1.2.1.1.3.0 : 146 days, 13:49:06.02 1.3.6.1.6.3.1.1.4.1.0 : 1.3.6.1.4.1.21317.1.3.2.2.3.4.7.9.2 1.3.6.1.4.1.21317.1.3.2.2.3.4.7.9.2.0 : [T=1;]
2	2018-09-18 06:14:16	Critical	10.3.167.31	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 : 1.3.6.1.4.1.21317.1.3.2.2.5 1.3.6.1.4.1.21317.1.3.2.2.5.0 : [00_PE7328J_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 : 1.3.6.1.4.1.21317.1.3.2.2.5 1.3.6.1.4.1.21317.1.3.2.2.5.0 : [00_PE7328J_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, 13:48:16.01 1.3.6.1.6.3.1.1.4.1.0 : 1.3.6.1.4.1.21317.1.3.2.2.3.4.7.9.2 1.3.6.1.4.1.21317.1.3.2.2.3.4.7.9.2.0 : [T=0;T=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 : 1.3.6.1.4.1.21317.1.3.2.2.5 1.3.6.1.4.1.21317.1.3.2.2.5.0 : [00_PE7328J_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 : 1.3.6.1.4.1.21317.1.3.2.2.5 1.3.6.1.4.1.21317.1.3.2.2.5.0 : [00_PE7328J_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 : 1.3.6.1.4.1.21317.1.3.2.2.5 1.3.6.1.4.1.21317.1.3.2.2.5.0 : [00_PE7328J_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 : 1.3.6.1.4.1.21317.1.3.2.2.5 1.3.6.1.4.1.21317.1.3.2.2.5.0 : [00_PE7328J_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 : 1.3.6.1.4.1.21317.1.3.2.2.5 1.3.6.1.4.1.21317.1.3.2.2.5.0 : [00_PE7328J_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 : 1.3.6.1.4.1.21317.1.3.2.2.5 1.3.6.1.4.1.21317.1.3.2.2.5.0 : [00_PE7328J_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 : 1.3.6.1.4.1.21317.1.3.2.2.3.4.7.9.2 1.3.6.1.4.1.21317.1.3.2.2.3.4.7.9.2.0 : [T=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 : 1.3.6.1.4.1.21317.1.3.2.2.5 1.3.6.1.4.1.21317.1.3.2.2.5.0 : [00_PE7328J_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, 13:41:15.29 1.3.6.1.6.3.1.1.4.1.0 : 1.3.6.1.4.1.21317.1.3.2.2.5 1.3.6.1.4.1.21317.1.3.2.2.5.0 : [00_PE7328J_Andrew_1] Disable Alarm Buzzer.
14	2018-08-25 05:46:28	Information	10.3.167.31	SNMPv1	administrator	1.3.6.1.4.1.21317.1.3.2.2.5.0 : [00_PE7328J_Andrew_1] administrator 10.0.90.168 logged out.

Operater: administrator

Print Date: Wed May 29 23:26:39 PDT 2019

Options

The Options page gives you control over SNMP trap's Retention Policy. When you select Options, a page similar to the one below appears:



Retention Policy

● The maximum number of SNMP traps 100000

○ Delete SNMP traps older than 180 (days)

To control your 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.

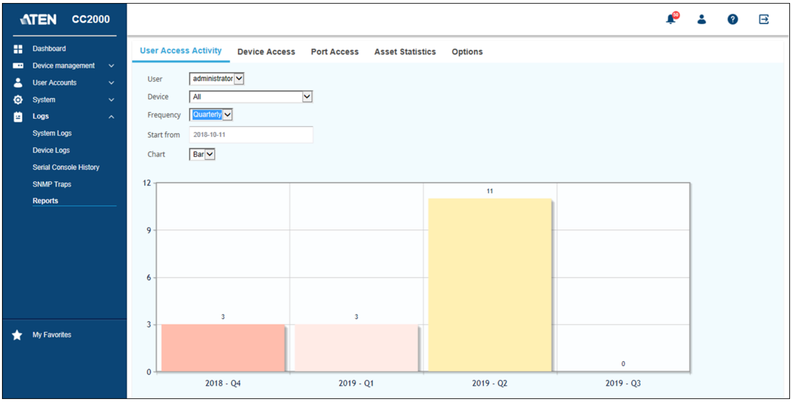
- Select **The maximum number of SNMP traps** if you want to maintain the SNMP trap database on a records basis.
- Select **Delete SNMP traps older than** if you want to maintain the SNMP trap database on a days basis.

Note:
- When the number of days and records is reached, events are discarded on a “first in first out” basis.
- The valid range for number of records is from 10000 - 1,000,000 SNMP traps.
- The valid range for 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

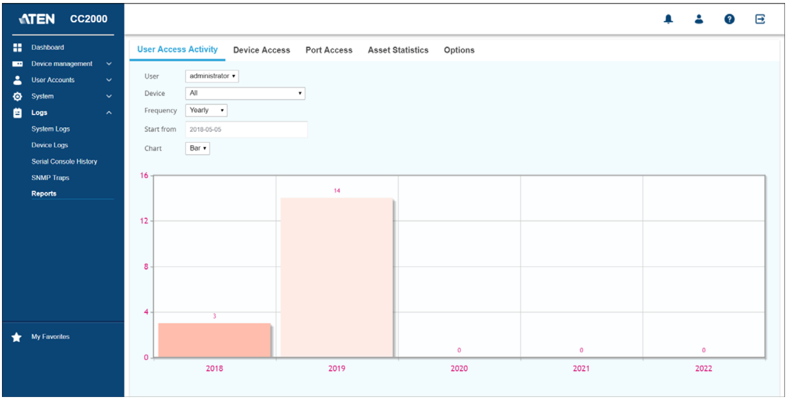
The Reports tab offers five tab menus: User Access Activity, Device Access, Port Access, Asset Statistics, and Options. You can view access statistics about users and devices on the CC2000 installation and set options for how the reports are displayed.



User: administrator
Device: All
Frequency: Quarterly
Start from: 2018-10-11
Chart: Bar

User Access Activity

This page provides Statistics for Device/Port Access Per User. The User Access Activity is the default page, and it looks similar to the one below:



User: administrator
Device: All
Frequency: Yearly
Start from: 2018-05-05
Chart: Bar

Fill in the fields from the main panel to build and display either a pie or bar chart, or both according to the parameters you set.

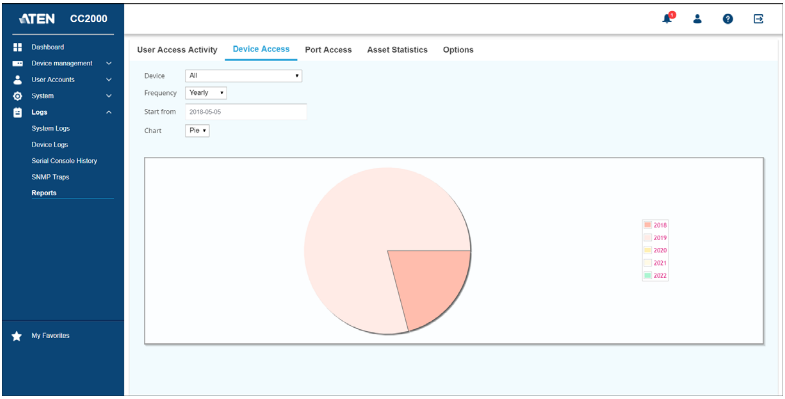
The meanings of each fields are described in the table below:

Item	Description
User	Use the drop-down menu User to browse a list of users to select from and to display their access statistics.
Device	Select All or an individual port/device to display statics for. 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 it's percentage of the whole.
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 on the Start From date. ◆ Weekly: Displays how many times the device was accessed each week, for a span of 4 weeks, beginning on 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 on the Start From date. ◆ Quarterly: Displays how many times the device was accessed each quarter, for 4 quarters of a year, beginning on the Start From date. ◆ Yearly: Displays how many times the device was accessed each year, for a span of 5 years, beginning on the Start From date. **Note:** If the device was not accessed no data will be displayed.
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 bar graphs 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 you set. When the **Pie** is selected for **Chart**, the Device Access page looks similar to the one below:



Device: All
Frequency: Yearly
Start from: 2018-05-05
Chart: Pie

The meanings of each fields are described in the table below:

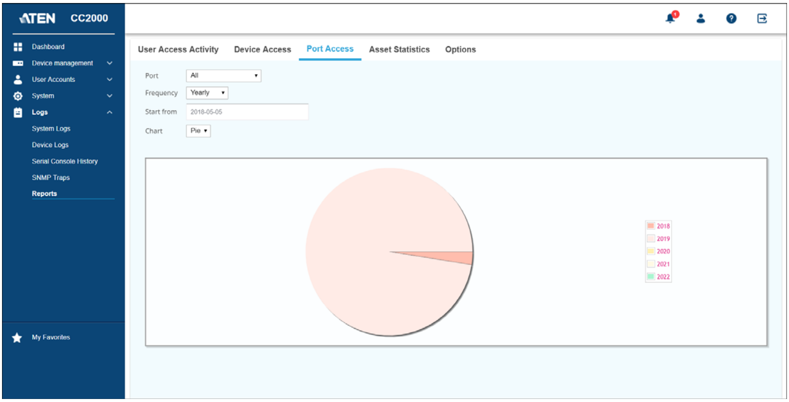
Item	Description
Device	Select All, Top 10 port, or an individual device that you want to display statics for. This will display a graph with the number of times the device(s) has been accessed, according to the Frequency you select. ◆ Top 10 port: Display the top 10 devices statics. The numbers displayed with each chart color show the number of times the device was accessed (on that day/week/month/quarter/year) and it’s percentage of the whole.
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 on the Start From date. ◆ Weekly: Displays how many times the device was accessed each week, for a span of 4 weeks, beginning on 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 on the Start From date. ◆ Quarterly: Displays how many times the device was accessed each quarter, for 4 quarters of a year, beginning on the Start From date. ◆ Yearly: Displays how many times the device was accessed each year, for a span of 5 years, beginning on the Start From date. **Note:** If the device was not accessed no data will be displayed.
Start From	Click the calendar to select a start date for the span of time that will be represented in the chart.

Item	Description
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 bar graphs divided into the time periods selected. ◆ All: Displays both a Pie and Bar chart.

Port Access

The Port Access page provides 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 you set. The Port Access page looks similar to the one below:



Port: All
Frequency: Yearly
Start from: 2018-05-05
Chart: Pie

The meanings of each fields are described in the table below:

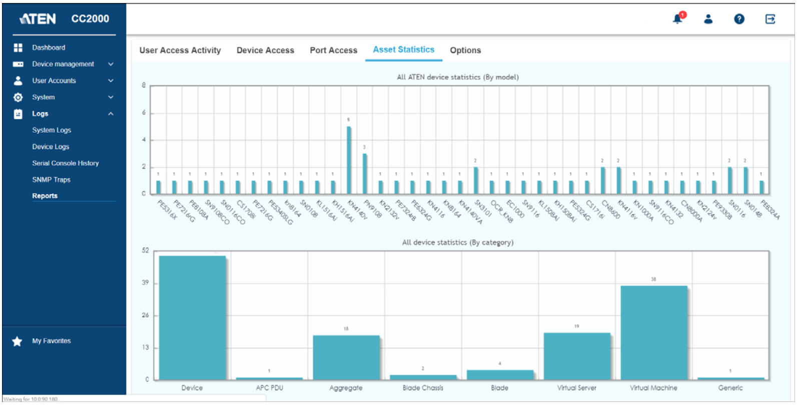
Item	Description
Port	Select All, Top 10 port, or an individual port that you want to display statics for. This will display a graph with the number of times the port(s) was accessed, according to the Frequency you select. ◆ Top 10 port: Display the top 10 devices statics. The numbers displayed with each chart color show the number of times the port was accessed (on that day/week/month/quarter/year) and it’s percentage of the whole.

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 on the Start From date. ◆ Weekly: Displays how many times the port was accessed each week, for a span of 4 weeks, beginning on the Start From date. The format 2013-W42 represents week 42 of the year 2013. ◆ Monthly: Displays how many times the port was accessed each month, for a span of 12 months, beginning on the Start From date. ◆ Quarterly: Displays how many times the port was accessed each quarter, for 4 quarters of a year, beginning on the Start From date. ◆ Yearly: Displays how many times the port was accessed each year, for a span of 5 years, beginning on the Start From date. **Note:** If the port was not accessed no data will be displayed.
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 bar graphs 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)**.

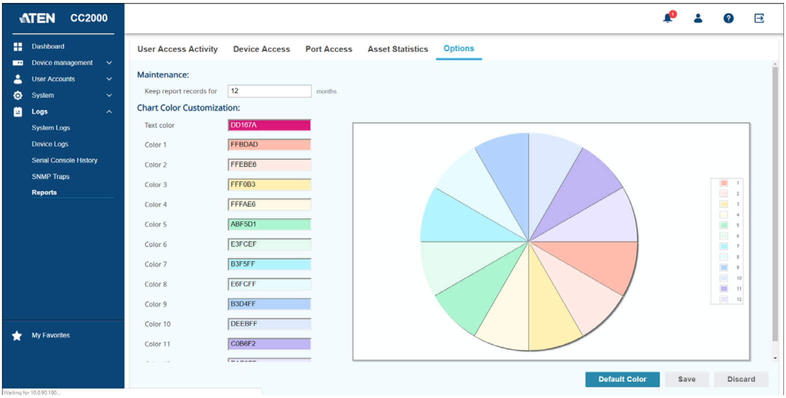
The Port Access page looks similar to the one below:



- **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, and it looks similar to the one below:



Maintenance:

Keep report records for 12 months

Chart Color Customization:

Text color	DD167A
Color 1	FFBDAD
Color 2	FFEBE6
Color 3	FFF0B3
Color 4	FFFAE6
Color 5	ABF5D1
Color 6	E3FCEF
Color 7	B3F5FF
Color 8	E6FCFF
Color 9	B3D4FF
Color 10	DEEBFF
Color 11	C0B6F2

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 text 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. After selecting a color the test chart to the right will change accordingly so you can see how your graph will look.

- Default Color tab: Click to return all colors back to the default settings.

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.

2.2

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/Altusen Products

Refer to the CC2000 webpage for a list of supported products.

Device ANMS Settings

To enable CC Management of a device from the device’s ANMS settings page, do the following:

1. Log into the device.
2. Refer to the device’s User Manual to locate its ANMS settings page.
3. In the ANMS page, click the checkbox to *enable* 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, 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 server – 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 speeding up network traffic.

Firewalls

When several CC2000 servers are located behind separate firewalls, the following service ports must be specified on the servers, and the corresponding ports must be opened on the firewall.

1. 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 inside the same firewall. Communication and access with the other CC2000 servers on the installation (outside of the firewall) takes place through the CC Port and Proxy port – 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 the 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) using the 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 viewer – 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 the service ports (HTTPS, Program, Virtual Media, Telnet, SSH, etc.) on the firewall 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, field entries can be input in any supported language.

Category		Length / Range	Default
Users	Login name	Up to the equivalent of 32 English alphanumeric characters. The minimum number is based on the account policy settings (see *CC2000 Authentication*, page 140). The following characters may not be used: **/ \ [ ] : ; | = , + * ? < > @ " '**	
	Password	The equivalent of 0–16 English alphanumeric characters. The minimum number is based on the account policy settings (see *CC2000 Authentication*, page 140). 0 means no password authentication.	
	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.	

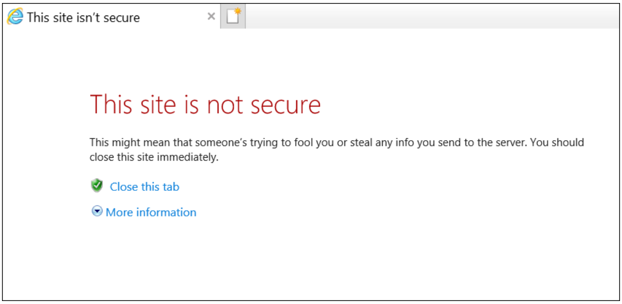
Category		Length / Range	Default
Authentication Server	Server name	2–32 Bytes. The following characters may not be used: **" '**	
	Description	Up to 256 Bytes.	
	Browser Method	Unlimited for Username and Password. **Note:** CC2000 performance is adversely affected if there are too many characters.	
CC2000 Authentication	Username Minimum	Up to the equivalent of 32 English alphanumeric characters. The minimum number is based on the account policy settings (see *CC2000 Authentication*, page 140). The following characters may not be used: **/ \ [ ] : ; | = , + * ? < > @ " '**	6
	Password Minimum	The equivalent of 0–32 English alphanumeric characters. The minimum number is based on the account policy settings (see *CC2000 Authentication*, page 140). 0 means no password authentication.	6
	Password Expires	No limit on the number of days.	
Devices	Name	0–32 Bytes.	
	Description	Up to 256 Bytes.	
	Contact name	No limit on the number of Bytes.	
	Telephone	No limit on the number of Bytes.	
	Email notification	No limit on the number of Bytes.	
Aggregate Devices	Name	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.	
	Export Device Log Pattern	No limit on the number of Bytes.	
System Log Options	By Period	30-1096 days	
	By Record	10,000–1,000,000	
	Records per page	100, 300, 500	

Category		Length / Range	Default
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 your browser, a Security Alert message appears to inform you that the device's certificate is not trusted, and asks if you want to proceed.



This site isn't secure

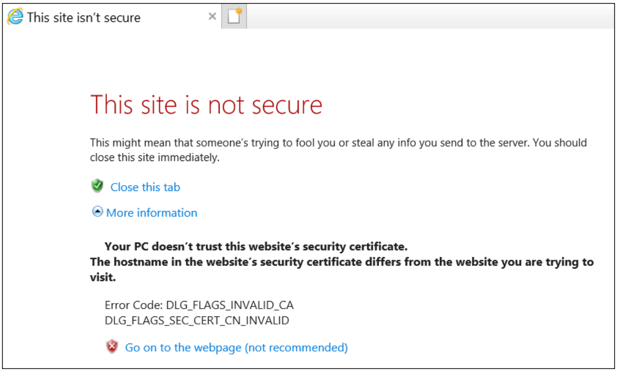
This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

Close this tab

More information

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.



This site isn't secure

This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

Close this tab

More information

Your PC doesn't trust this website's security certificate.
The hostname in the website's security certificate differs from the website you are trying to visit.

Error Code: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID

Go on to the webpage (not recommended)

You can ignore the warning, click **More information** and click **Yes** to go on.

Note: To avoid users having to go through the certificate acceptance prompt each time they log in, you can use a third party certificate authority (CA) to obtain a signed certificate. See *Importing a Signed SSL Server Certificate*, page 165, for details.

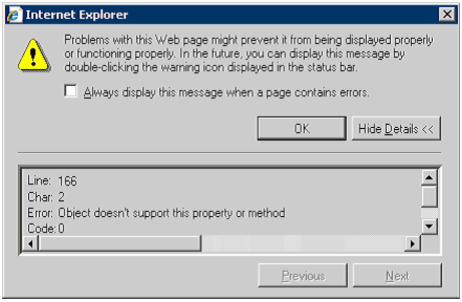
Troubleshooting

Problem	Resolution
After installing the CC2000, a few minutes later 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 5). 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 22). Uninstall the CC2000 following the procedures mentioned, and reinstall.
I key in the IP address for the CC2000 Website, but I can’t bring up the CC2000 login page.	1. The CC2000 only allows HTTPS requests. HTTP requests from a browser are automatically redirect 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 using the default ports. Use the CC2000 Utility (see page 241) 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 precedence of the login page is to first look at the language that your browser is set for, and next to look at what your OS language is. After you have logged in, the CC2000 will display in the language you have set it for in Preferences.
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 a login request once there already is a session open with the same session ID. Either: 1) end the currently open session and log in again; 2) log in from a different computer; or 3) log in with a non-Mozilla based browser.
When I log in, the browser generates a *CA Root certificate is not trusted*, or a *Certificate Error* response.	The certificate’s name is not found on Microsoft’s list of Trusted Authorities. The certificate can be trusted, however. See *Trusted Certificates*, page 233, for details.
After I log in to the CC2000, There is device management page.	You have not been authorized to access any ports. Check with your CC2000 administrator to get authorization to access 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 170, 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 settings.
When adding a Cat5e KVM switch, can I add all the ports at the same time?	Yes – provided all the ports have KVM Adapters attached and their devices are on line. See the note on page 53, 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 the device's ANMS settings to be sure that CC Management 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 187, for details.
My ATEN/Altusen device isn't being recognized by the CC2000.	1. The device in question may not be supported by the CC2000 management system. See *Supported Aten/ Altusen Products*, page 226, 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 one of the following:



Internet Explorer

Problems with this Web page might prevent it from being displayed properly or functioning properly. In the future, you can display this message by double-clicking the warning icon displayed in the status bar.

□ Always display this message when a page contains errors.

Line: 166
Char: 2
Error: Object doesn't support this property or method
Code: 0

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 the High security level for the Restricted sites zone and Microsoft Windows Server 2003 uses the High security level for both the Restricted sites zone and the 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 other, 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 the temporary Internet-related files

   To remove all the temporary Internet-related 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 the Java JRE installed.

   For information about how to install the latest version of the JRE visit the Java Web site: www.java.com

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 on one line (i.e., do not press [Enter] until all the 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 that you upload in the *Update CC2000 Server Certificate* panel (see *Import Private Key and Certificate*, page 166).

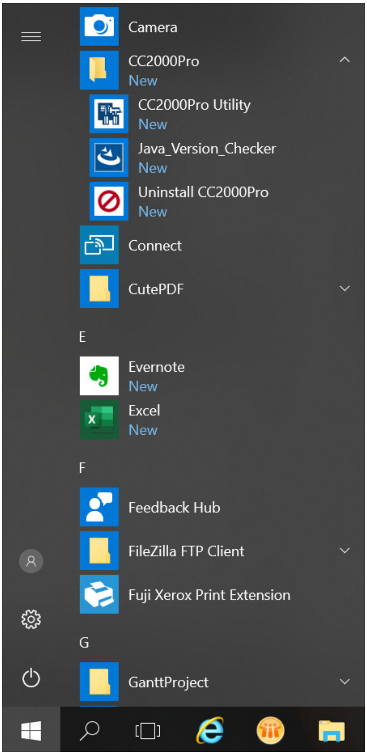
This Page Intentionally Left Blank

Appendix B
The CC2000 Utility

Overview

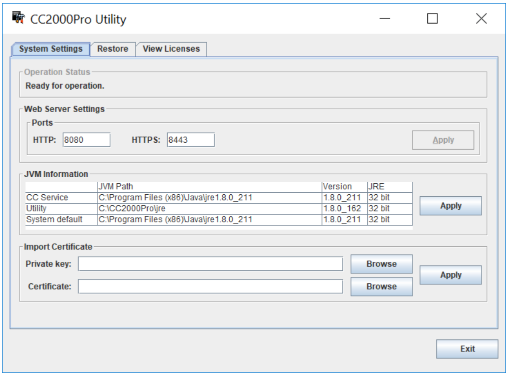
The CC2000Pro Utility gets installed as part of the CC2000 installation procedure. It allows you to configure a number of the CC2000's parameters from the desktop of the computer that the CC2000 runs on, without having to invoke the browser GUI.

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:



Operation Status

Ready for operation.

Web Server Settings

Ports

HTTP: 8080 HTTPS: 8443

JVM Information

	JVM Path	Version	JRE
CC Service	C:\Program Files (x86)\Java\jre1.8.0_211	1.8.0_211	32 bit
Utility	C:\CC2000Pro\jre	1.8.0_162	32 bit
System default	C:\Program Files (x86)\Java\jre1.8.0_211	1.8.0_211	32 bit

Import Certificate

Private key:

Certificate:

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 asks you to specify the ports that Apache Tomcat listens on for web requests.

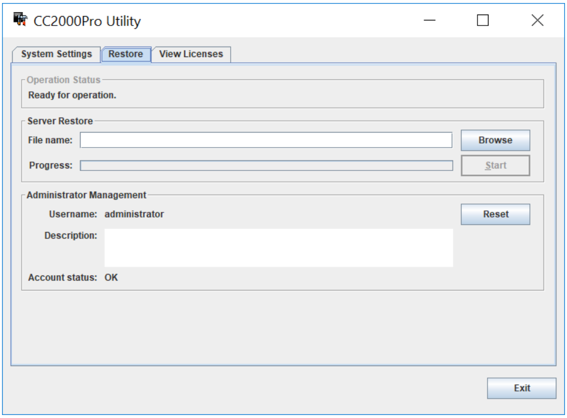
- The *HTTP* port is the regular port that Apache Tomcat listens on. The default is 80. If you use a different port, users must specify the port number in the URL of their browsers.
- The *HTTPS* port is the secure port that Apache Tomcat listens on. The default is 443. If you use a different port, users 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:



Operation Status
Ready for operation.

Server Restore
File name:
Progress:

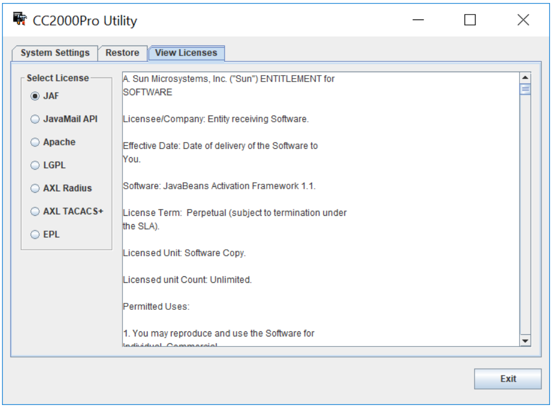
Administrator Management
Username: administrator
Description:
Account status: OK

The dialog box is divided into three panels, as described in the table below:

Panel	Description
Operation Status	You can use this to check that 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 173). Click **Browse** to navigate to the location of 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.
Administrator Management	Clicking **Reset** returns the default System Administrator's account to the default (administrator / password). If this account has been Locked (see *Lockout Policy*, page 194) it is automatically Unlocked.

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.



Select License

● JAF
○ JavaMail API
○ Apache
○ LGPL
○ AXL Radius
○ AXL TACACS+
○ EPL

A. Sun Microsystems, Inc. ("Sun") ENTITLEMENT for SOFTWARE

Licensee/Company: Entity receiving Software.

Effective Date: Date of delivery of the Software to You.

Software: JavaBeans Activation Framework 1.1.

License Term: Perpetual (subject to termination under the SLA).

Licensed Unit: Software Copy.

Licensed unit Count: Unlimited.

Permitted Uses:

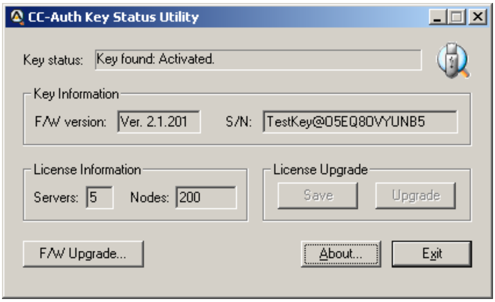
1. You may reproduce and use the Software for Individual, Commercial

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:



CC-Auth Key Status Utility

Key status: Key found: Activated.

Key Information

F/W version: Ver. 2.1.201 S/N: TestKey@05EQ80VYUNB5

License Information

Servers: 5 Nodes: 200

License Upgrade

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 when performing an Offline license upgrade.
F/W Upgrade	This button is used to upgrade the authentication key's firmware.

Key Utilities

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

Key Firmware Upgrade

The CC2000 Authentication Key's firmware is upgradable. As new revisions of the firmware become released, upgrade file 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 to a convenient location on your computer.
2. With the authentication key plugged in, run the *Key Status Utility* (CCAuthKeyStatus.exe).

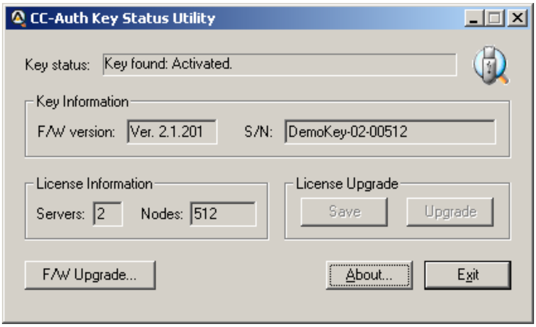
Note: 1. *CCAuthKeyStatus.exe* only runs under Windows.

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...**



CC-Auth Key Status Utility

Key status: Key found: Activated.

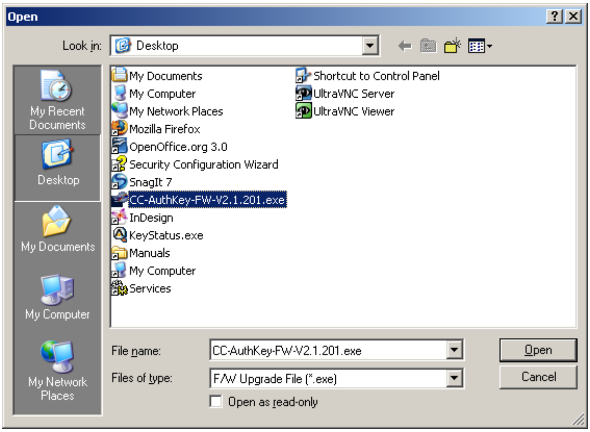
Key Information

F/W version: Ver. 2.1.201 S/N: DemoKey-02-00512

License Information

Servers: 2 Nodes: 512

5. In the *File Open* dialog box that appears, select the firmware upgrade file, then click **Open**.

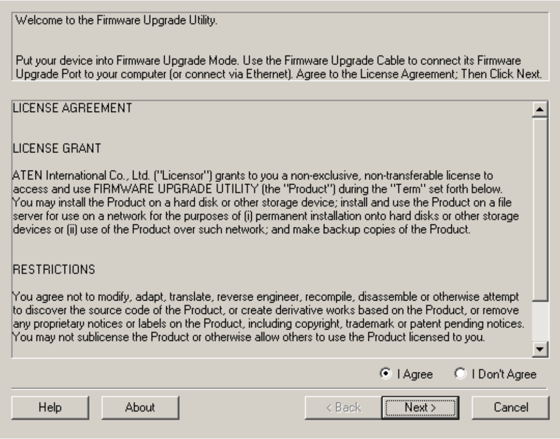


File name: CC-AuthKey-FW-V2.1.201.exe

Files of type: F/W Upgrade File (*.exe)

☐ Open as read-only

6. Read and *Agree* to the License Agreement (enable the *I Agree* radio button).



Welcome to the Firmware Upgrade Utility.

Put your device into Firmware Upgrade Mode. Use the Firmware Upgrade Cable to connect its Firmware Upgrade Port to your computer (or connect via Ethernet). Agree to the License Agreement; Then Click Next.

LICENSE AGREEMENT

LICENSE GRANT

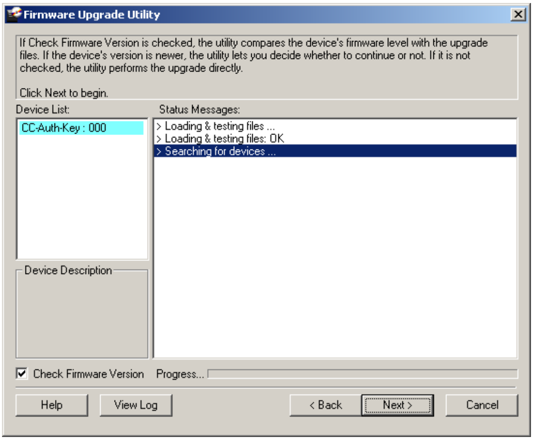
ATEN International Co., Ltd. ("Licensor") grants to you a non-exclusive, non-transferable license to access and use FIRMWARE UPGRADE UTILITY (the "Product") during the "Term" set forth below. You may install the Product on a hard disk or other storage device; install and use the Product on a file server for use on a network for the purposes of (i) permanent installation onto hard disks or other storage devices or (ii) use of the Product over such network; and make backup copies of the Product.

RESTRICTIONS

You agree not to modify, adapt, translate, reverse engineer, recompile, disassemble or otherwise attempt to discover the source code of the Product, or create derivative works based on the Product, or remove any proprietary notices or labels on the Product, including copyright, trademark or patent pending notices. You may not sublicense the Product or otherwise allow others to use the Product licensed to you.

● I Agree ○ I Don't Agree

7. The utility searches your installation. When it finds your device, it lists it in the *Device List* panel.



Firmware Upgrade Utility

If Check Firmware Version is checked, the utility compares the device's firmware level with the upgrade files. If the device's version is newer, the utility lets you decide whether to continue or not. If it is not checked, the utility performs the upgrade directly.

Click Next to begin.

Device List:

CC-Auth-Key : 000

Status Messages:

```
> Loading & testing files ...
> Loading & testing files: OK
> Searching for devices ...
```

Device Description

☑ Check Firmware Version

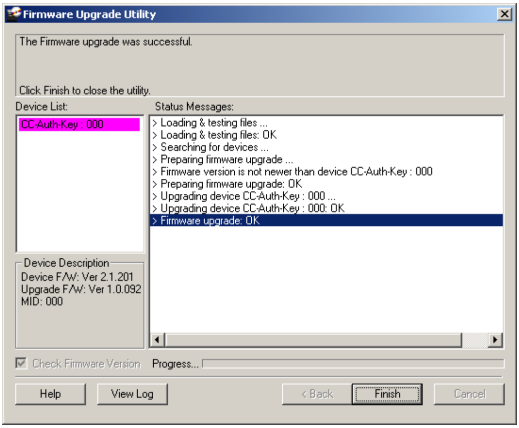
Note: If you enable *Check Firmware Version*, the Utility compares the device's firmware level with that of the upgrade files. If it finds that the device's version is higher than the upgrade version, it brings up a dialog box informing you of the situation and gives you the option to Continue or Cancel.

If you don't enable *Check Firmware Version*, the Utility installs the upgrade files without checking if they are a higher level.

Click **Next** to continue.

Upgrade Succeeded

After the upgrade has completed, a screen appears to inform you that the procedure was successful:



Firmware Upgrade Utility

The Firmware upgrade was successful.

Click Finish to close the utility.

Device List:

CC-Auth-Key : 000

Status Messages:

```
> Loading & testing files ...
> Loading & testing files: OK
> Searching for devices ...
> Preparing firmware upgrade ...
> Firmware version is not newer than device CC-Auth-Key : 000
> Preparing firmware upgrade: OK
> Upgrading device CC-Auth-Key : 000 ...
> Upgrading device CC-Auth-Key : 000: OK
> Firmware upgrade: OK
```

Device Description

Device F/W: Ver 2.1.201

Upgrade F/W: Ver 1.0.092

MID: 000

☑ Check Firmware Version

Progress...

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 stand-alone utility program (an Offline upgrade).

Clients first inform their dealers/distributors of the number of licenses to be upgraded. The dealers/distributors then place an order with an Altusen sales representative, specifying the number of licenses to be added. After processing the order, Altusen then sends a confirmation and authorization email 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:

- **On Line:** To perform the upgrade the key is inserted in the computer's USB port and a browser session is opened to directly upgrade the key. If the client performs the upgrade, the dealer/distributor provides him with the email authorization details; if the dealer/distributor performs the upgrade, the client provides him with the Authentication Key.
- **Off Line:** A Windows-based *Key Status Utility* is used to extract the key's information and write it to a Key Information Data File. The key information data file is then used in a a browser session to generate a license upgrade file. After the license upgrade file has been generated, the Key Status Utility is used again to write the upgrade file's information to the license key.
  - If the client is the one who updates the CC license database, the dealer/ distributor provides him with the email 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) which the dealer/distributor uses to generate the client's key license upgrade file. The dealer/distributor then returns the key license upgrade file to the client which the client uses with the Key Status Utility to upgrade the Authentication Key's license information.

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 Altusen sales representative, they receive a confirmation and authorization email, 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 7 more server(s) and 20500 more node(s)

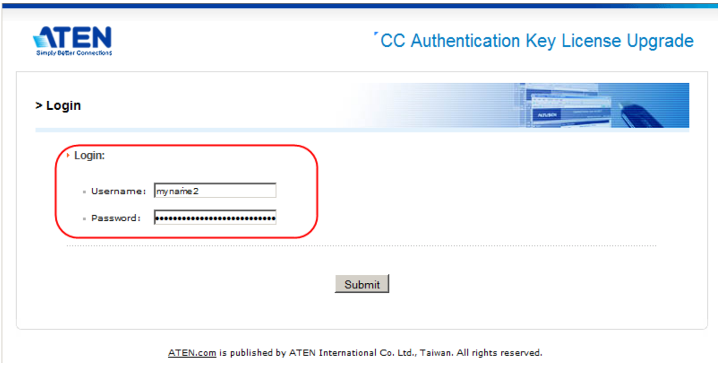
Either the client or the dealers/distributors can perform the upgrade. If the dealer does it, the client provides the dealer with his license key; if the client does it, the dealer forwards the confirmation email to him.

Follow the steps below to perform online upgrade.

1. Plug the authentication key into a USB port on your computer.
2. Open a browser, go to the website CC Authentication Key License Upgrade page:

   https://cc.aten.com.tw/

3. When the upgrade Login screen comes up, log in with the Username and Password provided in the authorization email.

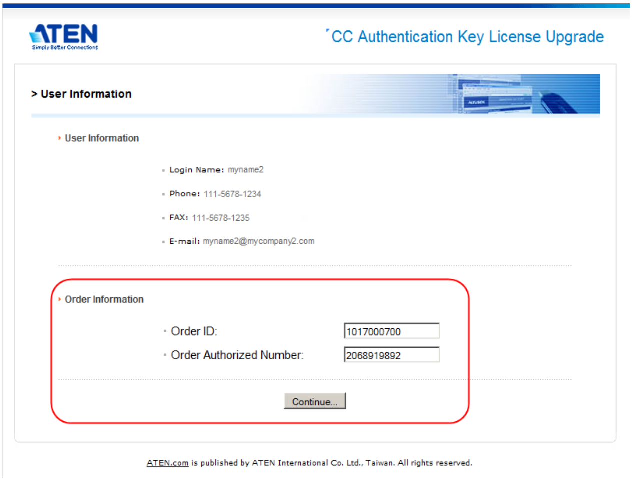

ATEN
Simply Better Connections
CC Authentication Key License Upgrade
> Login
Login:
Submit

Username: myname2

Password: ••••••••••••••••••••••••••

ATEN.com is published by ATEN International Co. Ltd., Taiwan. All rights reserved.

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**.



CC Authentication Key License Upgrade

> User Information

User Information

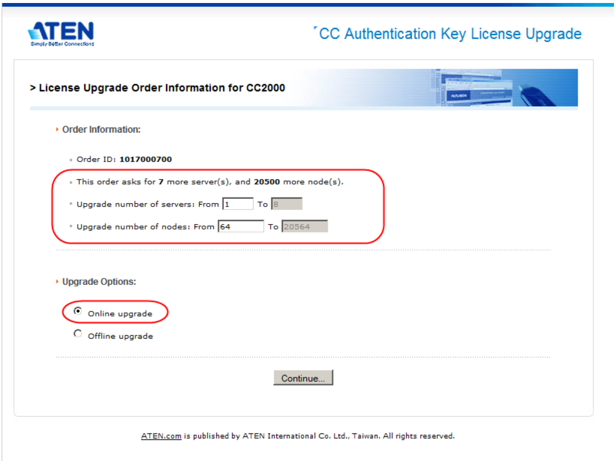
- Login Name: myname2
- Phone: 111-5678-1234
- FAX: 111-5678-1235
- E-mail: myname2@mycompany2.com

Order Information

- Order ID: 1017000700
- Order Authorized Number: 2068919892

ATEN.com is published by ATEN International Co. Ltd., Taiwan. All rights reserved.

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**.



CC Authentication Key License Upgrade

> License Upgrade Order Information for CC2000

Order Information:

- Order ID: **1017000700**
- This order asks for **7** more server(s), and **20500** more node(s).
- Upgrade number of servers: From 1 To 8
- Upgrade number of nodes: From 64 To 20564

Upgrade Options:

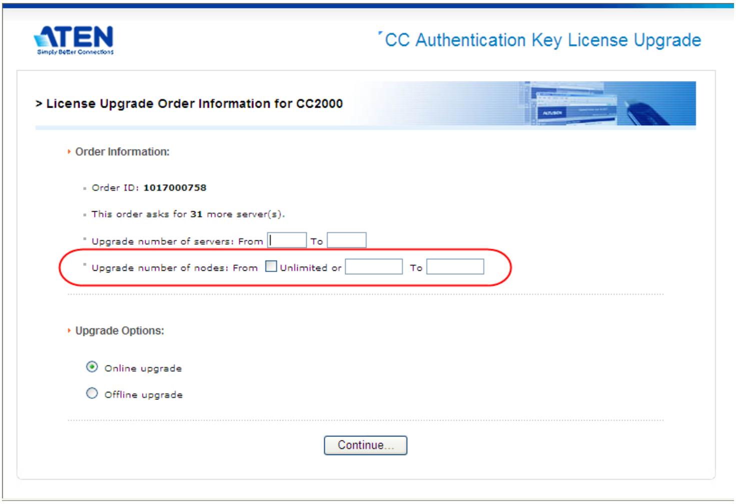
● Online upgrade

○ Offline upgrade

ATEN.com is published by ATEN International Co. Ltd., Taiwan. All rights reserved.

Note: You can use the Key status utility (CCAuthKeyStatus.exe) to see the current number of licenses.

If only server licenses are being upgraded, the Upgrade Order Information Screen looks like the one below. If the node licenses are already set to be *unlimited*, put a check in the checkbox; otherwise fill in the appropriate node numbers in the From field:



CC Authentication Key License Upgrade

> License Upgrade Order Information for CC2000

Order Information:

- Order ID: **1017000758**
- This order asks for **31** more server(s).
- Upgrade number of servers: From [ ] To [ ]
- Upgrade number of nodes: From □ Unlimited or [ ] To [ ]

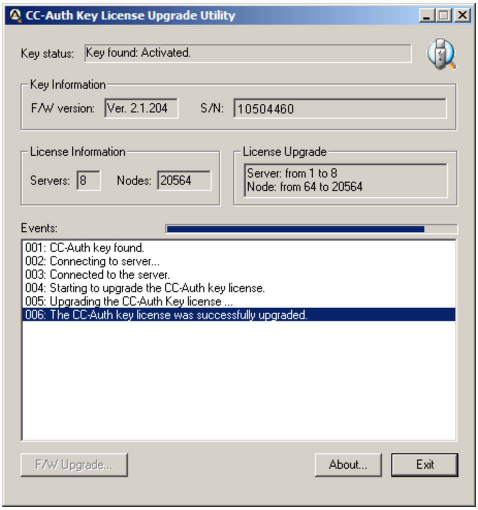
Upgrade Options:

● Online upgrade
○ Offline upgrade

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, exactly as it 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:



CC-Auth Key License Upgrade Utility

Key status: Key found: Activated.

Key Information

F/W version: Ver. 2.1.204 S/N: 10504460

License Information

Servers: 8 Nodes: 20564

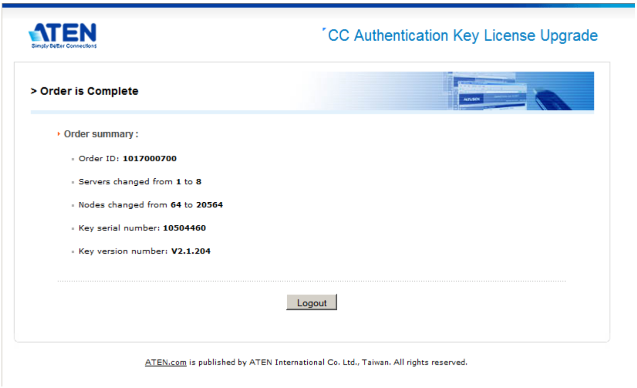
License Upgrade

Server: from 1 to 8
Node: from 64 to 20564

Events:

```
001: CC-Auth key found.
002: Connecting to server...
003: Connected to the server.
004: Starting to upgrade the CC-Auth key license.
005: Upgrading the CC-Auth Key license ...
006: The CC-Auth key license was successfully upgraded.
```

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:



CC Authentication Key License Upgrade

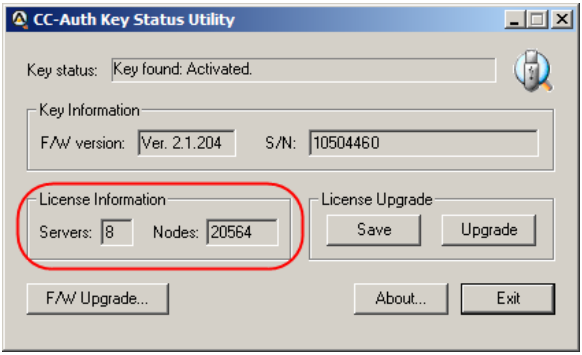
> Order is Complete

- Order summary :
  - Order ID: **1017000700**
  - Servers changed from **1** to **8**
  - Nodes changed from **64** to **20564**
  - Key serial number: **10504460**
  - Key version number: **V2.1.204**

ATEN.com is published by ATEN International Co. Ltd., Taiwan. All rights reserved.

11. Click **Logout** to exit.

You can use the Key status utility (CCAuthKeyStatus.exe) to confirm that the number of licenses on the key has been changed to reflect the successful upgrade:



CC-Auth Key Status Utility

Key status: Key found: Activated.

Key Information

F/W version: Ver. 2.1.204

S/N: 10504460

License Information

Servers: 8

Nodes: 20564

Upgrade Succeeded

After the upgrade has succeeded, the dealer/distributor receives an email from Altusen 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.

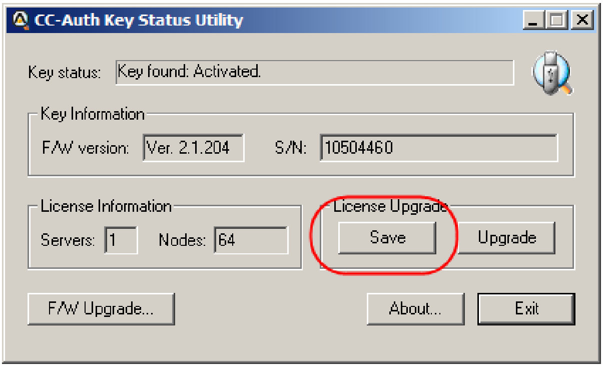
Offline Upgrade

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 email a 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 the *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).



CC-Auth Key Status Utility

Key status: Key found: Activated.

Key Information

F/W version: Ver. 2.1.204 S/N: 10504460

License Information

Servers: 1 Nodes: 64

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.

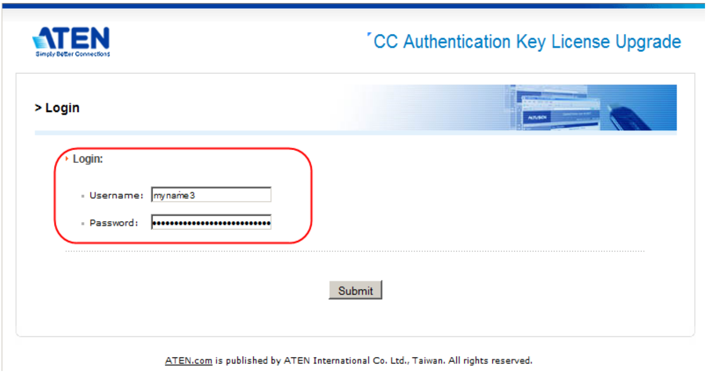
Performing the Upgrade

After the dealers/distributors place the upgrade orders with an Altusen sales representative, they receive a confirmation and authorization email 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:

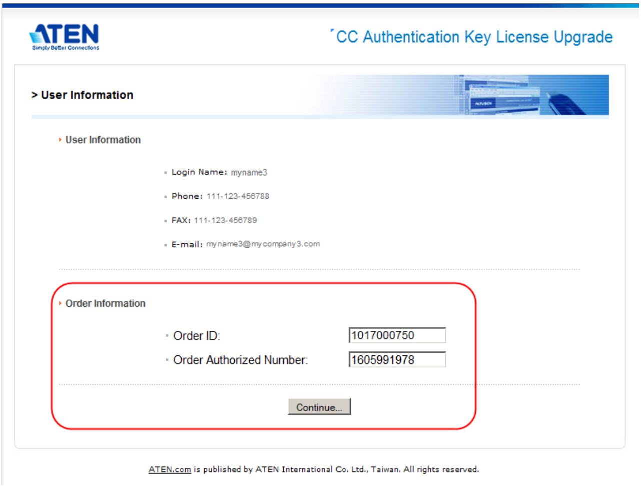
1. Follow steps 1 – 3 given for the Online Upgrade (see page 251).
2. When the upgrade Login screen comes up, log in with the Username and Password provided in the authorization email.


ATEN
Simply Better Connections
CC Authentication Key License Upgrade
> Login
Login:
Username:
Password:
Submit
ATEN.com is published by ATEN International Co. Ltd., Taiwan. All rights reserved.

Username: myname3

Password: ••••••••••••••••••••••••••

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**.



CC Authentication Key License Upgrade

> User Information

User Information

- Login Name: myname3
- Phone: 111-123-456788
- FAX: 111-123-456789
- E-mail: myname3@mycompany3.com

Order Information

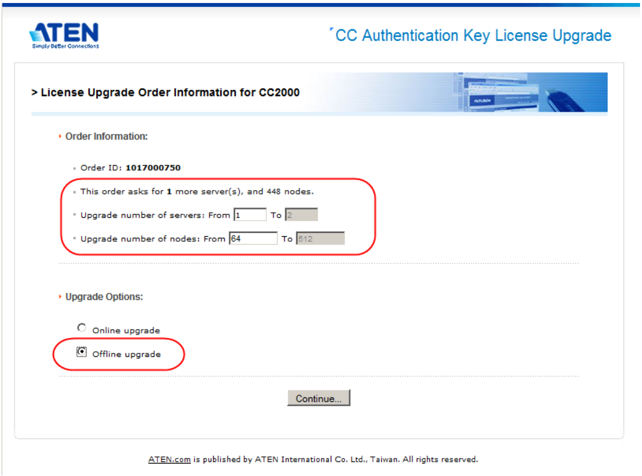
- Order ID: 1017000750
- Order Authorized Number: 1605991978

ATEN.com is published by ATEN International Co. Ltd., Taiwan. All rights reserved.

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 to be an Offline upgrade, then click **Continue**.



CC Authentication Key License Upgrade

> License Upgrade Order Information for CC2000

Order Information:

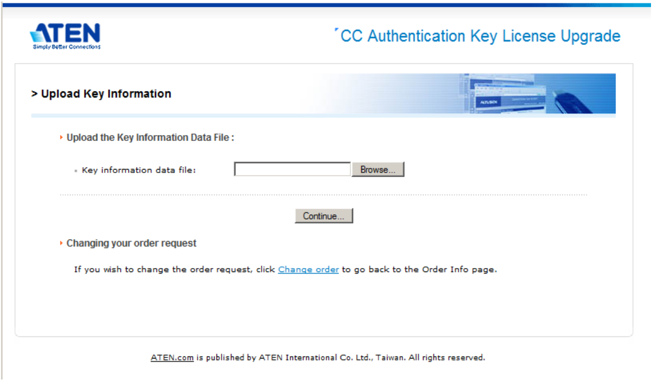
- Order ID: **1017000750**
- This order asks for **1** more server(s), and 448 nodes.
- Upgrade number of servers: From 1 To 2
- Upgrade number of nodes: From 64 To 512

Upgrade Options:

○ Online upgrade
● Offline upgrade

ATEN.com is published by ATEN International Co. Ltd., Taiwan. All rights reserved.

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**.



CC Authentication Key License Upgrade

> Upload Key Information

Upload the Key Information Data File :

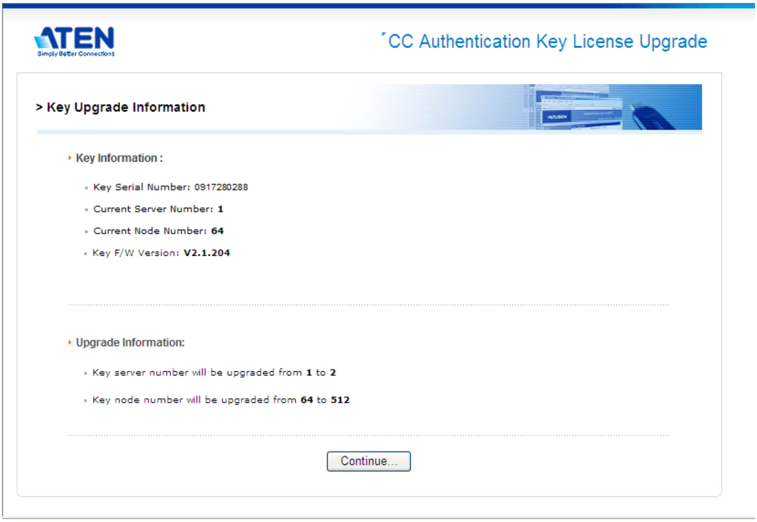
- Key information data file:

Changing your order request

If you wish to change the order request, click Change order to go back to the Order Info page.

ATEN.com is published by ATEN International Co. Ltd., Taiwan. All rights reserved.

7. The next screen that comes up summarizes the transaction up to this point.



CC Authentication Key License Upgrade

> Key Upgrade Information

Key Information :

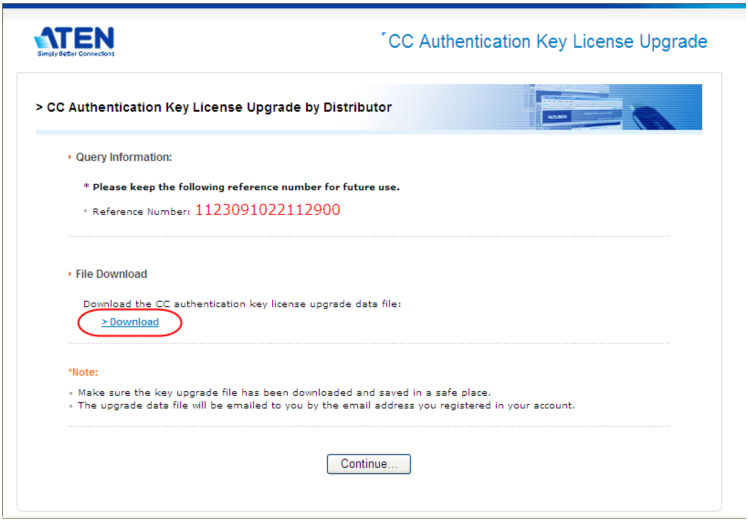
- Key Serial Number: 0917280288
- Current Server Number: **1**
- Current Node Number: **64**
- Key F/W Version: **V2.1.204**

Upgrade Information:

- Key server number will be upgraded from **1** to **2**
- Key node number will be upgraded from **64** to **512**

Click **Continue** to move on.

8. In the screen that appears next, click **Download** to download the key license upgrade data file (KeyUpgrade.dat).



ATEN

Simply Better Connections

CC Authentication Key License Upgrade

> CC Authentication Key License Upgrade by Distributor

Query Information:

* Please keep the following reference number for future use.

Reference Number: 1123091022112900

File Download

Download the CC authentication key license upgrade data file:

> Download

*Note:

- Make sure the key upgrade file has been downloaded and saved in a safe place.
- The upgrade data file will be emailed to you by the email address you registered in your account.

Continue...

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.

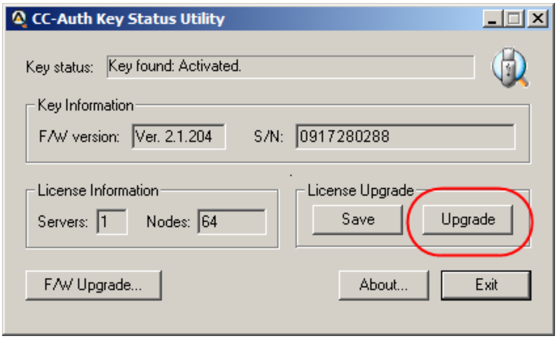
11. Click **Logout** to exit.

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**.



CC-Auth Key Status Utility

Key status: Key found: Activated.

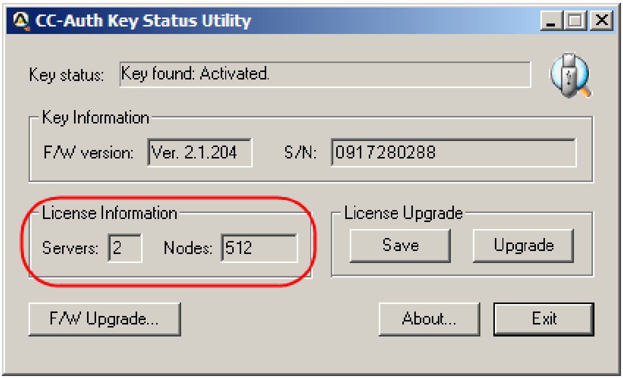
Key Information

F/W version: Ver. 2.1.204 S/N: 0917280288

License Information

Servers: 1 Nodes: 64

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.



CC-Auth Key Status Utility

Key status: Key found: Activated.

Key Information

F/W version: Ver. 2.1.204 S/N: 0917280288

License Information

Servers: 2 Nodes: 512

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 proceed:

- When the key upgrade file is downloaded, an email 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 email.

- 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 Altusen sends the dealer/distributor the confirmation/authorization email informing him that the order is ready to be processed, he has a total of two weeks to process the order. If during that time the order is not processed, two more emails 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 email is sent, informing the dealer/distributor that the order has expired, as follows:

Your order has expired and has been cancelled...
If you still wish to add licenses, you must place a new order.

This Page Intentionally Left Blank

Appendix D
External Authentication Services

Overview

In addition to its own internal *Username / Password* authentication procedure, the CC2000 supports authentication from external, third party authentication services. If a third party service has been specified for a user, the CC2000 transfers the login information to the appropriate service for authentication using an encrypted HTTPS (SSL) connection. The CC2000 supports the following third party external authentication servers: LDAP, LDAPS, Active Directory, RADIUS, TACACS+, and Windows NT Domain.

Approved Services

The following services have been tested and approved for use with the CC2000:

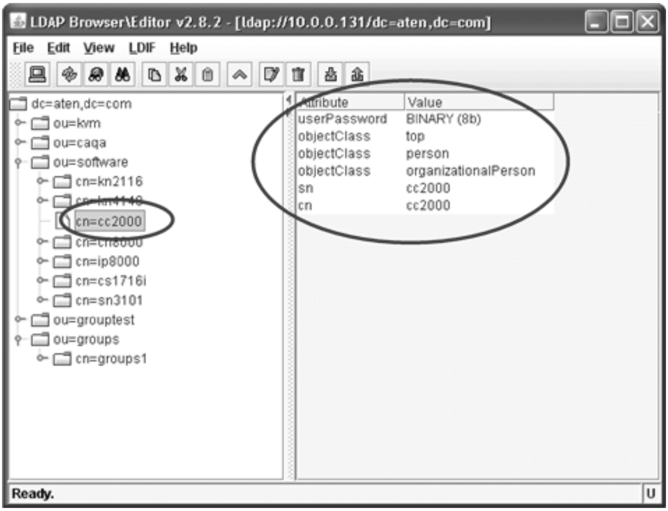
- AD Server: Microsoft Windows Server 2003
- LDAP: Microsoft Windows Server 2003; OpenLDAP
- RADIUS: Microsoft IAS for Windows Server 2003; FreeRADIUS
- TACACS+: Microsoft Windows Server 2003 (ClearBox)
- Microsoft Windows NT Domain

LDAP/LDAPS – OpenLDAP Setting Example

In this example, the external server uses OpenLDAP; its IP address is 192.168.10.100; its service port is 389, and the server administrator has created a file named: *cc2000ldap.ldif* in the OpenLDAP directory, that contains the following:

```
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:



LDAP Browser\Editor v2.8.2 - [ldap://10.0.0.131/dc=aten,dc=com]
File
Edit
View
LDIF
Help
Ready.
U

```
dc=aten,dc=com
  ou=kvm
  ou=caqa
  ou=software
    cn=kn2116
    cn=kn4140
    cn=cc2000
    cn=cn8000
    cn=ip8000
    cn=cs1716i
    cn=sn3101
  ou=grouptest
  ou=groups
    cn=groups1
```

Attribute	Value
userPassword	BINARY (8b)
objectClass	top
objectClass	person
objectClass	organizationalPerson
sn	cc2000
cn	cc2000

The CC2000 Administrator gets this information to use in the *Adding an External Authentication Server* procedure (see *LDAP*, page 137). 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

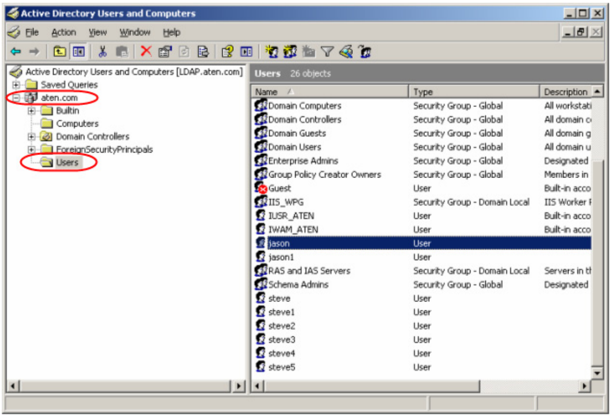
Full name attribute: sn

After the LDAP/LDAPS Authentication server has been added, the CC2000 Administrator can use the Browse button to browse all the user names in the *software* directory.

Active Directory Settings Example

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

1. Open Start → Control Panel → Administrative Tools → Active Directory Users and Computers → Domain (aten.com in our example) → Users. A window, similar to the one below, appears:


Active Directory Users and Computers
File
Action
View
Window
Help
Active Directory Users and Computers [LDAP.aten.com]
Saved Queries
aten.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
Users 26 objects

Name	Type	Description
Domain Computers	Security Group - Global	All workstati
Domain Controllers	Security Group - Global	All domain c
Domain Guests	Security Group - Global	All domain g
Domain Users	Security Group - Global	All domain u
Enterprise Admins	Security Group - Global	Designated
Group Policy Creator Owners	Security Group - Global	Members in
Guest	User	Built-in acco
IIS_WPG	Security Group - Domain Local	IIS Worker f
IUSR_ATEN	User	Built-in acco
IWAM_ATEN	User	Built-in acco
jason	User	
jason1	User	
RAS and IAS Servers	Security Group - Domain Local	Servers in th
Schema Admins	Security Group - Global	Designated
steve	User	
steve1	User	
steve2	User	
steve3	User	
steve4	User	
steve5	User	

The CC2000 Administrator gets this information to use in the *Adding an External Authentication Server* procedure (see *Active Directory*, page 136). In this example, the fields would be filled in as follows:

IP: 192.168.10.100

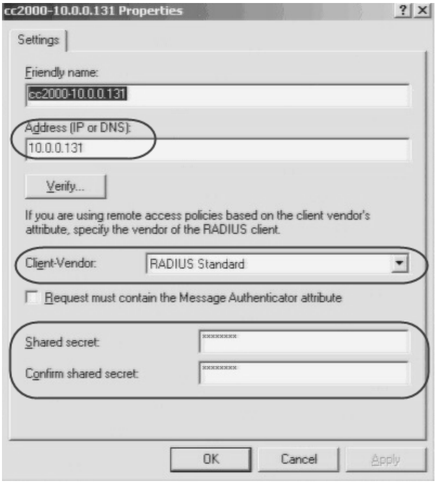
UserRDN: cn=users

After the Active Directory Authentication server has been added, the CC2000 Administrator can use the Browse button to browse all the user names in the *Users* directory.

RADIUS Settings Example

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

1. Open Start → Control Panel → Administrative Tools → Internet Authentication Services.
2. In the screen that comes up, right click on **RADIUS Client**.
3. Select **New RADIUS Client**.
4. In the screen that 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:



cc2000-10.0.0.131 Properties

Settings

Friendly name: cc2000-10.0.0.131

Address (IP or DNS): 10.0.0.131

If you are using remote access policies based on the client vendor's attribute, specify the vendor of the RADIUS client.

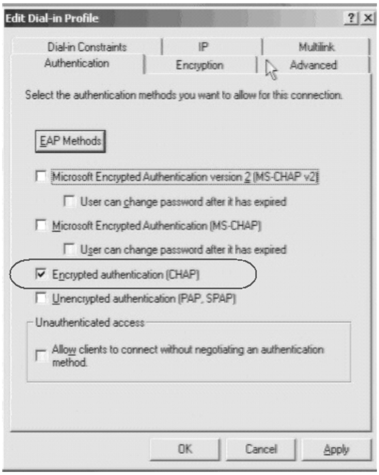
Client-Vendor: RADIUS Standard

□ Request must contain the Message Authenticator attribute

Shared secret: ********

Confirm shared secret: ********

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:



Select the authentication methods you want to allow for this connection.

☐ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

☐ User can change password after it has expired

☐ Microsoft Encrypted Authentication (MS-CHAP)

☐ User can change password after it has expired

☑ Encrypted authentication (CHAP)

☐ Unencrypted authentication (PAP, SPAP)

Unauthenticated access

☐ Allow clients to connect without negotiating an authentication method.

8. In this example we use CHAP for encrypted authorization

The CC2000 Administrator gets this information to use in the *Adding an External Authentication Server* procedure (see *RADIUS and TACACS+*, page 138). In this example, the fields would be filled in as follows:

IP: 10.0.0.100

Authentication type: CHAP

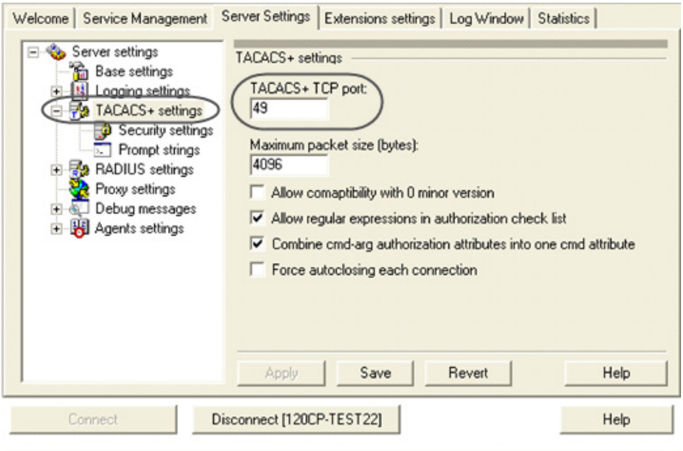
Shared secret: password

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 for the Login names.

TACACS+ Settings Example

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

1. Open Start → All Programs → ClearBox RADIUS TACACS+ Server → Server Manager.
2. In the screen that comes up, click **Connect**.
3. 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:



TACACS+ settings

TACACS+ TCP port: 49

Maximum packet size (bytes): 4096

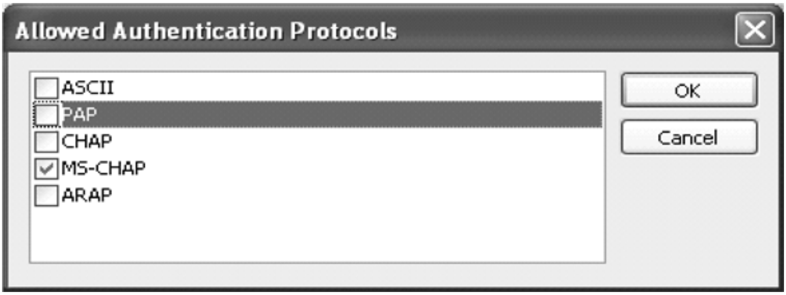
□ Allow comaptibility with 0 minor version

☑ Allow regular expressions in authorization check list

☑ Combine cmd-arg authorization attributes into one cmd attribute

□ Force autoclosing each connection

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:



Allowed Authentication Protocols

□ ASCII
□ PAP
□ CHAP
☑ MS-CHAP
□ ARAP

9. In this example we use MS-CHAP for the allowed authentication protocol.
10. You return to the *ClearBox Server Configurator* screen. In the left panel select Data Sources → users.
11. In the main panel of the screen that comes up, there is an MS Access entry field with a path specifying the *general.mdb* file. The accounts contained in this file are generated through MS Access.

The CC2000 Administrator gets this information to use in the *Adding an External Authentication Server* procedure (see *RADIUS and TACACS+*, page 138). In this example, the fields would be filled in as follows:

IP: 10.0.0.100

Port: 49

Authentication type: MSCHAP

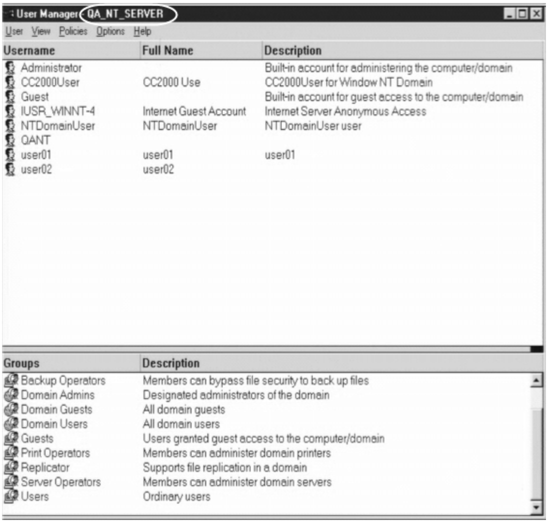
Shared secret: the password that you set when you installed the ClearBox RADIUS TACACS+ Server

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 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:



Username	Full Name	Description
Administrator		Built-in account for administering the computer/domain
CC2000User	CC2000 Use	CC2000User for Window NT Domain
Guest		Built-in account for guest access to the computer/domain
IUSR_WINNT-4	Internet Guest Account	Internet Server Anonymous Access
NTDomainUser	NTDomainUser	NTDomainUser user
QANT		
user01	user01	user01
user02	user02	

Groups	Description
Backup Operators	Members can bypass file security to back up files
Domain Admins	Designated administrators of the domain
Domain Guests	All domain guests
Domain Users	All domain users
Guests	Users granted guest access to the computer/domain
Print Operators	Members can administer domain printers
Replicator	Supports file replication in a domain
Server Operators	Members can administer domain servers
Users	Ordinary users

The CC2000 Administrator gets this information to use in the *Adding an External Authentication Server* procedure (see *Windows NT Domain*, page 139). In this example, the fields would be filled in as follows:

Server IP: QA_NT_SERVER

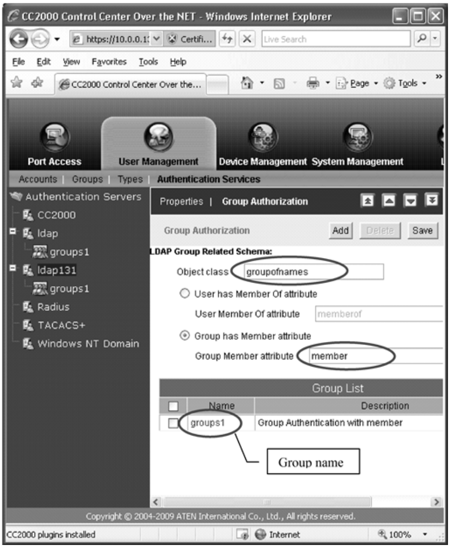
After the NT Domain server has been added, when the CC2000 Administrator adds user accounts, he must use the names that were configured under *User Manager for Domains*.

LDAP Group Authorization Setting Examples

Example 1

In this example the external server is OpenLDAP on Windows Server 2003 as shown in the LDAP/LDAPS Settings Example on page 265.

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 add the **groups1** group. The screen should look similar to the one below:


CC2000 Control Center Over the NET - Windows Internet Explorer
https://10.0.0.1
Certifi...
Live Search
File Edit View Favorites Tools Help
CC2000 Control Center Over the...
Page Tools
Port Access
User Management
Device Management
System Management
Accounts | Groups | Types | Authentication Services
Authentication Servers
CC2000
ldap
groups1
ldap131
groups1
Radius
TACACS+
Windows NT Domain
Properties | Group Authorization
Group Authorization
Add
Delete
Save
Copyright © 2004-2009 ATEN International Co., Ltd., All rights reserved.
CC2000 plugins installed
Internet
100%

LDAP Group Related Schema:

Object class: groupofnames

○ User has Member Of attribute

User Member Of attribute: memberof

● Group has Member attribute

Group Member attribute: member

Group List

□	Name	Description
□	groups1	Group Authentication with member

Group name

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

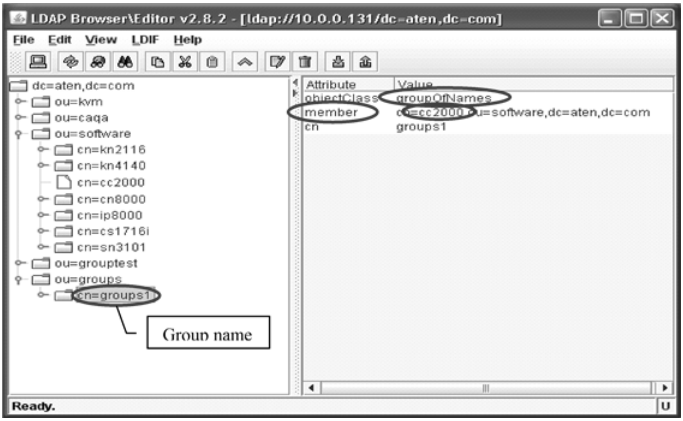
   cn: ***groups1***

Note: 1. The entry after dn: cn= should be the name of an actual group created under Group Authorization (see , page 142) on the CC2000 server.

2. The entry after objectclass: should be consistent with the name that was entered for the Object class when the group was created on the CC2000 server. Change the default entry in this file to match.

3. The entry after *member: cn*= should be an actual user login name.

3. You can check the group definition with LDAP Browser. You should see a screen similar to the one below:


LDAP Browser\Editor v2.8.2 - [ldap://10.0.0.131/dc=aten,dc=com]
File Edit View LDIF Help
Group name
Ready.
U

```
dc=aten,dc=com
  ou=kvm
  ou=caqa
  ou=software
    cn=kn2116
    cn=kn4140
    cn=cc2000
    cn=cn8000
    cn=ip8000
    cn=cs1716i
    cn=sn3101
  ou=grouptest
  ou=groups
    cn=groups1
```

Attribute	Value
objectClass	groupOfNames
member	cn=cc2000,ou=software,dc=aten,dc=com
cn	groups1

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* – can also supported under OpenLDAP by extending the schema.

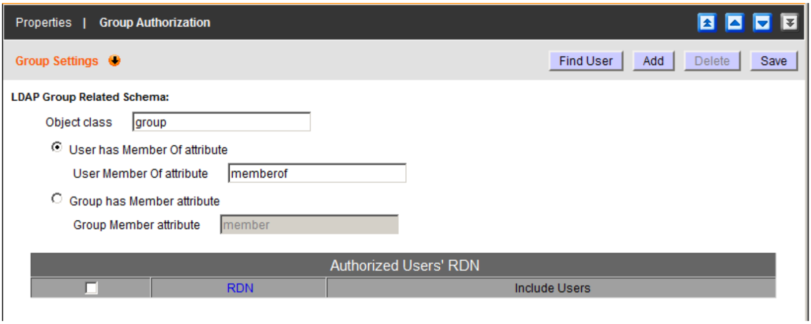
In this example the external server is OpenLDAP on Windows Server 2003 as shown in the LDAP/LDAPS Settings Example on page 265.

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 add the **groups1** group. The screen should look similar to the one below:



LDAP Group Related Schema:

Object class: group

● User has Member Of attribute

User Member Of attribute: memberof

○ Group has Member attribute

Group Member attribute: member

Authorized Users' RDN		
□	RDN	Include Users

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

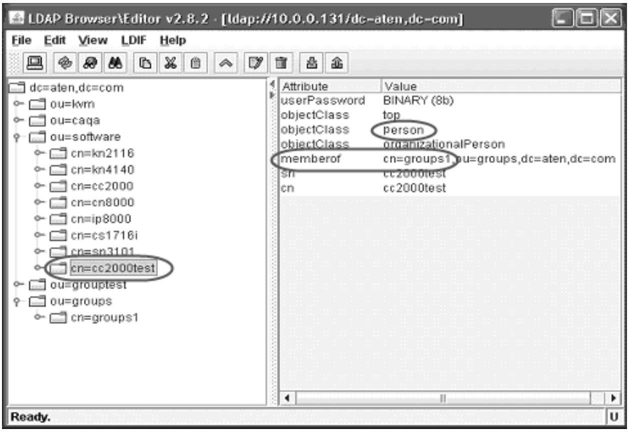
userPassword: password

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 (see , page 142) on the CC2000 server.

3. You can check the group definition with LDAP Browser. You should see a screen similar to the one below:


LDAP Browser\Editor v2.8.2 - [ldap://10.0.0.131/dc-aten,dc-com]
File
Edit
View
LDIF
Help
Ready.
U

```
dc=aten,dc=com
  ou=kvm
  ou=caqa
  ou=software
    cn=kn2116
    cn=kn4140
    cn=cc2000
    cn=cn8000
    cn=ip8000
    cn=cs1716i
    cn=sn3101
    cn=cc2000test
  ou=grouptest
  ou=groups
    cn=groups1
```

Attribute	Value
userPassword	BINARY (8b)
objectClass	top
objectClass	person
objectClass	organizationalPerson
memberof	cn=groups1,ou=groups,dc=aten,dc=com
sn	cc2000test
cn	cc2000test

4. Repeat step 2 for each user account that you want to add to the group.

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.

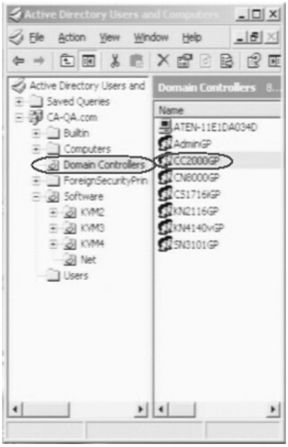
Active Directory Group Authorization Setting Example

In this example the external server is Active Directory on Windows Server 2003 as shown in the Active Directory Settings Example on page 267.

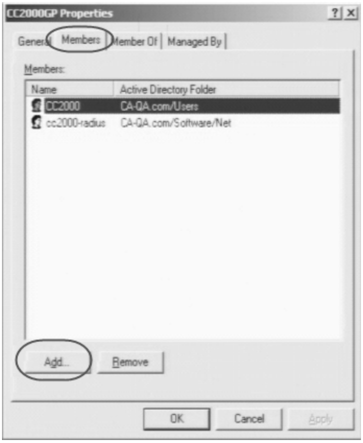
1. Under the CC2000 User Manager tab, select Authentication Services → Authentication Servers.
2. Select the Active Directory server; then click **Group Authorization**.
3. In this example add the **CC2000GP** group.

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:



Name	Active Directory Folder
CC2000	CA-QA.com/Users
cc2000-radius	CA-QA.com/Software/Net

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).

This Page Intentionally Left Blank

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 the HTML sample codes is 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>
&nbsp;&nbsp;
          </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">  &nbsp;&nbsp;&nbsp;&nbsp; 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>
```