ALTUSEN™
Enterprise KVM Solutions by ATEN

Control Center Over the NET™
CC1000
User Manual

FCC Information

This is an FCC Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

RoHS

This product is RoHS compliant.

SJ/T 11364-2006

The following contains information that relates to China.

部件名称	有毒有害物质或元素					
	铅	汞	镉	六价铬	多溴联苯	多溴二苯醚
电器部件	●	○	○	○	○	○
机构部件	○	○	○	○	○	○

○: 表示该有毒有害物质在该部件所有均质材料中的含量均在SJ/T 11363-2006规定的限量要求之下。

●: 表示符合欧盟的豁免条款，但该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T 11363-2006的限量要求。

×: 表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T 11363-2006的限量要求。

User Information

Online Registration

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

- International – http://support.aten.com
- North America – http://www.aten-usa.com/product_registration

Telephone Support

- International – 886-2-8692-6959
- North America – 1-888-999-ATEN

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 CC1000 package consists of:

1 CC1000 USB Authentication Key

1 USB Extension Bracket

2 USB Cables (1 External; 1 Internal)

1 Software CD

1 User Manual*

1 Quick Start Guide

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 CC1000 installation.

***** Features may have been added to the CC1000 since this manual was printed. Please visit our Website to download the most up to date version of the manual.

Manual Part No. PAPE-0263-3AXG
Printing Date:05/2007

Contents

Chapter 4.
The CC1000J Administrator Utility

Chapter 12.
Browser Operation

Appendix A
Technical Information

Appendix B
Authentication Key Utility

About This Manual

Overview

Chapter 1, Introduction, introduces you to the CC1000 System. Its purpose, features and benefits are described.

Chapter 2, CC1000J Server Installation, takes you through the procedures involved in installing the Java version of the CC1000 (CC1000J) on both Linux and Windows platforms.

Chapter 3, The CC1000J Manager, explains the CC1000J Manager interface and the procedures involved in configuring the CC1000J system.

Chapter 4, The CC1000J Administrator Utility, describes in detail how to manage users, groups, and devices.

Chapter 5, CC1000J Browser Operation, describes how to use a standard browser to log in and access the devices on your CC1000J installation.

Chapter 6, CC1000 Installation Overview, provides an installation overview of the Windows-based component of the CC1000.

Chapter 7, Authentication Server Setup, describes how to set up your Authentication Server on a Windows 2000 Server or Windows Server 2003 system.

Chapter 8, CC1000 Server Setup, takes you through the steps involved in installing the CC1000 program on your Windows 2000 Server or Windows Server 2003.

Chapter 9, The Log Server, explains how to configure the Log Server and how to query its records.

Chapter 10, The CC1000 Manager, explains the CC1000 Manager interface and the procedures involved in configuring the CC1000 system.

Chapter 11, The Administrator Utility, describes in detail how to use this utility to manage users, groups, and devices.

Chapter 12, Browser Operation, describes how to log in and access the devices on your CC1000 installation using a standard browser.

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

Appendix B, Authentication Key Utility, explains how to use the utility to upgrade the authentication key's firmware, and user licenses.

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**
- North America – **http://www.aten-usa.com**

Chapter 1
Introduction

Overview

The CC1000 Control Center Over the Net™ provides secure, centralized access, administration and management of your entire network—local and worldwide—anywhere; anytime. By consolidating the management of your ALTUSEN/ATEN IT devices, the CC1000 allows every device to be securely accessed and controlled by means of a single IP address.

Servers and network equipment are integrated into a single tree view, making the CC1000 ideal for enterprises with data centers and branch offices, located in several remote locations. An intuitive, browser-based GUI interface provides convenient access and control of all equipment.

The system comes in two configurations: one designed to run under Windows; the other—to allow multiplatform operation—designed to run under Java. The Java-based configuration (for Windows and Linux) is discussed in Chapters 2–5; the Windows-based configuration is discussed in Chapters 7–12.

Note: For Windows systems, you can install both the Java-based and Windows-based configurations. You can run either one, but you can't run them both at the same time.

Features

Secure Centralized Management

- Complete control of your enterprise – consolidates the management of all ATEN IT devices
- Single IP address to securely access every device on the installation
- All devices are integrated into a single tree view for centralized access, administration, and management of a worldwide network from anywhere at anytime
- Web browser access over Internet/Intranet provides secure remote connections to all installed devices

Highlights

- Java version runs on Windows and Linux for multiplatform support
- Ideal for enterprises with one or more data centers, or a number of remote offices
- Easy to use – intuitive browser-based GUI for simplified access to IT equipment in global data centers and remote offices
- Scalability – Multi-user access to hundreds of ATEN IT appliances and more than ten thousand servers and serially controlled devices
- A single login provides secure, centralized management of multiple data centers, branch offices and remote locations
- Provides centralized management, Role-Based Access and Control (RBAC), and Reporting Capabilities

Powerful Security

- Powerful security features that enable integration with LDAP (Java version) and Active Directory (Windows AP version) external authentication tools
- Robust security policies for individual user authorization to the port level
- 128-bit SSL encryption of all data on the network
- Flexible session time-outs
- “Strong” user name and password authentication
- Devices can identify themselves by Name or IP in the browser – device’s IP can remain hidden from people passing by

- **Network Interfaces**
  - TCP/IP
  - HTTP / HTTPS
  - SSL
  - DNS
  - LDAP / LDAPS
- **Software Features**
  - All features - including access, configuration and administration - accessible over the Net
  - Powerful portal-like interface provides customized permission-based groupings and device views
  - ATEN IT appliance auto-discovery with device-availability status, and alarms
- **Access and Control from Anywhere at Anytime**
  - An array of flexible logging and reporting options with audit trails for diagnostics and troubleshooting
  - View and manage active user sessions and active ports in real time
  - Maximum number of simultaneous connections can be set for each device

This Page Intentionally Left Blank

Chapter 2
CC1000J Server Installation

Overview

Recognizing the increasing importance of Linux in the server environment, CC1000J, the Java version of the CC1000 Control Center Over the NET system makes the CC1000's management capabilities available to both Windows and Linux platforms that have Java 2 installed.

Requirements

- A supported Operating System:
  - Windows: 2000, XP, 2000 Server, Server 2003 or Windows Vista

    Note: Windows Vista is supported in CC1000J version 1.2.111 and higher.

  - Linux: (most versions)
- JDK Ver. 1.5 or higher
- All ALTUSEN/ATEN 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.

CC1000J Components

The CC1000J comprised of two components as shown in the table below:

Component	Function
CC1000 Administrator Utility	Manages users and devices.
CC1000 Server	Provides the user interface to the CC1000 system; manages CC1000 sessions and access to devices. Stores user and device information; authenticates user access. Stores all system logs in a searchable database.

Note: Both components get installed to the same computer. Users with proper authorization, however, can log into the CC1000J with a browser and download the CC1000 Administrator Utility component to any computer to administer the installation remotely.

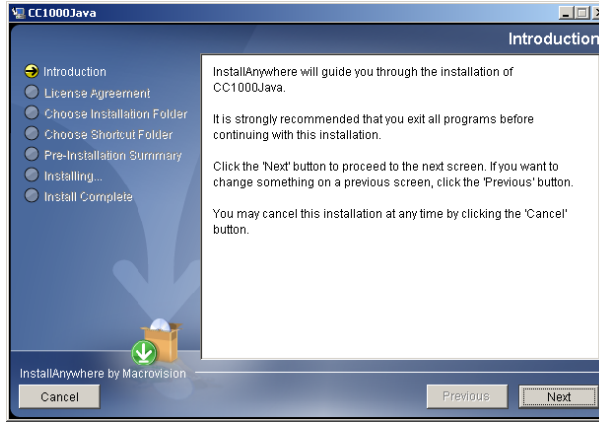
Windows Version Installation

Before running the installation program make sure of that version 1.5 or higher of the JDK has been installed on your system. If not, you need to download and install it. You can get the latest version of the JDK from the Sun Java web site:

http://java.sun.com

After the JDK has been installed on your system, you are ready to install the CC1000J program. To install CC1000J on a Windows system, do the following:

1. Plug the CC1000 USB Authentication Key into a USB port on the computer you are installing the CC1000J Server on. For security purposes, the key can be installed inside the case. See page 196 for details.
2. Copy *CC1000J-Setup-ForWindows.exe* from the software CD that came with your package to a convenient location on your server.
3. Go to the folder where *CC1000J-Setup-ForWindows.exe* is located, and execute it. A screen, similar to the one below, appears:

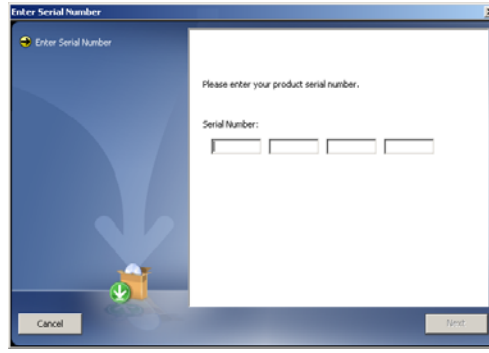


Click **Next** to move on.

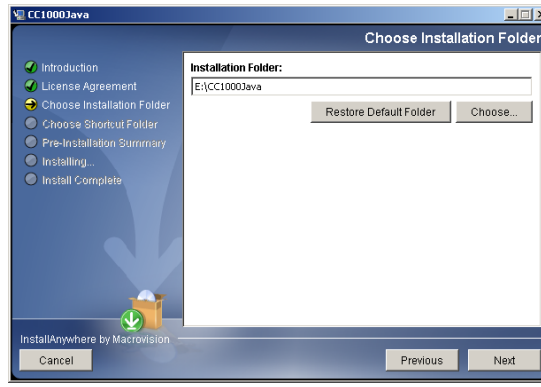
4. In the *License Agreement* screen that comes up, scroll down to the very bottom to activate the *I accept...* radio button:

5. Click to enable the *I accept...* radio button, then click **Next** to continue.

6. In the dialog box that comes up, key in your product's serial number (the serial number can be found on the CC1000's CD case), then click **Next** to continue.

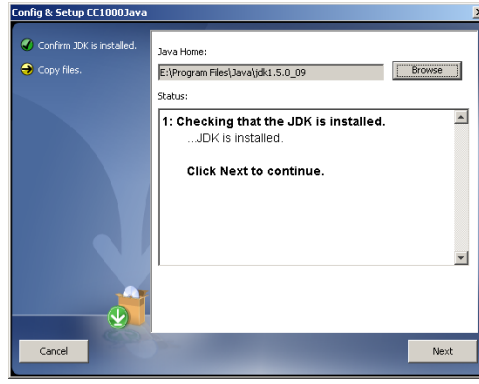


7. In the *Choose Installation Folder* dialog box, specify the CC1000J's installation folder. If you don't want to use the default entry, click **Choose...** to browse to the location that you want, then click **Next** to continue.

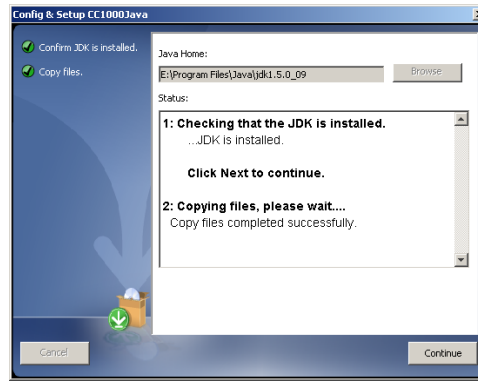


8. In the *Choose Shortcut Folder* dialog box, click one of the radio buttons to specify where you would like to create product icons, then click **Next** to continue.

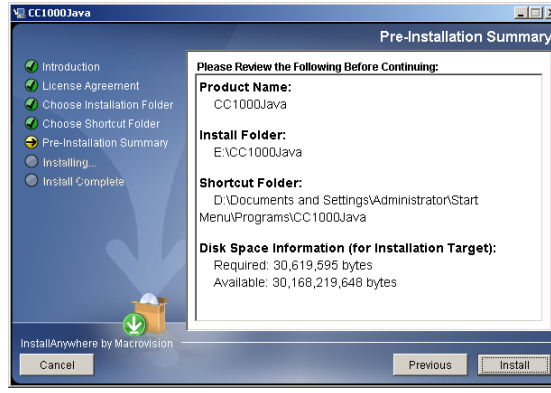
9. In the dialog box that comes up, specify the Java Home location (where the JDK has been installed). After the location has been confirmed, click **Next** to continue.



10. 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.



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

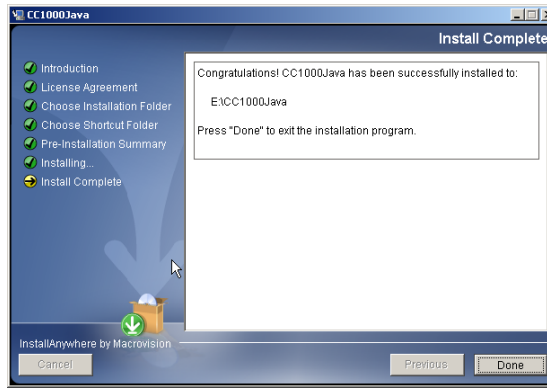


If you wish to change anything, click **Previous** to go back, If the information is correct, click **Install**.

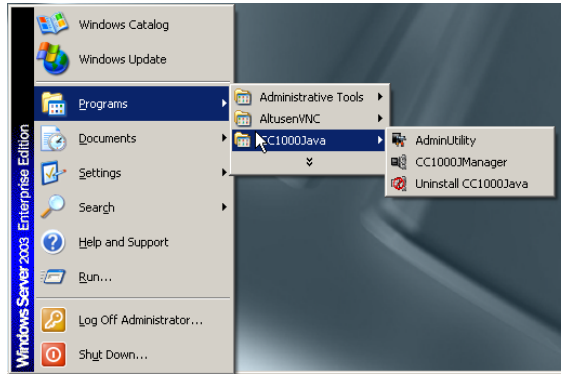
Note: If a dialog box comes up during the install informing you that a newer version of the *lax.jar* file already exists, you can overwrite it or not overwrite it – it doesn't matter which.

---

12. When the installation utility brings up a screen informing you that the installation has completed successfully, click **Done** to exit the installer.



13. At the completion of the installation, a CC1000J entry is created in the Windows *Start* menu:



Linux Version Installation

Before you Begin

The procedure for installing CC1000J on a Linux system is similar to that for Windows, but there are Java considerations to take note of first.

- Some distributions install an earlier version of Java than the JDK 1.5 required by the CC1000J program. To determine the Java version on your system, open a terminal and enter the following:

  ```
  java -version
  ```

  If the version it displays refers to a Java version that is earlier than JDK 1.5, you must install a JDK version that is 1.5 or higher.

  Note: The above only checks the JRE (Java Runtime Environment) version. This is usually the same as the JDK, but may not be so. If you are unsure that the JDK is high enough, we recommend a fresh install using a JDK version at least as high as the one specified in the requirements section of this manual (see *Requirements*, page 5).

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

  ```
  PATH=/usr/java/jdk1.5.0_09/bin:$PATH:$HOME/bin:./
  JAVA_HOME=/usr/java/jdk1.5.0_09
  BASH_ENV= $HOME/.bashrc
  USERNAME= "root"
  export USERNAME BASH_ENV PATH JAVA_HOME
  ```

- 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 *CC1000J-Setup-ForLinux.bin* file from the distribution CD to a folder on your hard disk.
  2. Open a terminal and go to the directory where the *CC1000J-Setup-ForLinux.bin* file is located.
  3. Enter the following commands:

     ```
     export LAX_DEBUG=1
     sh CC1000J-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 JDK has been installed, do the following:

1. If you haven't already done so, copy the *CC1000J-Setup-ForLinux.bin* file from the distribution CD to a folder on your hard disk.

2. Open the folder that you copied the installation file to, and run the *CC1000J-Setup-ForLinux.bin* program.

Note: 1. You must run the installation program as the root user. For some versions of Linux, the program must be run in a terminal.

2. Make sure that the installation file has executable permissions

---

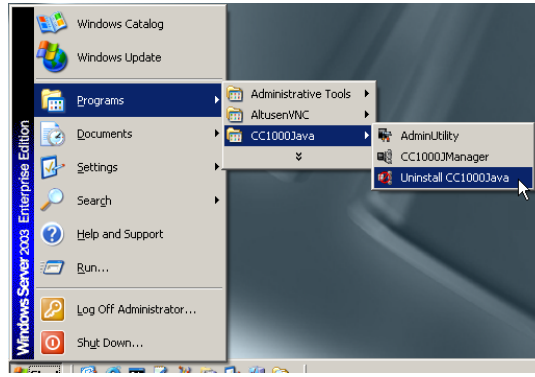
3. Refer to the Windows installation procedure (see page 6), for details on how to proceed once you start the installation program.

Uninstalling CC1000J

Uninstalling from a Windows System

To uninstall CC1000J from a Windows system, do the following:

1. Open the *Start* menu.
2. Navigate to the CC1000Java entry (Programs → CC1000Java), and select **Uninstall CC1000Java**.



Uninstalling from a Linux System

To uninstall CC1000J from a Linux system, as root, execute the following command:

```
/install-path/Uninstall_CC1000Java/Uninstall_CC1000Java
```

Where */install-path* represents the directory that you specified for CC1000J's location when you installed the program.

Upgrading the CC1000J

If CC1000J has already been installed, it is not necessary to perform a full install. You can upgrade to the latest CC1000J version by running the CC1000J-Upgrade program:

- CC1000J-Upgrade-ForWindows.exe (for Windows)
- CC1000J-Upgrade-ForLinux.bin (for Linux)

The files can be found in the *CC1000 Java Version* folder on the software CD that came with your CC1000J package (CC1000 Software → CC1000 Java Version).

When you run the upgrade program, simply follow the Wizard to complete the procedure.

Note: 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.

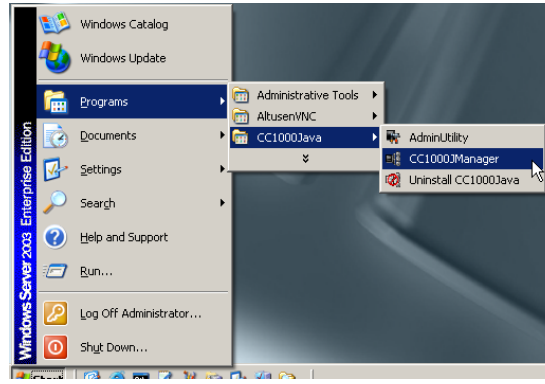
Chapter 3
The CC1000J Manager

Overview

The CC1000J Manager works in tandem with the Administrator Utility, and the CC1000J configuration parameters are set here.

To run the program make sure that the USB authentication key is attached, then do the following:

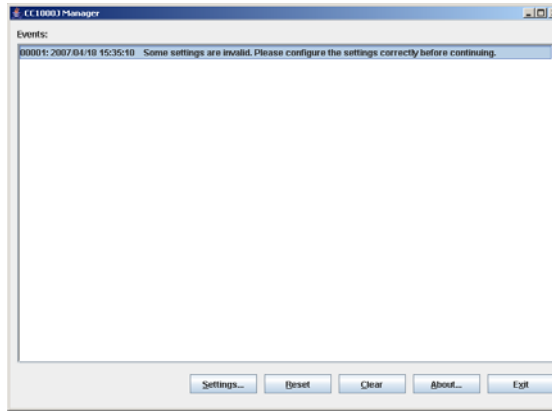
- On a Windows system, Open the *Start* menu; navigate to the CC1000Java entry (Programs → CC1000Java), and select **CC1000JManager**.



- On a Linux system, open a terminal session; go to the directory that CC1000J is installed on; and run the CC1000J Manager shell file (CC1000JManager).

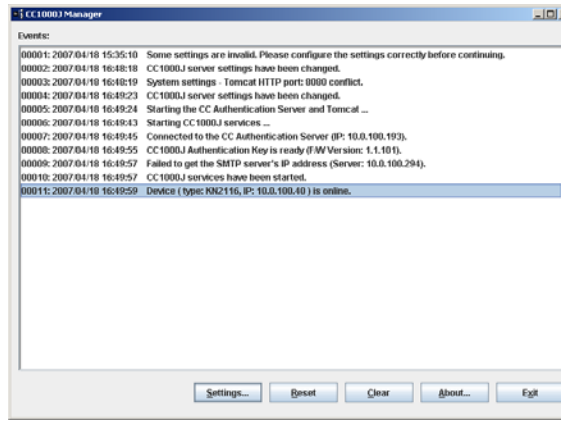
The First Time

The first time the CC1000J Manager comes up, a screen like the one below appears:



This screen appears with this message because the configuration parameters haven't been set yet. After a brief pause, the program automatically brings up the Settings dialog box where you specify the configuration parameters.

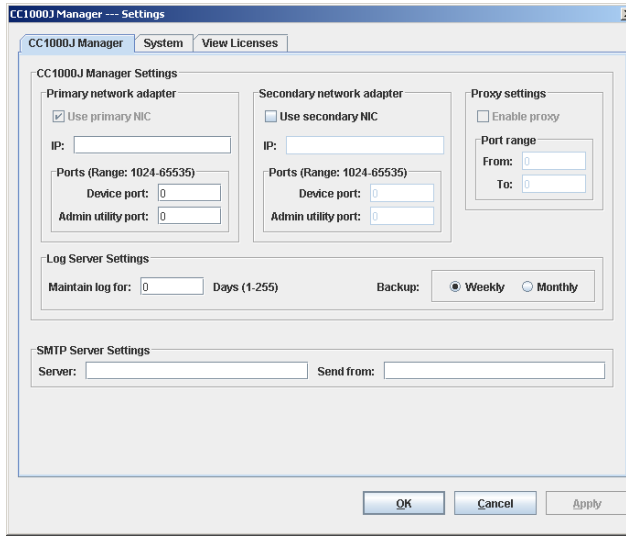
Once the settings have been properly configured (see page 18 for details), and you go back to the CC1000J Manager screen, it now looks similar to this:



- Messages concerning events that take place on the CC1000J appear in the *Events* panel.
- The *Settings* button brings up a dialog box that lets you set configuration values for the CC1000J system. (Details are provided in the sections that follow.)
- The *Reset* button stops the program and then restarts it - saving you the trouble of having to close the window and go through the execution procedure again.
- The *Clear* button erases the contents of the Events panel and starts over with a clean screen.
- The *About* button provides information about the CC1000J Manager program.

Configuration

When you click the *Settings* button, the CC1000J Manager Settings dialog box appears:



The settings dialog box has three tabs: *CC1000J Manager*, *System*, and *View Licenses*. Each of the tabs is described in the sections that follow.

The Manager Tab

The CC1000J Manager tab is divided into five panels as follows:

The Primary and Secondary Network Adapters:

The CC1000 makes use of one or two network adapters (two are recommended). If you use only one, it is the Primary adapter; its checkbox is enabled, and can't be disabled.

If you use two adapters – one for an Intranet (internal) and one for the Internet (external), for example – then you must enable the Secondary adapter (click to put a check in the *Use Secondary NIC* checkbox), and provide the appropriate IP address and port information.

The meanings of the fields are described in the following table:

Field	Meaning
IP	The IP address assigned to the network adapter of the computer that CC1000J is installed on.
Device port	The port is the port that the CC1000 Manager uses to communicate with the devices on the installation (CN-6000, PN9108, SN0116, etc.).
Admin utility port	The port that the CC1000 Manager uses to communicate with the Administrator Utility.

Note: 1. You cannot use 0.0.0.0 or 255.255.255.255 for the IP address of either the Primary or Secondary NIC.

2. No two ports on the same NIC can have the same value.

Proxy Settings:

To allow users to access CC1000 managed devices over a WAN you have to enable the proxy function (put a check in the *Enable Proxy* checkbox). Since this function makes use of the Secondary Network Adapter, it only becomes available if the Use Secondary NIC function is enabled (refer to the discussion in the previous section).

After enabling *Proxy Setting*, specify a range of ports for the CC1000 Manager to use for this function. The valid range is from 1024 to 65535, with a minimum difference of 500.

Note: 1. If the CC1000 Server is behind a firewall, the proxy ports set here must be allowed by the firewall.

2. If you use this feature, when you Save the settings the program checks the *Secondary network adapter* and *Proxy settings* fields. If there is an error, it brings the cursor to the invalid field and asks you to re-enter the information for that field.

Log Server Settings:

There are two settings for this panel, as shown in the table, below:

Field	Setting
Maintain Log For	Allows you to specify the number of days that the log entries can be kept in the current working database.
Backup	Allows you to specify the timeframe for database backups.

SMTP Server Settings:

The CC1000 sends email notification of event traps (as defined by each device), on installed devices to users of those devices.

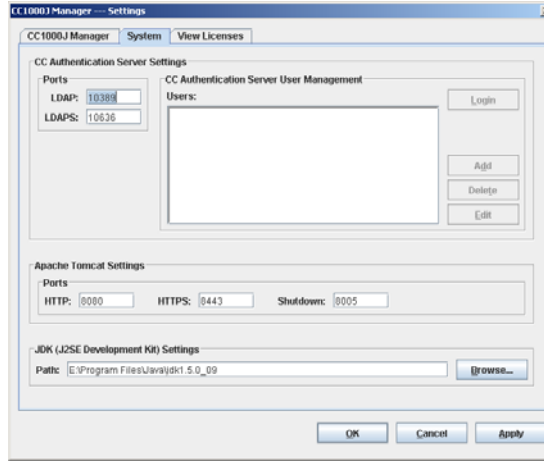
Note: Recipients are designated in each device's configuration settings. See the device's User Manual for details.

Specify the IP address or the domain name of the computer running your SMTP server in the *Server* field. Specify the CC1000 administrator's email address in the *Send From* field.

Note: This field cannot be blank.

The System Tab

The System Tab lets you configure your LDAP, Apache Tomcat, and JDK settings:



LDAP:

- In the *Ports* panel, set the ports that LDAP and LDAPS (secure LDAP) listen on.
- The **LDAP User Management** section becomes active after an administrator or user logs in by clicking the **Login** button. After a successful log in, the *Users* panel lists all the users that have been added to the CC1000J LDAP authorization database.

  Note: This is an authorization list that gives the users who are on it authorization to access the *Administrator Utility* (The *Administrator Utility* is discussed in Chapter 4.)

- The preconfigured *LDAPManager* entry is for the person responsible for managing the LDAP database. Only the LDAPManager can **Add** or **Delete** users. Regular users can only access the **Edit** function to modify their passwords.
- The default LDAPManager Login name is *ldapmanager*; the LDAPManager password is *password*. For security reasons, we recommend that you change the password to something unique.
- To add a user, click **Add**; fill in the user's username and password information; then click **OK**.
- To delete a user, select the user from the list, then click **Delete**. In the confirmation dialog box that comes up, click **OK** to delete the user, or **Cancel** to abort the operation.
- To change a user's password, click **Edit**. In the dialog box that comes up, make your changes, then click **OK**.

Apache Tomcat:

- The *HTTP* port is the regular port that Apache Tomcat listens on.
- The *HTTPS* port is the secure port that Apache Tomcat listens on.
- The *Shutdown* port is the regular port that Apache Tomcat listens on.

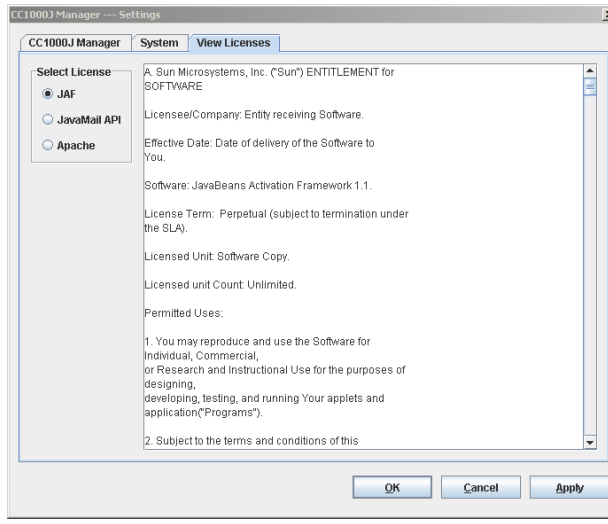
Note: If the default port settings conflict with other programs, you can change them to whatever you wish. You must restart CC1000J in order for the new settings to take effect.

JDK:

This field indicates the Java Development Kit's location.

The View Licenses Tab

The View Licenses Tab lets you view the licenses that are related to the CC1000J package. To view a license, click its radio button.



Finishing Up

When you have finished making all your configuration entries, click **OK** to save your settings. If there is an error in any of the entries, the pointer will move to the invalid field. Change the entry to a valid one, then click **OK**, again. A dialog box appears informing you that the CC1000J Manager must be restarted and asks if you want to proceed. Click **Yes** to confirm; click **No** to discard the changes.

To exit without saving any changes that you made, click **Cancel**. A dialog box appears, asking you to confirm that you want to discard your changes. Click **Yes** to confirm and exit; click **No** to return to the Configuration dialog box.

After you have saved your settings, you return to the CC1000J Manager main screen. This time, events that have taken place are listed in the main panel.

Chapter 4
The CC1000J Administrator Utility

Introduction

The CC1000J Administrator Utility is a client utility that allows administrators to manage users and devices in LDAP. The utility provides four management functions: device management; user management; group management; and the import/export of configuration data. All devices, folders, users, and groups are managed in a tree view. Specific context menus can be accessed by right clicking on each item.

Getting Started

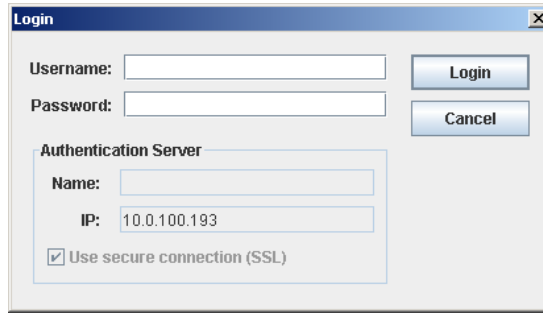
To start the program:

- Under Windows, open Start → Programs → CC1000Java→ AdminUtility
- Under Linux, as root, run **AdminUtility** from a terminal session.

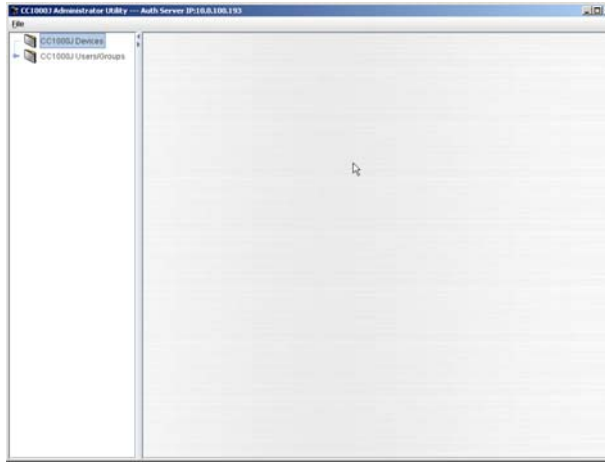
> **Note:** If your version of Linux supports it, you can run the program by clicking or double clicking the **AdminUtility** icon.

Logging In

After launching CC1000J, a login dialog box similar to the one below appears:



Key in Username and Password (set in LDAP – see page 21 for details), then click **Login** to bring up the Administrator Utility Main Screen:



Devices, Users, and Groups are created and managed from this screen. The first time you run the utility, except for a *Super Administrator* installed under the *Users* folder, there are no device folders, devices, users, or groups listed under the root folders. The following sections describe how to create and manage Devices, Users, and Groups.

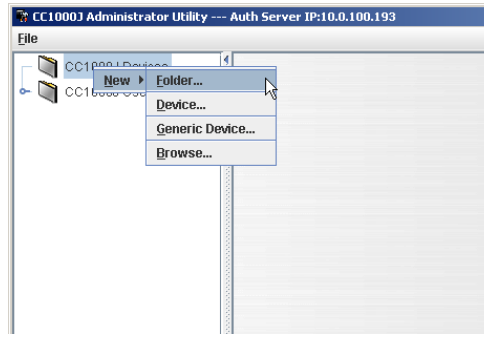
Note: For security purposes, the default Super Administrator password (*password*), should be changed to something unique.

Device Management

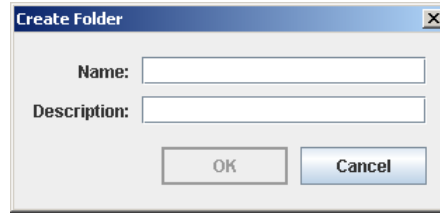
Creating Device Folders

Device folders are containers for devices which allow you to organize your enterprise-wide devices into useful categories (location, department, etc.). To create a device folder, do the following:

1. Right click on the *CC1000J Devices* folder.
2. In the pop-up menu that appears, select New → Folder.

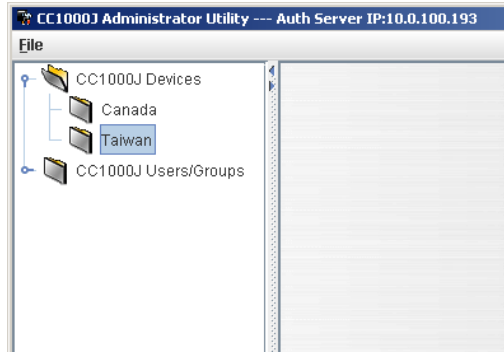


3. The *Create folder* dialog box appears.



4. Enter a name and a description for the folder.

5. Click **OK**. The folder appears as a subfolder of the CC1000J *Devices* root folder:

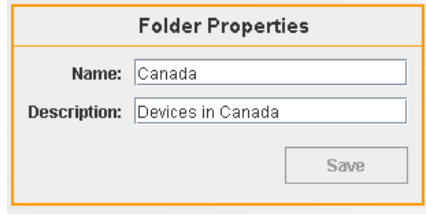


Nesting Device Folders

You can nest device folders. For example, you could have a Taipei device folder and a Taizhong device folder as sub folders under the Taiwan folder. Just right click on the folder you want to put a sub folder in and select *New* from the pop-up menu, as above.

Folder Properties

When you create a folder, its *Properties* screen appears with the name and description you assigned it.



This box disappears when you make another selection in the *Tree List*.

You can change a device folder's name and/or description at any time by selecting it in the tree list. When its *Properties* screen comes up, make your changes and click **Save**.

Adding Devices

Devices are added to the device folders that are appropriate for them. For example, you would create a device for a PN9108 that was in Taiwan, in the *Taiwan* device folder.

There are two methods to add a device. The first is to manually add it; the second is to use the CC1000J to add it by browsing the device list (see *Adding Devices by browsing:*, page 30).

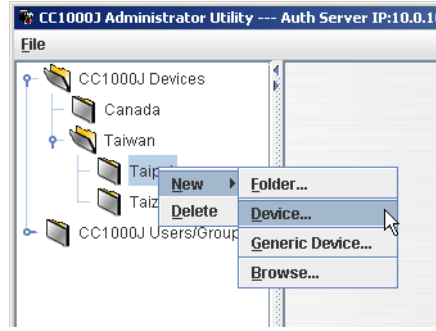
Note: Devices to be added must be powered on and have CC management enabled and configured in their settings.

Browsing the device list is the simplest way to add a device to a folder, because the device provides information about itself, such as its name, type, and MAC address. In this way, you ensure the accuracy of the device information and save the time normally required to gather and type in the information.

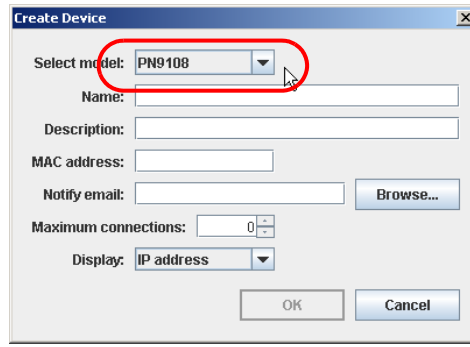
Adding Devices Manually:

To manually add a device, do the following:

1. Right click on the folder that you want to add the new device to.
2. In the pop-up menu that appears, select New → Device.



3. In the dialog box that appears, drop down the *Select Model* list and select the device type that you want to add:



Note: In this example we are adding a PN9108. The procedure for adding other devices is the same.

4. Enter a name, description, and MAC address for the device in the appropriate fields.
5. Enter an email address for the person that the device will send messages to when events (such as SNMP traps) occur, in the *Notify email* field.

Note: 1. This step is optional.

2. You can use the *Browse* button to select the address from a list of users rather than inputting the address manually.

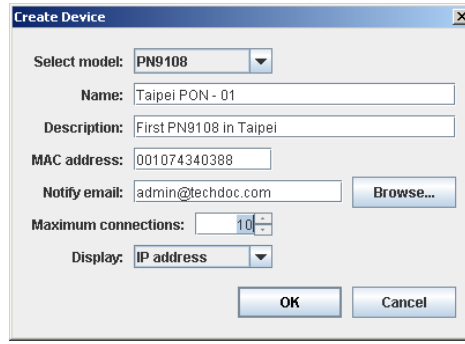
6. Specify the maximum number of simultaneous connections to the device that you want CC1000J to allow.

Note: 1. A number of 0 (zero) means unlimited connections (up to the maximum number of connections set in the device, itself).

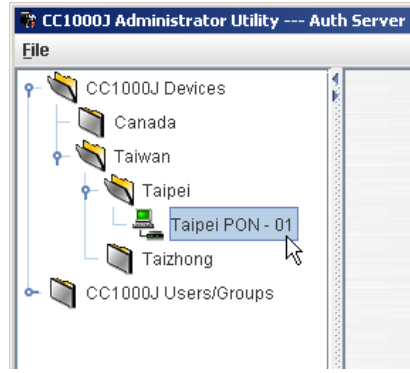
2. If the number specified here is greater than number of connections allowed by the device itself, the number allowed by the device takes precedence over this number. More connections than the ones allowed by the device will not be accepted.

7. Choose whether to display the device's name or IP address when users log into the CC1000J via their browsers. For security, selecting the device's name keeps its IP address from being visible under the *Operation Notes* in the main panel when the device's information displays in a browser.

When your settings have been made, the dialog box should resemble the example below:



8. Click **OK** to finish. The new device is created in its device folder:



Note: When you create the device, its *Properties* screen appears. Ignore this for the time being. A complete discussion of how to configure the screen entries is given on page 44

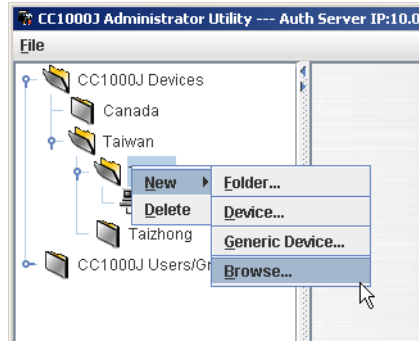
Adding Devices by browsing:

Browsing is the most convenient way to add devices, since most of the device information is automatically inserted, rather than having to be keyed in.

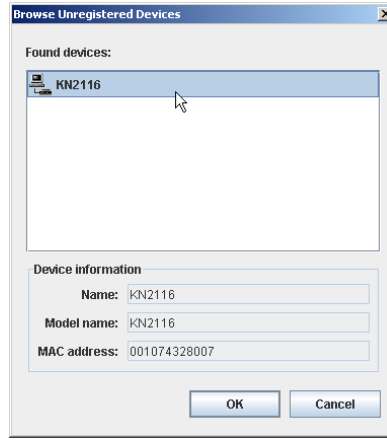
Note: Devices to be added by browsing must be powered on and have CC management enabled and configured in their settings.

To add a device by browsing, do the following:

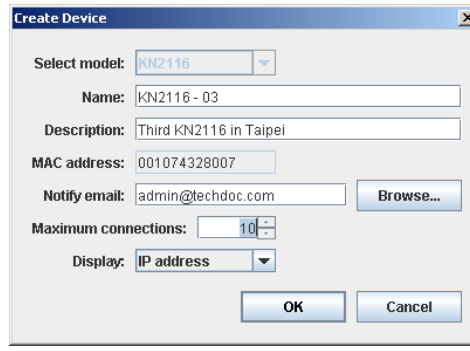
1. Right click on the folder that you want to add the new device to.
2. In the popup menu that appears, select New → Browse:



3. In the *Browse Unregistered Devices* dialog box that appears, select the device you want to add from the *Found devices* list, then click **OK**.



4. In the dialog box that appears, the *Name* and *MAC address* fields are already filled in.



5. Give the device a more descriptive name, and fill in the *Description* field, if you like.
6. Enter an email address for the person that the device will send messages to when important events (such as SNMP traps) occur on it in the *Notify email* field

---

Note: 1. This step is optional.

2. You can use the *Browse* button to select the address from a list of users rather than inputting the address manually.

---

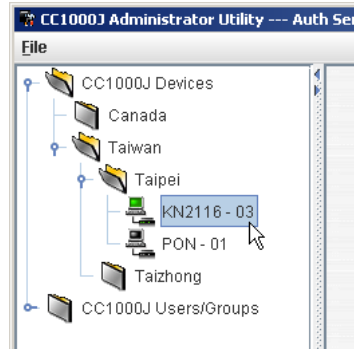
7. Specify the maximum number of simultaneous connections to the device that you want CC1000J to allow.

Note: If the number specified here is greater than number of connections allowed by the device itself, the number allowed by the device takes precedence over this number. More connections than the ones allowed by the device will not be accepted.

---

8. Choose whether to display the device's name or IP address under the *Operation Notes* in the main panel when users log into the CC1000J via their browsers.

9. Click **OK** to finish up. The device is added to the folder:



Note: When you create the device, its *Properties* screen appears. Ignore this for the time being. A complete discussion of how to configure the screen entries is given on page 44

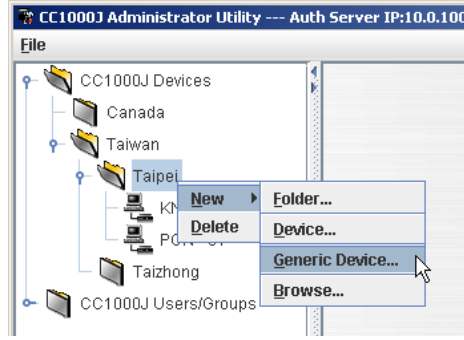
Adding Generic Devices:

The CC1000J supports the creation of a *Generic* device type. This refers to a device that is not part of the Aten / Altusen *On the Net™ / Over the Net™* line of products.

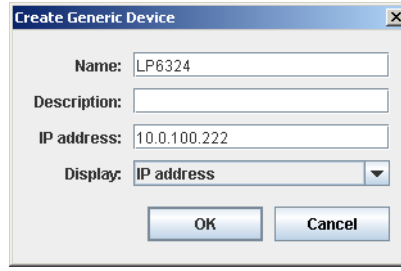
Generic devices have no provision for CC management support and, therefore, cannot be added by browsing, or be authenticated through the CC1000J. You must log in to them with their own Username/Password authentication procedure. In addition, they must be capable of browser-based access.

To add a generic device, do the following:

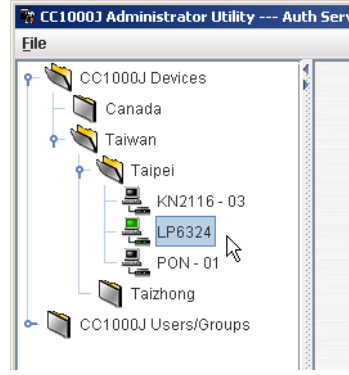
1. Right click on the device folder that you want to add the new device to.
2. In the popup menu that appears, select New → Generic Device:



3. In the dialog box that appears, key in a name, description (optional) and IP address for the device:



4. Choose whether to display the device's name or IP address under the *Operation Notes* in the main panel when users log into the CC1000J via their browsers.
5. Click **OK** to finish up. The device is added to the folder:

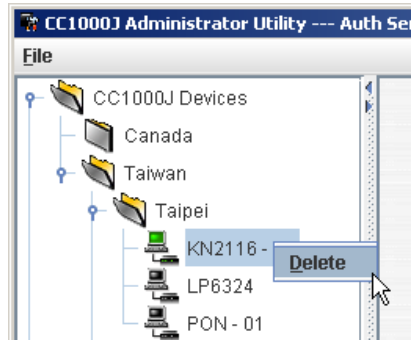


Note: When you create the device, its *Properties* screen appears. The screen displays the device's information, and is used to configure User and Group permissions for the device. You can ignore it for the time being. Configuration of Users, Groups, and Devices is discussed in the sections that follow.

Deleting Devices

With the exception of the *CC1000J Devices* root folder, all folders and devices can be deleted by doing the following:

1. Right click on the item you want to delete.
2. In the pop-up menu that appears, select *Delete*.



Note: When you delete a folder, all subfolders and devices contained in it are also deleted.

Moving Folders/Devices

Folders and devices can be moved to other folders by dragging and dropping.

Device Properties

A device's *Properties* screen displays the device's information, and is used to configure User and Group permissions for the device (see *Device Properties Configuration*, page 44). You can view it and make changes to its information and permission configuration by selecting it in the tree list.

User Management

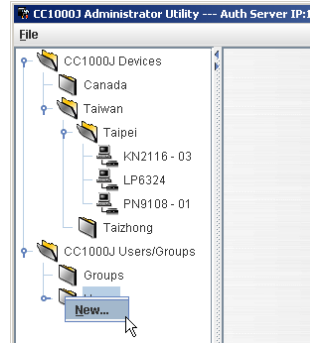
The CC1000J Administrator Utility allows administrators to add, delete and modify users and user attributes.

Note: The Administrator Utility comes with a pre installed *superadmin* (super administrator) account. The Username for this account is *superadmin*; the password is *CC1KPassword*. The password is case sensitive. For security purposes, we strongly recommend changing the password to something unique.

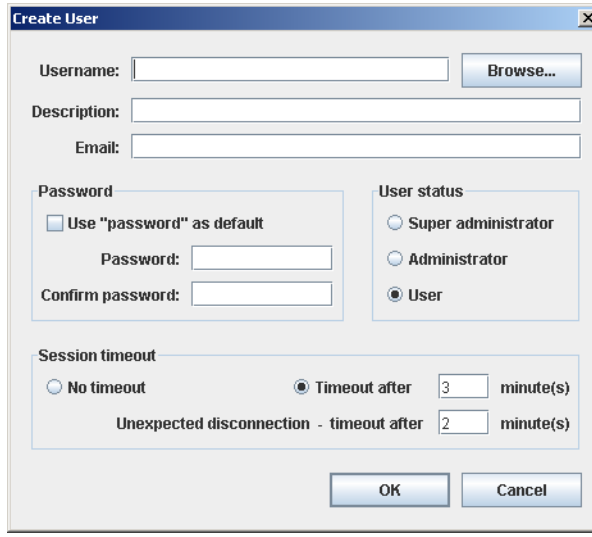
Adding Users

To add a user, do the following:

1. Expand the *CC1000J Users/Groups* folder.
2. Right click on the *Users* folder. In the pop up menu that appears, click **New**:



3. The *Create User* dialog box appears.



Enter the required information in the appropriate fields.

A description of each of the items is given in the table below:

Field	Description
Username	Enter a username here.
Description	Additional user information you may wish to include.
Browse	For installations that make use of Windows Active Directory, the information for the *Username* and *Description* fields can be filled in automatically by clicking Browse and selecting the user from a list of users registered in AD.
Email	The user's email address. If the email address is entered here, it will show up in a device's *Notify email* list.
Use "password" as default password	Selecting this sets "password" as the user's password.
Password	You must set the password unless you select *Use "password" as default*.
Confirm password	To be sure there is no mistake in the password you are asked to enter it again. The two entries must exactly match.

(Continues on next page.)

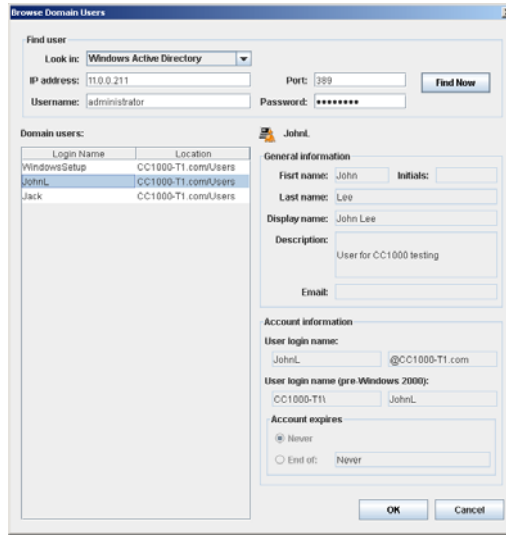
(Continued from previous page.)

Field	Description
User status	There are three categories: Super Administrator, Administrator and User (see *User Type Options*, page 39). There is no limitation on the number of accounts that can be created in each category. **Note:** 1. The Super Administrator is not allowed to access devices from a browser login to the CC1000J. 2. If the User status you want to choose is already selected, click it again to bring up its *User Type Options* dialog box.
Session timeout	1. If there is no online device connected to the CC1000J, and there is no operator input for the amount of time specified here, the CC1000J session is ended. The Super Administrator timeout interval is from 1–1440 minutes; default is 3 minutes. The timeout interval for Administrators and Users can either be 1–1440 minutes or no timeout; default is 3 minutes. 2. If an operator is connected to a device and that device has its own timeout interval, the CC1000 timeout interval won't begin until the operator is first timed out of the device session.
Unexpected disconnection timeout	If the user unexpectedly disconnects (i.e. closes the browser), the CC1000J times out the user's session after the amount of time specified here. The timeout interval is from 2 - 10 minutes; default is 2 minutes.

(Continues on next page.)

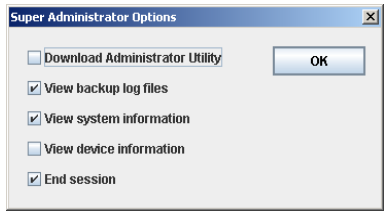
(Continued from previous page.)

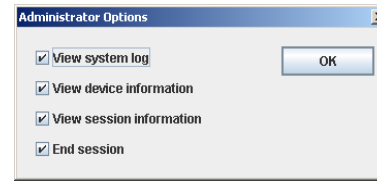
Note: If you click the Browse button (see *Browse*, page 36), to add the Username and Description, a *Browse Domain Users* input screen appears:



1. Specify the AD Server's IP address and port.
2. Provide a valid Username and Password for the AD Server.
3. Click **Find Now** to generate a list of users in the *Domain Users* column.
4. Select the user in the *Domain Users* column. The user's information displays in the fields to the right of the column.
5. Click **OK**

4. Click one of the *User Status* options that is appropriate for the User. Depending on your choice, one of the following dialog boxes appears.





A description of the options is given in the table, below:

Option	Description
Download Administrator Utility	This option allows a Super Administrator to download the Administrator Utility executable file from the CC1000J Servers site. The Administrator Utility can run as an independent module on Windows (2000 and higher) and most Linux systems.
View backup log files	Selecting this option allows the Super Administrator to view and query the backup log files.
View system information	Selecting this option allows the Super Administrator to view system information – such as the number of Licenses and Connections available to the system.
View device information	Selecting this option allows the Super Administrator to view information for all online devices on the installation. Administrators can view information for the online devices that they have access rights to.
End session	Selecting this option allows the Super Administrator to end Administrator and User CC1000J sessions. Administrators can end User CC1000J sessions.

(Continues on next page.)

(Continued from previous page.)

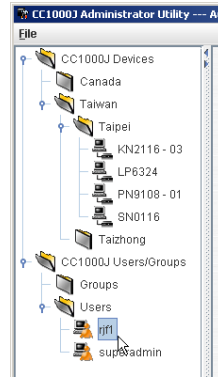
Option	Description
View system log	Selecting this option allows the Super Administrator or Administrator to view and query the system log files.
View session information	Selecting this option allows the Super Administrator, Administrator, or User to see information regarding the sessions currently taking place online.
View device log	Selecting this option allows the Super Administrator, Administrator, or User to view and query the device logs for the devices they have access rights to.

Note: 1. *View system log*, *View session information*, and *View device log* are the defaults for the Super Administrator; *View device log* is the default for Administrators.

2. See *Main Page Links*, page 65 for screenshots and more details regarding these selections.

5. Place a check in the boxes to enable the options that you want to allow, then click **OK**.

6. When you return to the *Create User* dialog box, click **OK**. The new user is added to the *Users* folder.

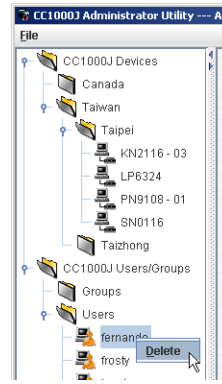


7. Repeat steps 2–6 for each new user you want to add.

Deleting Users

To delete a user, do the following:

1. Navigate to the *Users* folder (CC1000J Users/Groups → Users) and right click on the username.
2. Click **Delete**.



User Properties

User accounts and permissions are managed through the *User Properties* screen. See *User Properties Configuration*, page 47, for details.

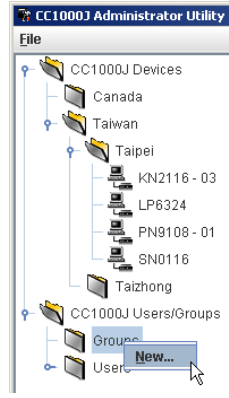
Group Management

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 those devices.

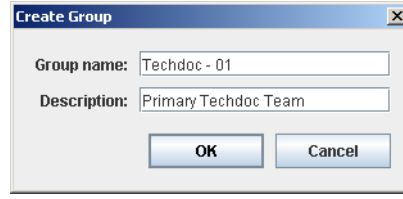
Creating Groups

To create a group, do the following:

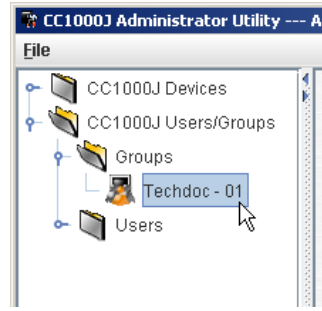
1. Expand the *CC1000J Users/Groups* folder.
2. Right click on the *Groups*.
3. In the pop up menu that appears, choose **New**.



4. In the *Create Group* dialog box that appears, enter a group name and description, then click **OK**.



5. The new group is added to the *Groups* folder:



Deleting Groups

To delete a group, do the following:

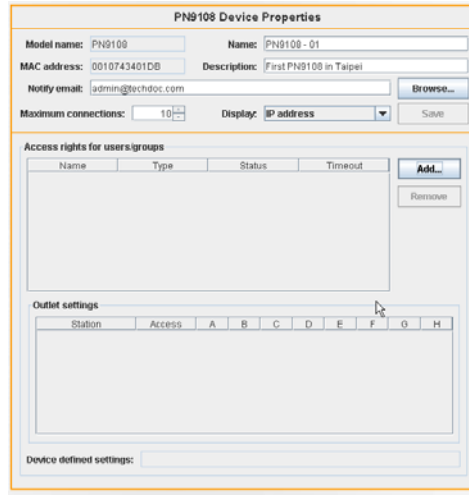
1. Navigate to the *Groups* folder (CC1000J Users/Groups → Groups) and right click on the Group's name.
2. Click **Delete**.

Group Properties

User accounts and permissions are managed through the *Group Properties* screen. See *Group Properties Configuration*, page 52, for details.

Device Properties Configuration

User access and permissions for particular devices are configured through the device's *Device Properties* screen. To bring up a device's screen, navigate to the folder that the device resides in and click on its name. A screen, similar to the one below, appears:



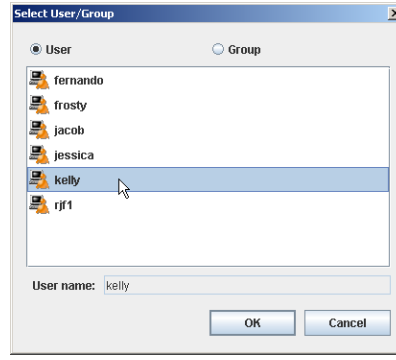
The screen is divided into three major areas:

- The top contains information about the device that was specified when the device was created (see *Adding Devices*, page 27).
- The middle panel lets you add the users and groups that will have access rights to the device.
- The bottom panel lets you specify the access rights for each user and group.

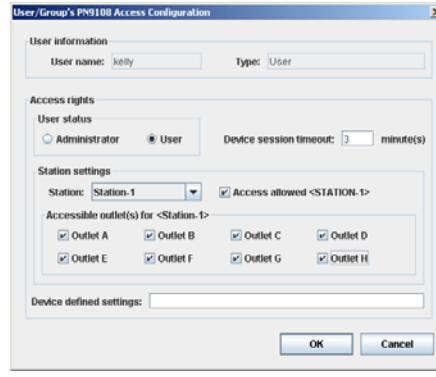
Adding Users / Groups to Devices

To add a user or group to the device's access list, do the following:

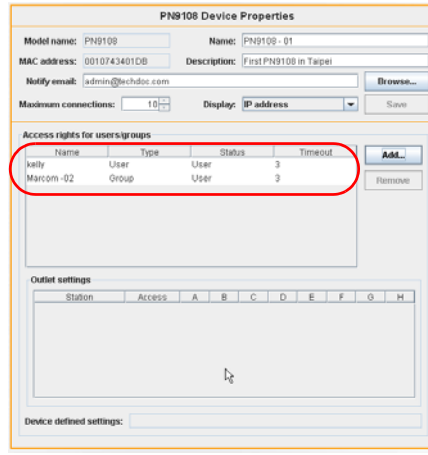
1. Click the *Add* button at the right of the middle panel.
2. In the dialog box that appears:
   a) Click one of the radio buttons to select whether you are adding a User or a Group
   b) Select the User or Group to be added
   c) Click OK



3. The permissions dialog box comes up. Set the permissions according to the information contained in the device's User Manual, then click **OK**.



4. When you return to the *Device Properties* screen the Users and Groups that you added appear in the middle panel.

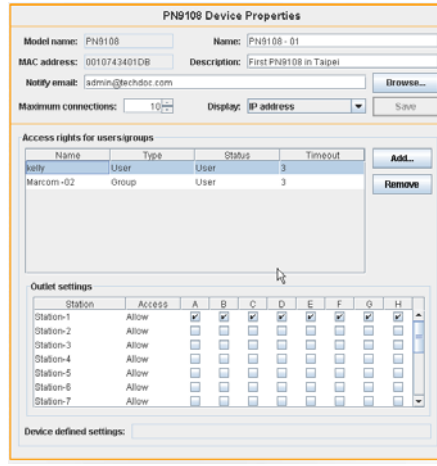


Removing Users / Groups from Devices

To remove a User / Group from a device's access list, select the User or Group from the list, then click **Remove**.

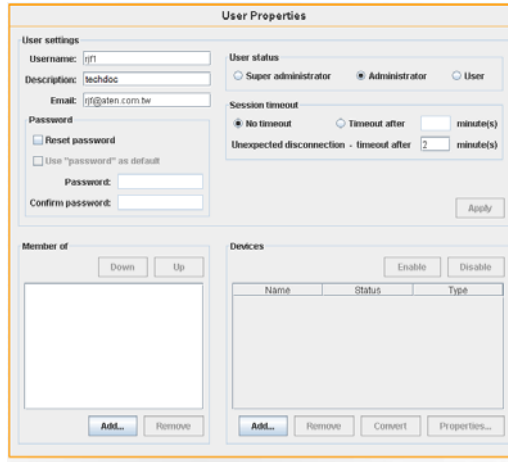
Viewing / Editing User / Group Device Permissions

To view or edit the permissions for a User or Group, click on the name in the middle panel. The information appears in the bottom panel. Make any necessary changes, then click **OK**.



User Properties Configuration

User accounts are configured through the *User Properties* screen. To bring up the screen, open the *Users* folder (CC1000J Users/Groups → Users) and click on the user's name. The *User Properties* screen appears.



The screen is divided into three major areas:

- The top contains information about the user that was specified when the user was created (see *Adding Users*, page 35), as well as an area to reset or change a user's password (see *Resetting Passwords:*, below).
- The *Member of* panel lets you add the user to a group. See *Adding Users to Groups*, page 52 for details.
- The *Devices* panel lets you assign devices to the user. See *Adding Devices to Users*, page 49 for details.

> **Note:** Users and Groups can also be added to devices from the *Device Properties Configuration* screen. See *Adding Users / Groups to Devices*, page 45

Resetting Passwords:

To reset a user's password, do the following:

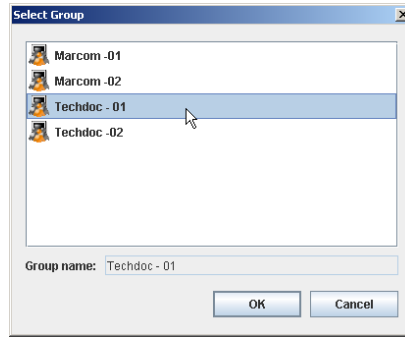
1. Check **Reset password**. This enables the *Password* fields.
2. Enter the new password; then enter it again to confirm it.
3. Click **Apply** to finish.

Users and Groups

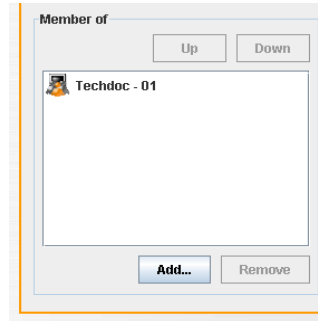
Adding a User to a Group

To add a user to a group, do the following:

1. Click the Add button at the bottom of the *Member of* panel.
2. In the dialog box that appears, select the group that you want the user to be a member of, then click **OK**.

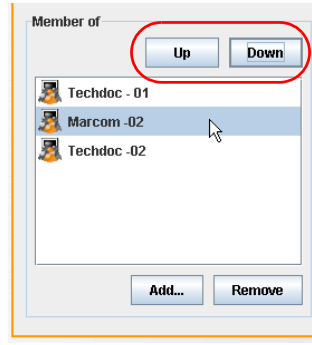


3. When you return to the *User Properties* screen, the group can be seen in the *Member of* list:



Group Priority

If the user is a member of more than one group, you can adjust a group's priority by selecting and then clicking **Up** or **Down** to move it accordingly:



Removing Users From Groups

To remove a user from a group, select the group from the *Member of* list, then click **Remove**.

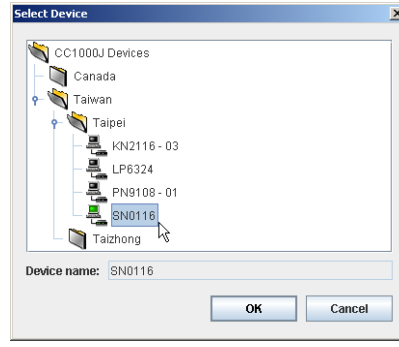
Users and Devices

Adding Devices to Users

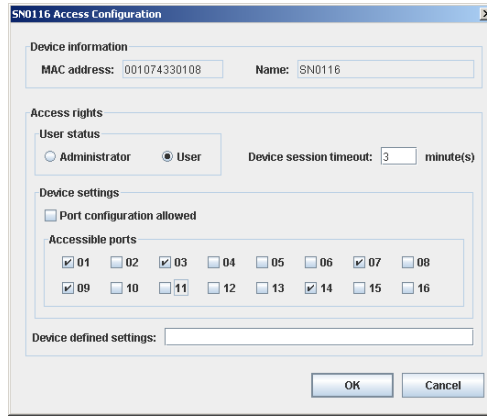
To add a device for the user to access, do the following:

1. Click the Add button at the bottom of the *Devices* panel.
2. In the dialog box that appears, select the device, then click **OK**.

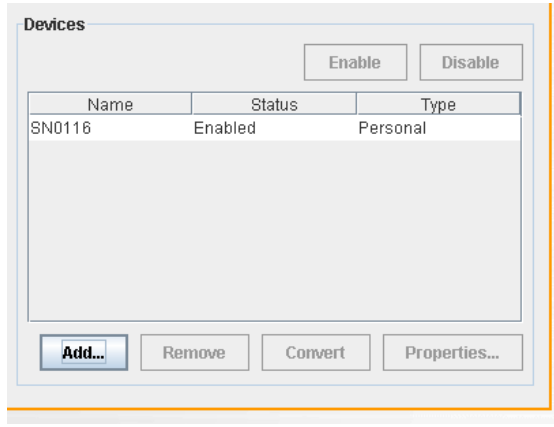
> **Note:** You may have to expand the folders to get to the device.



3. The *Access Configuration* dialog box comes up. Set the permissions according to the information contained in the device's User Manual, then click **OK**.



4. When you return to the *User Properties* screen the device that you selected appears in the *Devices* panel.



Device Panel Headings

The headings at the top of the Device panel are described in the table, below:.

Heading	Description
Name	Lists the name of the device.
Status	Indicates whether the device is set as enabled or disabled. If it is set as enabled, it shows up in the user's tree view. If it is set as disabled, it doesn't show up in the user's tree view – even though it is on line. The administrator can use this function to temporarily deny a user access to a device without having to delete it and then reinstall it.
Type	Indicates whether the device is accessed privately or as part of a group.

Device Button Functions

The functions of the buttons associated with the panel are described in the table, below:

Heading	Description
Enable	Highlight a device in the list box and click **Enable**, to allow the user to access the device. This function only works for devices that are accessed privately.
Disable	Highlight a device in the list and click **Disable**, to disable user access to the device. This function only works for devices that are accessed privately.
Add	Allows the administrator to add devices to the list of devices that a user can access.
Remove	Highlight a device and click **Remove**, to remove a device from the list. This function cannot be used to remove a device that the user accesses through a group.
Convert	This function converts a device that is accessed through a group to device that is personal to the user. To convert a *group* device in the list to a *personal* one, select it and click **Convert**. The status of the new, personal, device is **Enabled**; the status of the old group device is now **Disabled**. If the private device is removed, however, the status of the original group device automatically reverts to being **Enabled**. **Note:** A personal device cannot be converted to a group device.
Properties	To view and change device properties, select the device and click **Properties**, or double click the device. **Note:** Properties of devices belonging to groups can only be viewed, not changed.

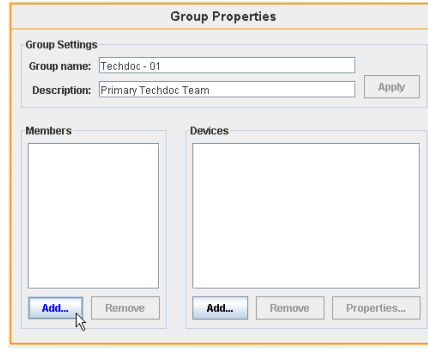
Group Properties Configuration

Groups are managed through their Group Properties screen. To bring up the screen, navigate to the *Groups* folder (CC1000J Users/Groups → Groups), and click on the name of the group. A screen, similar to the one below, appears:

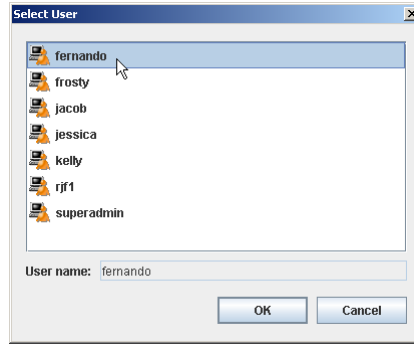
Adding Users to Groups

To add a user to a group, do the following:

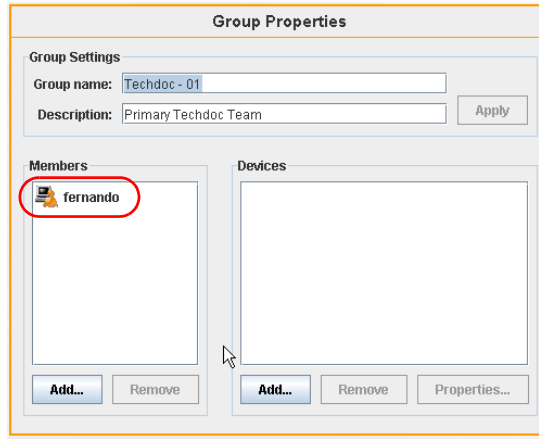
1. Navigate to the group folder that you want to add a user to, and click on the name of the group.
2. In the *Group Properties* screen that appears, go to the bottom of the *Members* panel and click **Add**.



3. In the *Select User* dialog box that appears, select the user you want to add to the group from the list of users.



4. Click **OK**. The user is added to the group's *Members* list.



5. Click **Exit** to close the screen.

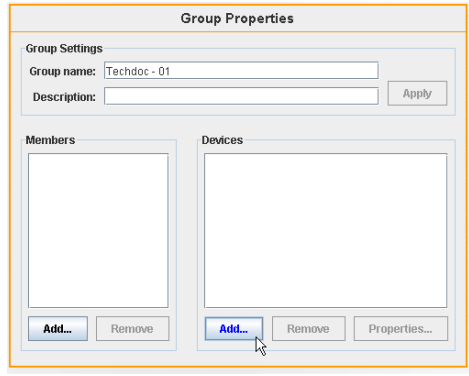
Removing Users from Groups:

To remove a user from a group, select the group in the *Member of* panel, then click **Remove**.

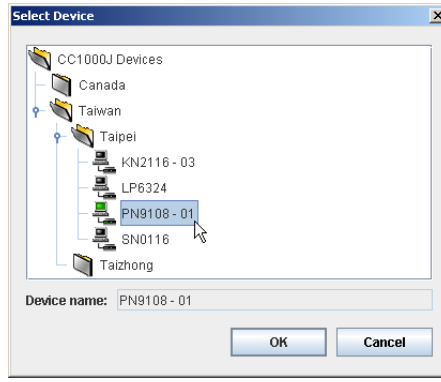
Adding Devices to Groups

To add a device to a group, do the following:

1. Navigate to the group folder that you want to add a device to, and click on the name of the group.
2. In the *Group Properties* screen that appears, go to the bottom of the *Devices* panel and click **Add**.

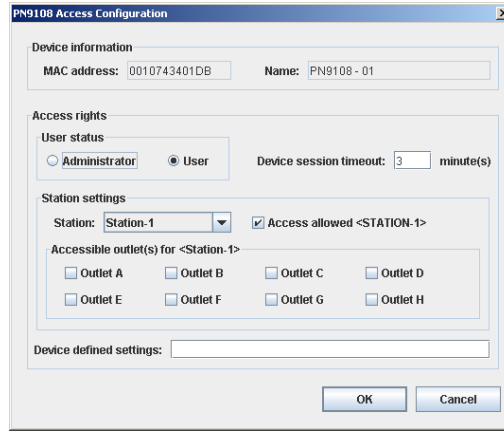


3. Select the device that you want to add to the group.

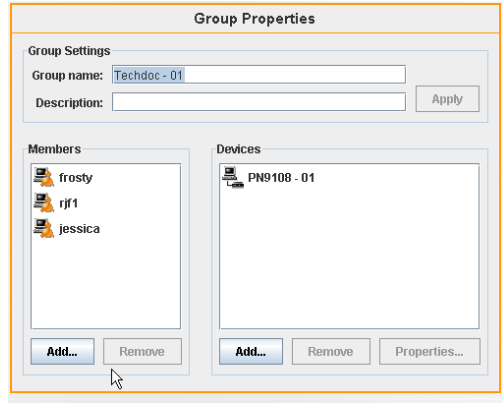


4. Click **OK**.

5. In the *Access Configuration* dialog box that appears, set the permissions according to the information contained in the device's User Manual, then click **OK**.



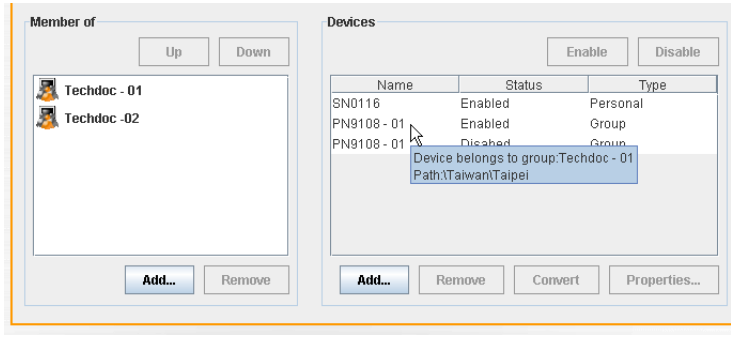
6. When you return to the *Group Properties* screen the device that you selected appears in the *Devices* panel.



Device Conflict

If a user is a member of more than one group and each group has access to the same device, the device's name will appear more than once in the *Devices* panel of the user's *Properties* screen. Only the first entry of the device is enabled, however. Users are only able to access the device from the group that the first instance of the device is pointing to.

To ascertain which group a device is pointing to, hover the mouse pointer over the device's name in the *Devices* list. The balloon that appears displays which group (if any), the device points to – as shown in the screen, below.



In order for a user to access the device, the group that it points to must have first priority. The group at the top of the *Member of* list has the highest priority. To change a group's priority, see *Group Priority*, page 49.

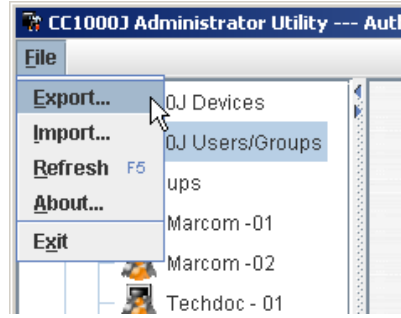
Export / Import Configurations

The Administrator Utility can export CC1000J user and device configurations to a file. It can also import CC1000J user and device configurations from previously generated configuration files.

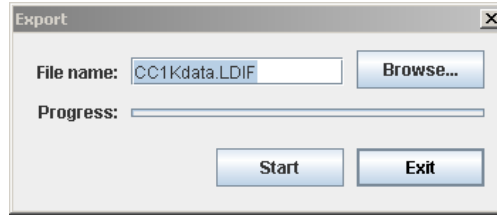
Exporting Configurations

To export configurations to a file, do the following:

1. From the *File* menu, choose **Export**.



The *Export* dialog box appears:



2. Click **Start**. The configurations are exported to the specified file.

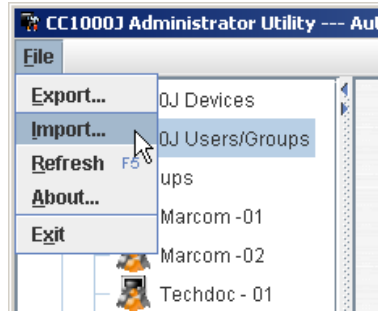
Note: 1. You can change the default filename if you wish.

2. By default, the file is saved in the *\CC1000Java\CC1000J-App* folder, but you can key in, or browse, to a different folder.

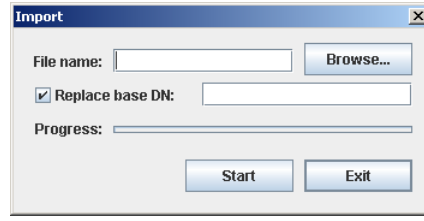
Importing Configurations

To import configurations from a file, do the following:

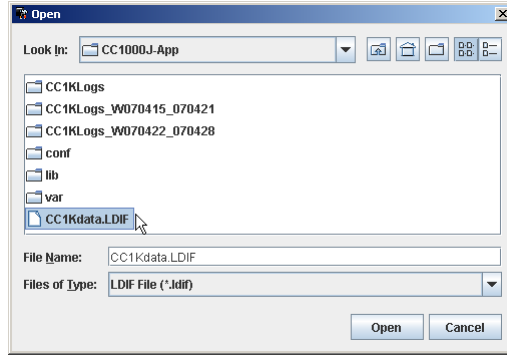
1. From the *File* menu, choose **Import**.



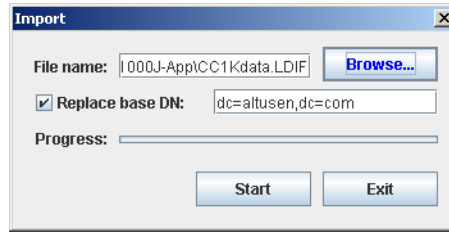
The *Import Directory* dialog box appears.



2. Key in, or browse to, the path and filename where the import file is located.



3. When you come back to the dialog box, it looks similar to the one, below:



   If the file was originally exported by the Administration Utility, its DN (Distinguished Name) configuration data appears in the text box to the right of the *Replace base DN* entry.

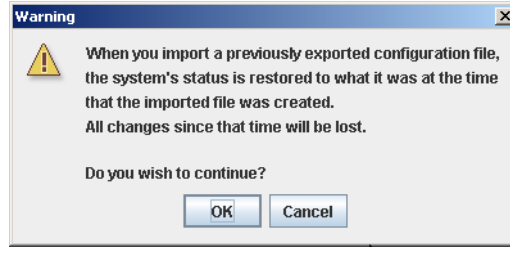
4. Choose whether to enable or disable the *Replace base DN* entry.
   - By default, the *Replace base DN* checkbox is enabled. That means that the import file's DN configuration data (the entries in the text box to its right), will be replaced by the LDAP DN configuration.

     If you are importing a file that was not created by exporting it from this Administrator Utility (running on this computer), you must key in this computer's DN configuration in the text box.

   - If the *Replace base DN* checkbox is not enabled, only the data in the import file that matches the CC Authentication Server DN will be imported.

5. Click **Start**.

   A cautionary message appears:



6. Click **OK** to import the configuration file's information; click Cancel to abort the operation.

After the file is successfully imported, a message appears on screen to inform you of the fact.

This Page Intentionally Left Blank

Chapter 5
CC1000J Browser Operation

Devices on a CC1000J installation are accessed from a browser based GUI. Only a single login to the CC1000J Server is required to access any of them. An expandable tree view lets you locate and access any device on the entire installation - no matter where in the world - with just a few clicks of the mouse.

Logging In

To log into the CC1000J, do the following:

1. Open the browser and specify the IP address of the CC1000J in the browser's URL location bar.

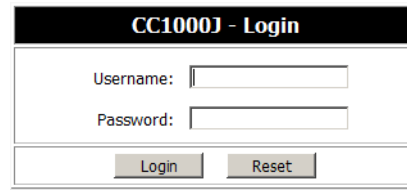
Note: 1. You must include **http://** or **https://** before the IP address, and you must specify the http or https port that the CC1000J listens on when you enter its URL in your browser. For example:

```
http://192.168.0.30:8080
https://192.168.0.30:8443
```

2. The http and https ports are set in the *Apache Tomcat* panel of the CC1000J Manager's *System* tab (see *The System Tab*, page 20).

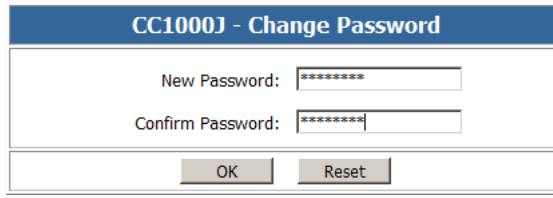
---

2. When the Security Alert dialog box appears, accept the certificate. The Login page appears:



3. Provide your CC1000J Username and Password, then click **Login**.

4. If this is the first time you are logging in, or your password was reset, a dialog box comes up for you to set up your password again. Reenter and confirm your password. You can keep your original password if you like.



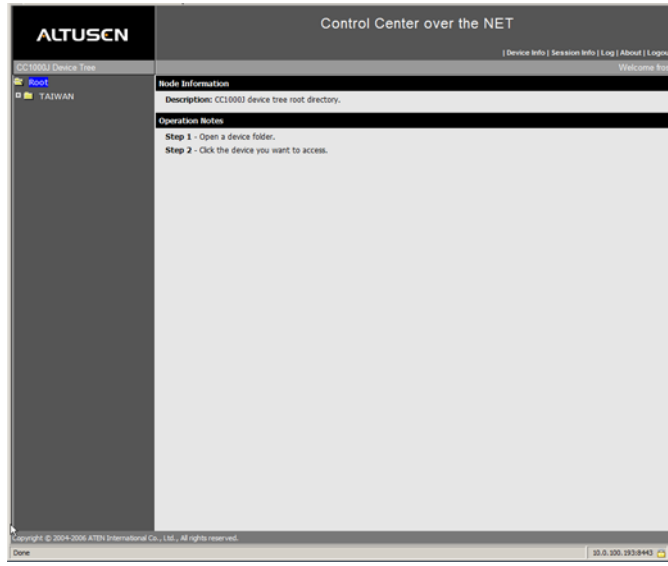
Note: 1. The CC1000J provides a limited number of login licenses. If no licenses are available, a window informing you that there are no more licenses available appears instead of the login screen.

2. If a message saying that the CC1000J *Service is not available*, make sure that the CC1000J Manager is running and that its settings are correct.

3. The CC1000J supports multiple logins for Administrators and Users; Super Administrators are restricted to a single login.

Main Page Layout

After you have successfully logged in, the CC1000J Main Web Page appears:

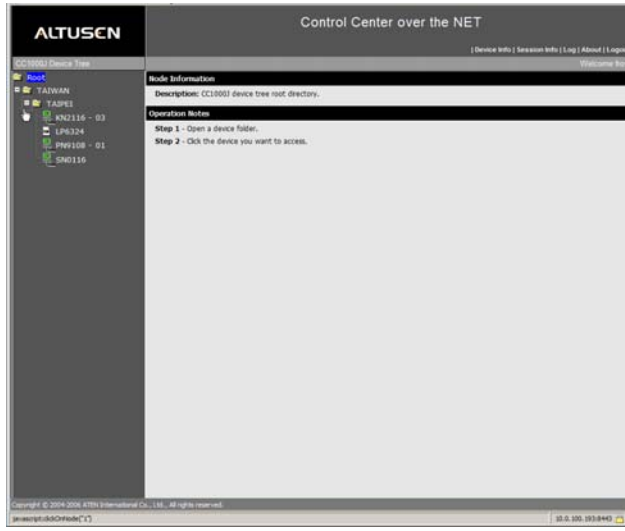


The CC1000J Main Page is divided into three major sections: a left panel; a right panel; and a row of links at the top-right.

- The left panel displays a tree view of all the device folders on the installation that the user is authorized to access. The Tree View is discussed in the next section.
- The main panel provides information about the item in the Device Tree that is currently selected.
- Clicking a link on the row at the top-right, brings up additional screens. The number and type of links displayed, are determined by the user's type (Super Administrator, Administrator, User) and the options selected when the user was created. The links are discussed under *Main Page Links*, page 65.

Tree View

- Only devices the user is authorized to access are listed in the Tree View (See *Adding Users / Groups to Devices*, page 45 for details.)
- A plus sign (+) in front of a folder means that there are items nested inside of it. Click the plus sign to expand the tree and show the nested items.
- To access a device, navigate through the folders to select it. A screen similar to the one below appears:



- If the device is on line, its icon lights green, and its IP address or device name appears under the *Operation Notes* heading in the main panel when you select it.
- Usually, there are two choices available to access a device:
  - Accessing it directly and logging in manually
  - Accessing it via the CC1000J – which doesn't require another log in.

  If the device cannot be accessed directly, however, only the CC1000J access method appears.
- Click the IP address or device name to bring up a new browser window with the device's web page displayed.

Note: The device must be configured to operate with the CC1000J, or its status will be displayed as *Off Line*. Refer to the device's User Manual for information on how to configure and operate it.

Main Page Links

Overview

Clicking the links at the top-right of the main page brings up additional screens. The number and type of links displayed, are determined by the user's type (Super Administrator, Administrator, User) and the options selected when the user was created.

The table below shows the relation between the User Type and link type:

Link	Accessible By	Access
Download	Super Administrator	Optional
System Info	Super Administrator	Optional
Device Info	Super Administrator	Optional
	Administrator	Optional
Session Info	Super Administrator	Default
	Administrator	Optional
	User	Optional
Log (System)	Super Administrator	Default
	Administrator	Optional
Log (Device)	Super Administrator	Default
	Administrator	Default
	User	Optional
Log (Backup)	Super Administrator	Optional
About	All	Default
Logout	All	Default

- If a link is designated as *Default*, it always appears on the web page.
- If a link is designated as *Optional*, it only appears if it has been selected as an option in the user's configuration.
- For further details regarding configuration of User Types, see *User Management*, page 35.

Each link is explained in the sections that follow.

Download

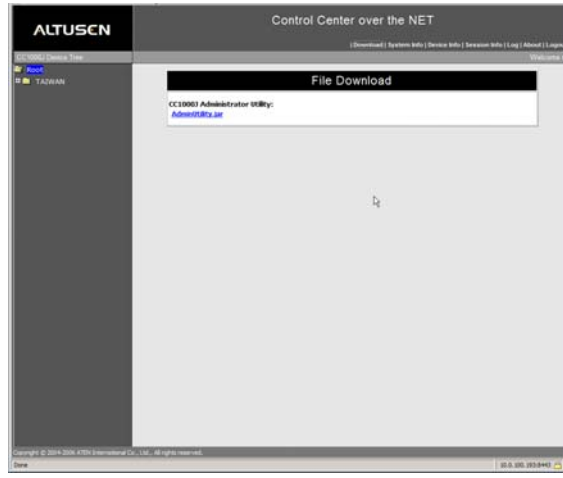
Download provides a way for the Super Administrator to download the Administrator Utility executable file from the CC1000J Web Server – thereby allowing the Super Administrator to manage the CC1000J from anywhere on the Internet.

Note: 1. The Administrator Utility runs on most Linux systems. For Windows systems, you must use Windows 2000 or higher.

2. Java 1.5 or higher must be installed on the computer that will run the Administrator Utility.

To download and run the Administrator Utility, do the following:

1. Click the **Download** link. The following screen appears:

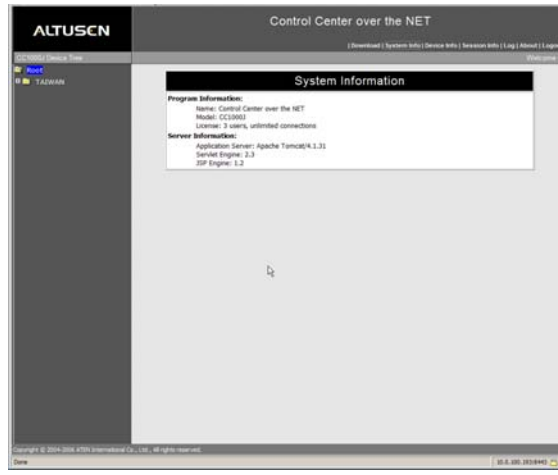


2. Click the *CC1KAdmin.jar* link.
3. When the confirmation screen comes up, click **Save**.
4. In the dialog box that comes up, pick a location on your computer to save the file to.
5. To run the program, navigate to the directory where it resides, and double click the program icon. See Chapter 4, *The CC1000J Administrator Utility* for details on using the program.

Note: Only users who have been authorized in LDAP (see *LDAP:*, page 21), will be able to log in.

System Info

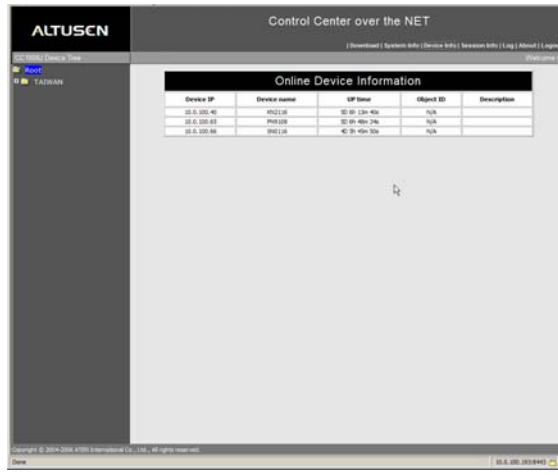
When the Super Administrator clicks the *System Info* link, a screen, similar to the following appears:



System Info shows system information – such as the number of Licenses and Connections available to the system.

Device Info

When the Super Administrator or Administrator clicks the *Device Info* link, a screen, similar to the following appears:

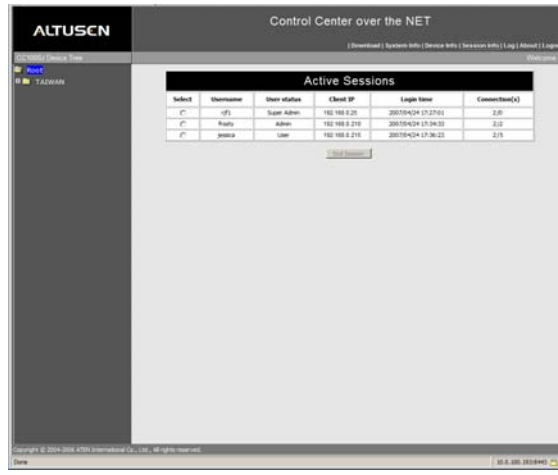


The screen provides information regarding all online devices.

- The *Object ID* entry represents the SNMP related OID (Object Identifier). If the device doesn't support SNMP, **N/A** will appear in this field.
- *UP Time* refers to the amount of time the device has been powered on (up).

Session Info

Session Info provides information regarding online active sessions. When you click the *Session Info* link, a screen, similar to the following appears :



- The Super Administrator can end any Administrator or User session by selecting the desired Username and clicking **End Session**.
- The numbers under the *Connections* heading represent the number of connections to installed devices and the number of subconnections to them.

  For example, if the entry under the heading were 2/5, it would mean that the user was connected to two devices through the CC1000J, and that there were a total of five connections under those devices (the subconnections).

Log

When you click the *Log* link, a screen, similar to the one below appears:

To query a log record, do the following:

1. Click the arrow at the right of the *Log File* field to drop down a list of available log files. Only the log files that you have rights to view are available.

   Note: If you have rights to query the system log, it will appear in the list.

2. Select the items that you want to perform a query on in the *Target List*, and add them to the *Selected Targets* list. If you are searching on more than one item, the order of the search will follow the order of your selection.

   Note: If you have rights to query backup log records, you may need to select the main log file in the *Log File Select* field in order to have the backup log file appear in the Target List.

3. If you want to search on a keyword, enter it in the *Keywords* field – otherwise leave the field blank.

   Note: The keyword can be a single word, a phrase, or even a sentence.

(Continues on next page.)

(Continued from previous page.)

4. In the *Time* panel, if you want to search the entire record regardless of the time frame, select *All*.

   If you want to search a particular time range, click the calendar icons at the right of the *Start* and *End* fields to bring up a dialog box to choose the dates and times for the search, then choose whether the search will *include* or *exclude* the date/time range.

5. When all your choices have been made, click **OK** to perform the search.

About

The About page provides information regarding the current version of the CC1000J.

Logout

Clicking this button logs you out of your CC1000J session.

This Page Intentionally Left Blank

Chapter 6
CC1000 Installation Overview

System Requirements

The requirements for the computers running the CC1000 components under the Windows-based configuration are given in the table below:

Component	PC Requirements
CC1000 Server	◆ Windows Server Family[1] with IIS 5.0/6.0 and higher; Certificate Services (CA)[2], and SNMP configured ◆ At least one network card installed - two are recommended ◆ A USB host controller and USB Type A (F) port installed so that it can accept the CC1000 USB Authentication Key
CC1000 Log Server	Windows 2000 / XP / or Windows Server Family[1] with Microsoft Jet Database **Note:** This component can either be installed on a PC running one of the other components, or on an independent PC.
CC1000 Authenticaton Server	Windows Server Family[1] with Active Directory (AD); and Certificate Services (CA) configured **Note:** This component can either be installed on the PC that the CC1000 Manager is on, or on an independent PC.
CC1000 Administrator Utility	Windows 2000 / XP / or Windows Server Family[1] **Note:** This component can either be installed on a PC running one of the other components, or on an independent PC.

Note: 1. For the *Windows Server Family* you can use any of the following Windows operating systems: Windows 2000 Server, Windows 2000 Advanced Server, Windows 2000 Data Center, Windows Server 2003 Standard Edition, Windows Server 2003 Small Business Edition, or Windows Server 2003 Enterprise Edition.

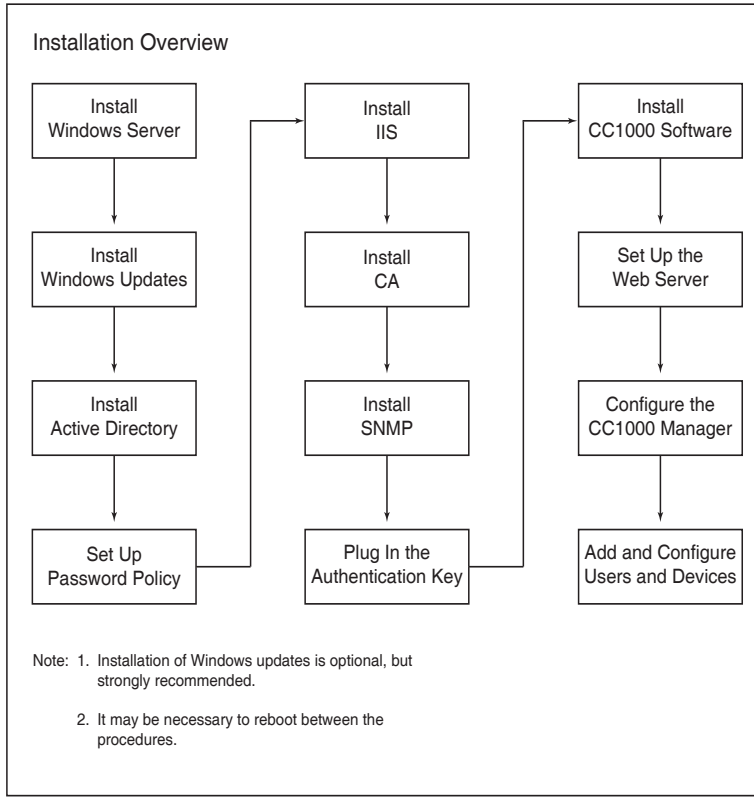
2. All PCs must be have all of the latest updates from the Microsoft Update Website installed.

3. All ALTUSEN/ATEN 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.

Installation and Operation Overview

The procedures involved in setting up and operating a CC1000 system are explained in detail in the chapters of this manual. The diagram and descriptions below offer a brief overview of the steps you will perform.

Installation



1. Install and set up Windows Server; making sure to install AD (Active Directory), IIS (Internet Information Services), and CA (Certification Authority). This is described in Chapter 7, *Authentication Server Setup*.
2. Install and set up the CC1000 Server software - making sure that IIS and SNMP have been properly configured, and that the USB Authentication Key has been plugged into the computer running the CC1000 Server software. This is described in Chapter 8, *CC1000 Server Setup*.

3. Launch the CC1000 Log Server. Configuration of the Log Server must be performed the first time that the program is launched. This is described in Chapter 9, *The Log Server*.

   Note: If the Log Server is installed on the same machine as the CC1000 Manager, you don't have to launch the Log Server. It will launch automatically when you launch the CC1000 Manager.

4. Launch the CC1000 Manager. Configuration of the CC1000 Manager must be performed the first time that the program is launched. This is described in Chapter 10, *The CC1000 Manager*.

5. Launch the CC1000 Administrator Utility to add and configure devices and users. These procedures must be performed the first time the program is launched, and whenever device or user information changes. This is described in Chapter 11, *The Administrator Utility*.

   Note: Make sure that ANMS (Authentication Network Management Service) support has been properly set up in your ALTUSEN/ATEN IP devices. See the User Manuals for those devices for details.

Operation

To operate the CC1000:

1. Open your browser and key the CC1000's IP address into the URL field.
2. Accept the certificates that appear.
3. Log in with your Username and Password.

   This is described in Chapter 12, *Browser Operation*.

Upgrading the CC1000

If CC1000J has already been installed, it is not necessary to perform a full install. You can upgrade to the latest CC1000 version by running the CC1000 upgrade program: *CC1000SWUpgrade.exe*

The file can be found in the *CC1000 Windows Version* folder on the software CD that came with your CC1000J package (CC1000 Software → CC1000 Windows Version).

When you run the upgrade program, simply follow the Wizard to complete the procedure.

Note: 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.

Chapter 7
Authentication Server Setup

Overview

The Authentication Server component provides User and Device authentication services for the CC1000. Since it utilizes Windows 2000 Server or Windows Server 2003's *Active Directory* and *Certification Authority* services, this chapter takes you through configuring these services to work with the CC1000 system.

Note: Since Active Directory Service is based on the Domain Name System (DNS), the DNS service must be installed on your Windows 2000 Server or Windows Server 2003.

DNS is a component of *Network services*. When Setup brings up the Network services dialog box during your installation of Windows 2000 Server or Windows Server 2003, be sure to enable *Domain Name System* (put a check mark in its checkbox).

Configure Active Directory

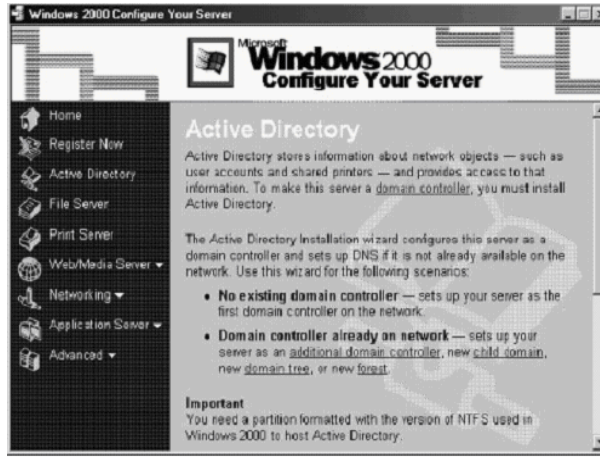
Windows 2000 Server

After you have installed Windows 2000 server (refer to the Microsoft documentation for this product for proper installation), make sure that the network adapter is working correctly. Open Control Panel → Network and Dial-up Connections.

If *Local Area Connection* appears in the window and the status is enabled, the network is working correctly. If not, check if the network adapter appears under the *Device Manager*. If the network adapter doesn't show up there, it means you have to install a driver for it. When everything is working correctly, follow the steps described below.

(continues on next page)

When your server comes up, the *Configure Your Server* dialog box appears:

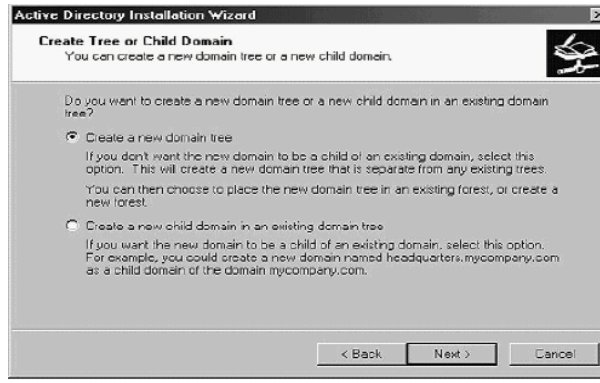


Note: If, for some reason, this dialog box doesn't come up automatically, open Control Panel → Administrative Tools → Configure Your Server

1. In the left panel, click **Active Directory**, then click **Start** at the bottom of the right panel to bring up the *Active Directory Installation Wizard*:

(Continues on next page.)

2. Select *Domain Controller For A New Domain*, then click **Next**.
   The following dialog box comes up:



3. Select *Create a new domain tree*, then click **Next.** The following dialog box comes up:

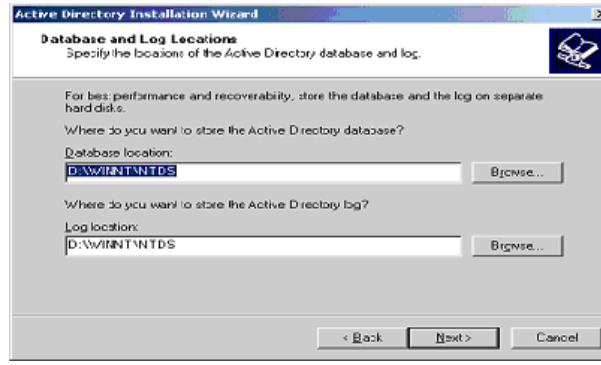
(continues on next page)

4. Select *Create a new forest of domain trees*, then click **Next**. The *New Domain Name* dialog box comes up:

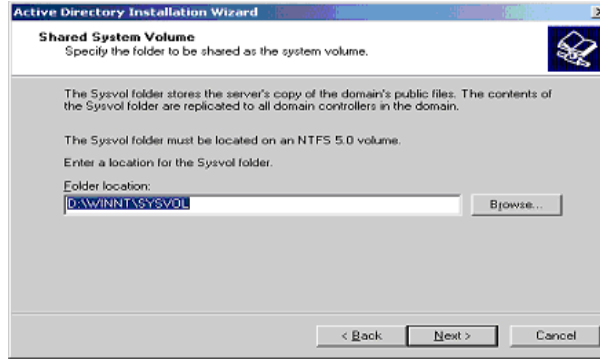
5. Key in a name for the new domain (in our example, we used cc1k.com, but you should give it a name that is meaningful for your installation.), then click **Next**. The *NetBIOS Domain Name* dialog box comes up:

(continues on next page)

6. Key in a NetBIOS domain name (in our example, we used CC1K, but you should give it a name that is meaningful for your installation.), then click **Next**. The *Database and Log Locations* dialog box appears.

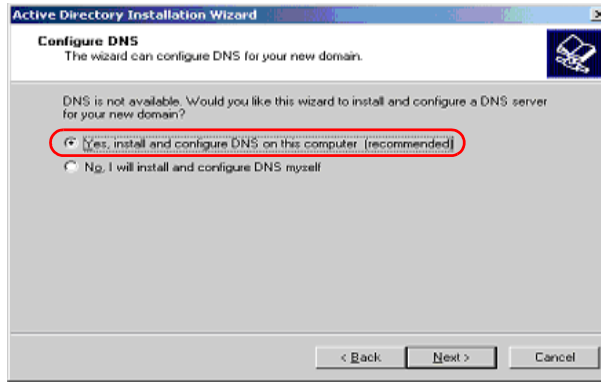


7. We suggest that you keep the default values, as shown in the diagram, and click **Next** to move on. The *Shared System Volume* dialog box appears:

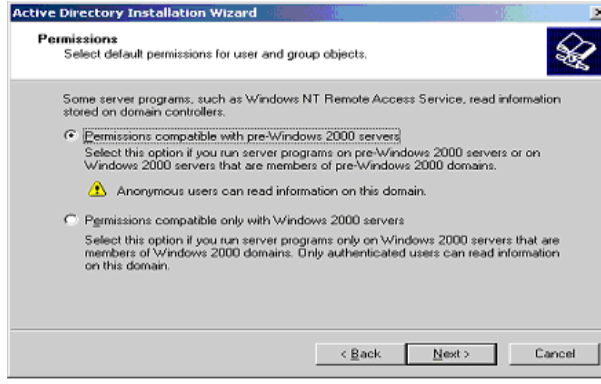


(continues on next page)

8. We suggest that you keep the default value, as shown in the diagram, and click **Next** to move on. The *Configure DNS* dialog box appears:



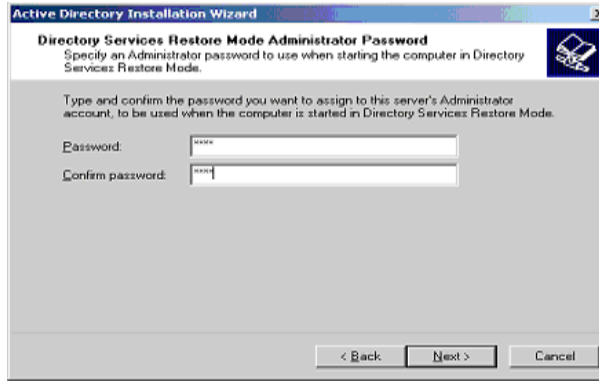
9. Select *Yes, install and configure DNS on this computer (recommended)*, then click **Next**. The *Permissions* dialog box comes up:



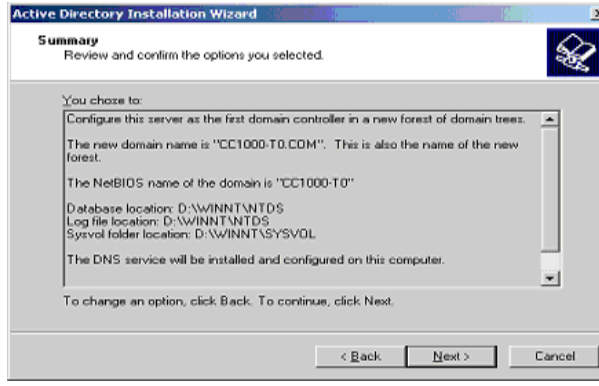
10. Depending on your installation, you can choose either option. Click **Next** to move on.

(continues on next page)

The *Directory Service Restore Mode Administrator Password* dialog box comes up:



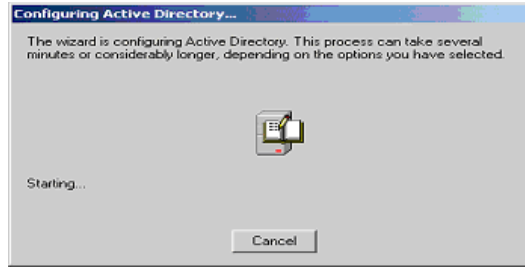
11. Key in a password; confirm it; then click **Next**. A *Summary* screen appears, allowing you to review and confirm the options you selected:



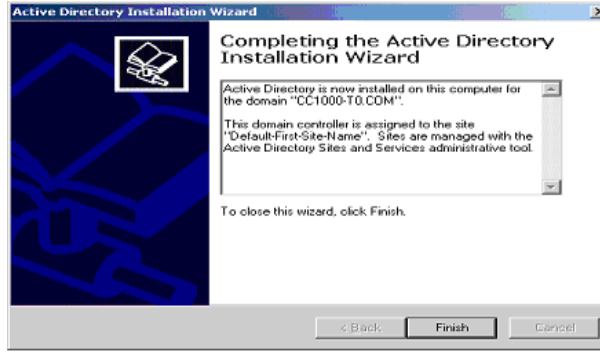
12. If you want to make any changes, click **Back**. If the information is satisfactory, click **Next**. The wizard now configures Active Directory.

(continues on next page)

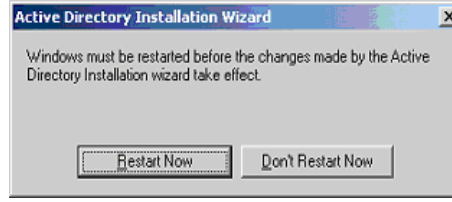
During configuration, the wizard displays the following screen:



When configuration has completed, the following screen appears:



13. Click **Finish** to complete the procedure. A screen pops up informing you that the system must be restarted before the changes can take effect:



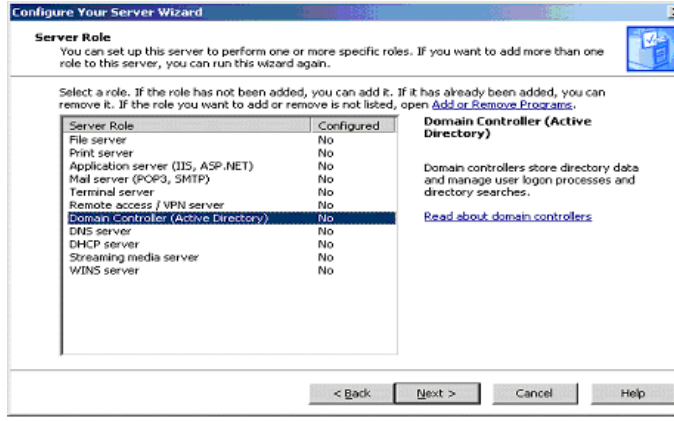
14. Click **Restart Now** to restart your system.

Windows Server 2003

After installation of Windows Server 2003, make sure that the network adapter is working correctly. Open Control Panel → Network and Dial-up Connections.

If *Local Area Connection* appears in the window and the status is enabled, the network is working correctly. If not, check the network adapter under the *Device Manager*. If you can't find the network adapter, it means you have to install a driver for it. When you have made sure that everything is working correctly, follow the steps described below to configure Active Directory.

1. If the *Manage Your Server* window is available, select *Add or remove a role*, then click **Next**. The *Configure Your Server Wizard* appears:

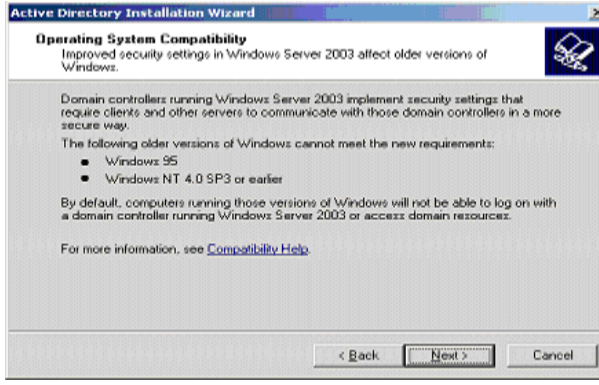


Note: If the *Manage Your Server* window is not available, open Control Panel → Administrative Tools → Configure Your Server Wizard

(continues on next page)

2. Select *Domain Controller (Active Directory)*, and click **Next**. The *Active Directory Installation Wizard* appears:

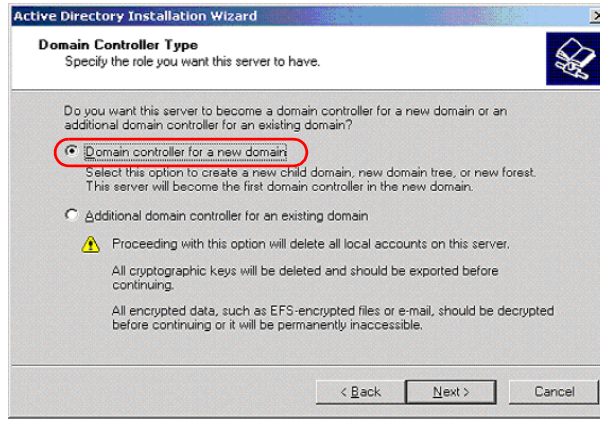
3. Click **Next** to move on. The *Operating System Compatibility* screen appears:



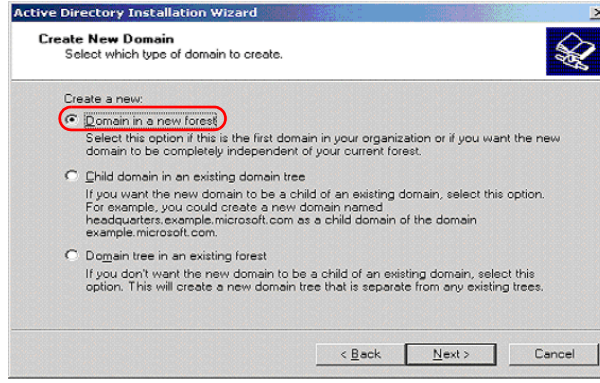
4. Click **Next** to move on.

(continues on next page)

The *Domain Controller Type* dialog box appears:

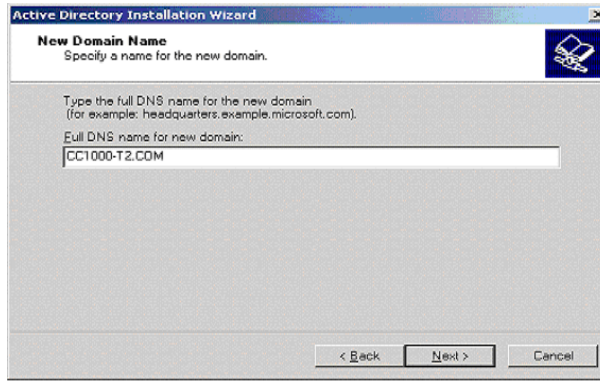


5. Select *Domain controller for a new domain*, then click **Next**. The following dialog box appears:

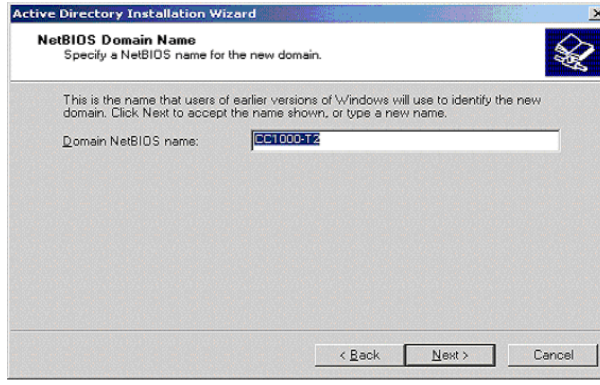


(continues on next page)

6. Select *Domain in a new forest*, then click **Next**. The *New Domain Name* dialog box appears:

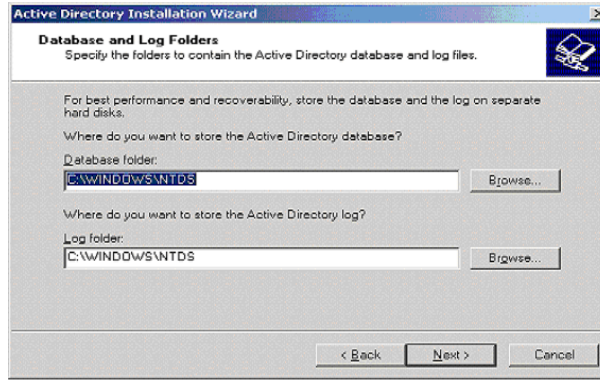


7. Key in a name for the new domain (in our example, we used CC1000.T2.COM, but you should give it a name that is meaningful for your installation.), then click **Next**. The *NetBIOS Domain Name* dialog box comes up:

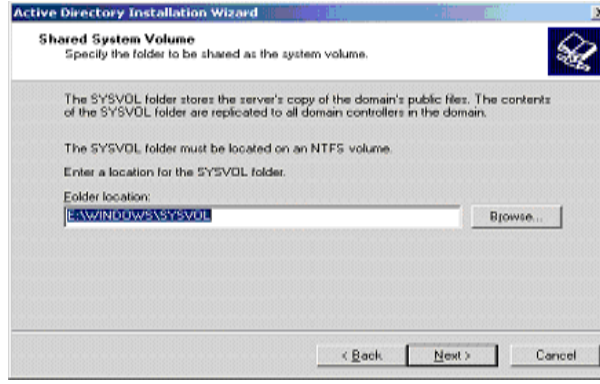


(continues on next page)

8. Key in a NetBIOS domain name (in our example, we used CC1000-T2, but you should give it a name that is meaningful for your installation.), then click **Next**. The *Database and Log Folders* dialog box appears:

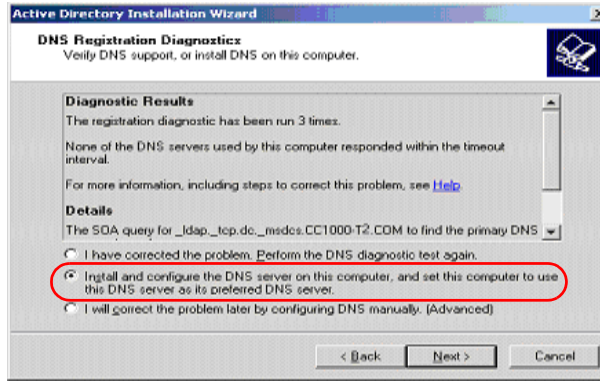


9. We suggest that you keep the default values, as shown in the diagram, and click **Next** to move on. The *Shared System Volume* dialog box appears:

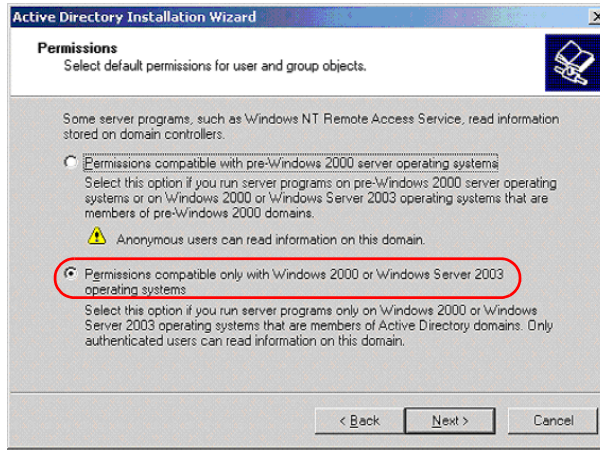


(continues on next page)

10. We suggest that you keep the default value, as shown in the diagram, and click **Next**. The *DNS Registration Diagnostics* dialog box appears:



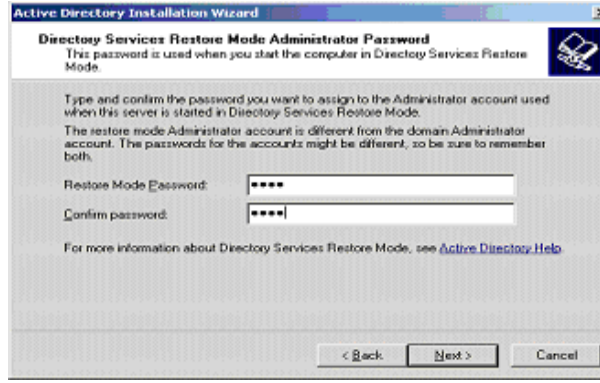
11. Select *Install and configure DNS server on this computer* (etc.), then click **Next**. The *Permissions* dialog box comes up:



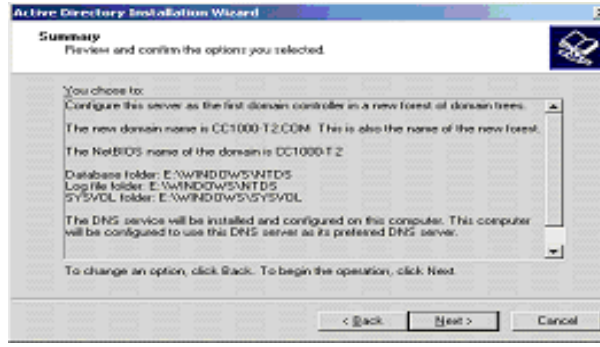
Depending on your installation, you can choose either option. Unless you have a specific reason to change the setting, however, we recommend that you select *Permissions compatible only with Windows 2000 or Windows 2003 operating systems*, then click **Next** to continue.

(continues on next page)

The *Directory Service Restore Mode Administrator Password* dialog box comes up:

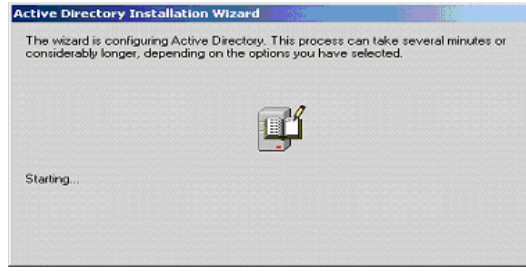


12. Key in a password; confirm it; then click **Next**. A *Summary* screen appears, allowing you to review and confirm the options you selected.

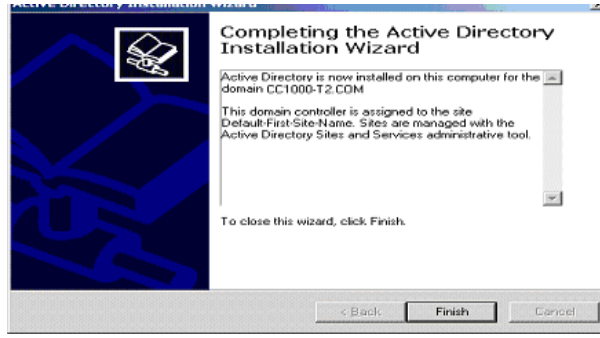


(continues on next page)

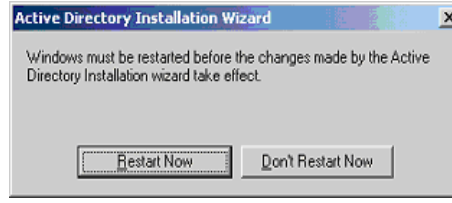
13. If you want to make any changes, click **Back**. If the information is satisfactory, click **Next**. The wizard now configures Active Directory.



When configuration has completed, the following screen appears:



14. Click **Finish** to complete the procedure. A screen pops up informing you that the system must be restarted before the changes can take effect:



15. Click **Restart Now** to restart your system.

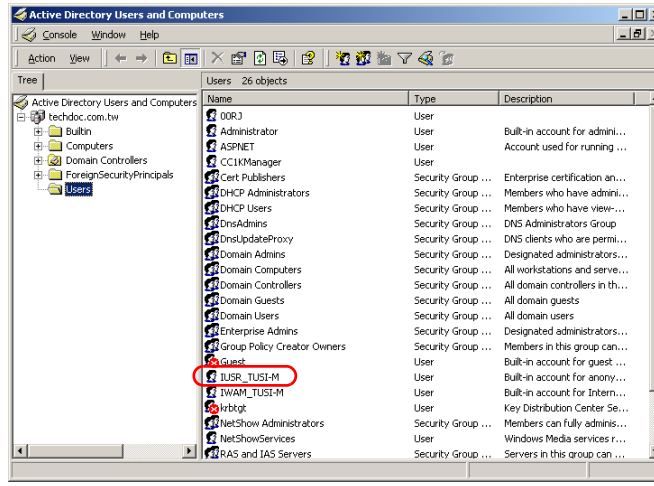
Password Setup

The following sections describe how to set up the password for anonymous users for IIS and CC1000 web access.

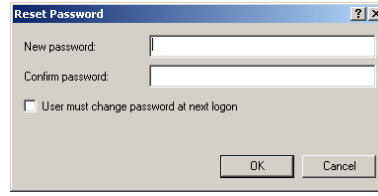
Windows 2000 Server

To reset the anonymous user password on Windows 2000 Server, do the following:

1. Open Control Panel → Administrative Tools → Active Directory Users and Computers → Users. A screen similar to the one below appears:



2. In the user list, right click on the **IUSR_XXXX** entry (where XXXX represents your computer name).
3. In the context menu that appears, click **Reset Password...** The following dialog box comes up:



4. Key in the new password. For something easy to remember, you can simply key in “password”.

> **Note:** Make sure that you **don’t** have a check in the “User must change password at next logon” check box.

5. Click **OK**. A confirmation message appears:

6. Click **OK** to finish up.

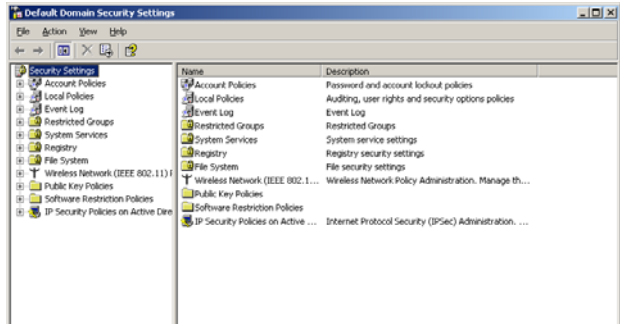
Windows Server 2003

Since operators can log into the CC1000 with fewer characters than Windows Server 2003’s Password Policy allows, this section describes how to adjust the Windows Server 2003 Password Policy to allow users to log in with passwords of fewer characters.

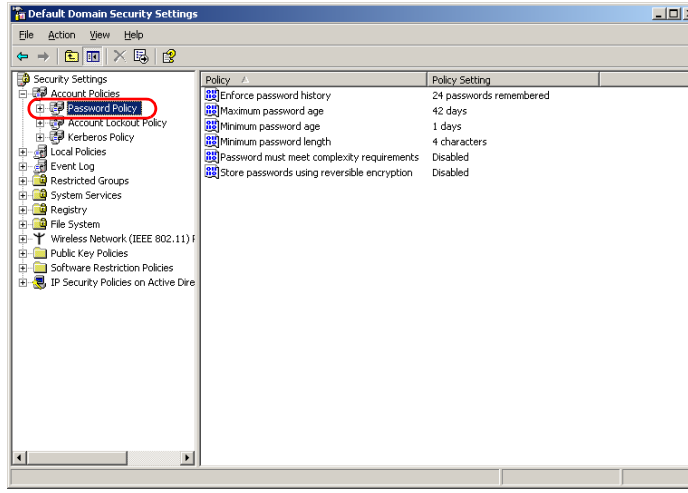
Although this procedure is optional, unless the Password Policy is adjusted, CC1000 operators won’t be able to log in with simpler passwords. Be aware, however, that by lowering the password policy you are also lowering system security.

To adjust the Windows Server 2003 Password Policy, do the following:

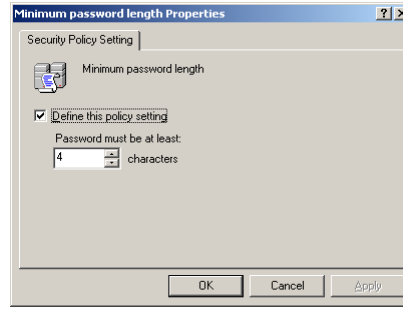
1. Open Control Panel → Administrator Tools → Domain Security Policy. The following screen appears:



2. Under *Security Settings*, expand *Account Policies* then select *Password Policy.* The following dialog box appears:



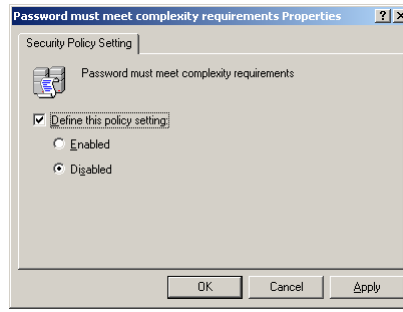
3. The default setting for the minimum password length is seven. If you want to change the default length, double click **Minimum password length**. The *Minimum password length Properties* screen appears:



Change the setting, then click **OK** to return to the *Default Domain Security Settings* dialog box.

Note: If you do change the setting, we recommend that you set it to a length of four or greater. This is because the minimum password length for CC1000 authentication is four, and the CC1000 login password must match the password set in AD.

4. In he *Default Domain Security Settings* dialog box, double click **Password must meet complexity requirements**. The *Password must meet complexity requirements Properties* screen appears:



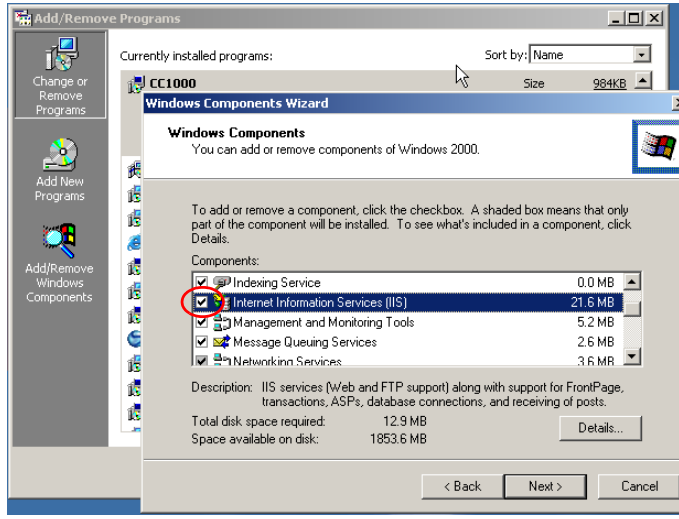
5. Click to put a check in the *Define this policy setting* checkbox; click to select **Disabled**; then click **OK** to return to the *Default Domain Security Settings* dialog box.
6. Close the *Default Domain Controller Security Settings* dialog box.

IIS Installation and Setup

Windows 2000 Server

By default, IIS 5.0 is installed on Windows 2000 Server. If your server did not install IIS, do the following to install IIS now:

1. Open Control Panel → Add/Remove Programs.
2. In the left panel of the screen that appears, click **Add/Remove Windows Components**.
3. In the *Windows Component Wizard*, enable *Internet Information Services (IIS)* by putting a check in its checkbox.

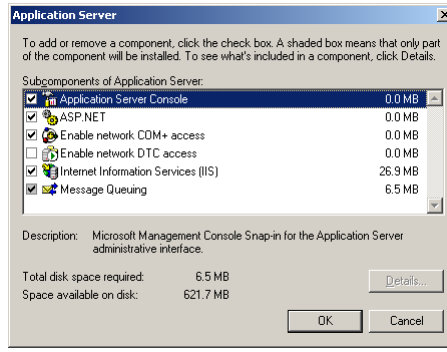


4. Click **Next**, then click **Finish** to close the wizard.

Windows Server 2003

When you install Windows Server 2003 you have the option of installing IIS at the same time. If you did not install IIS when you installed Windows Server 2003, do the following to install it now:

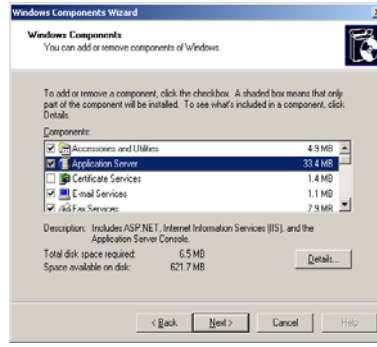
1. Open Control Panel → Add/Remove Programs.
2. In the left panel of the screen that appears, click **Add/Remove Windows Components**.
3. In the Windows Components page, select *Application Server* and click **Details**. A screen similar to the one below appears:



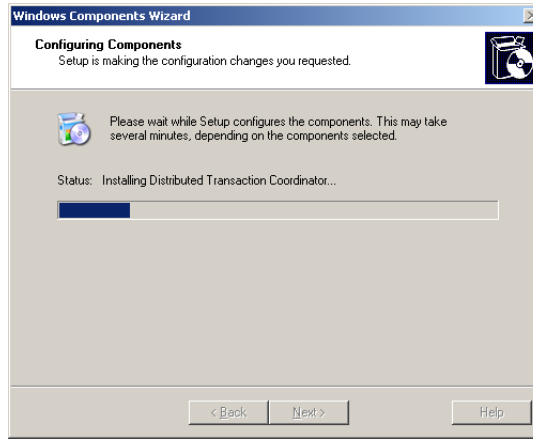
4. Make sure that *Application Server Console* and *Internet Information Services (IIS)* are enabled (click to put a check in the checkbox).
5. Select *Internet Information Services (IIS)* and click **Details**. Make sure that *Common Files*, *Internet Information Services Manager*, and *World Wide Web Service* are enabled.
6. Select *World Wide Web Service*, and click **Details**. Make sure that all the items listed are enabled, then click **OK**.

(continues on next page)

7. Click **OK** in all the opened dialog boxes until you are back at the main *Windows Components* screen, pictured in the following diagram:



8. Click **Next** to have the components configured. While the configuration procedure takes place, a screen similar to the one below appears:



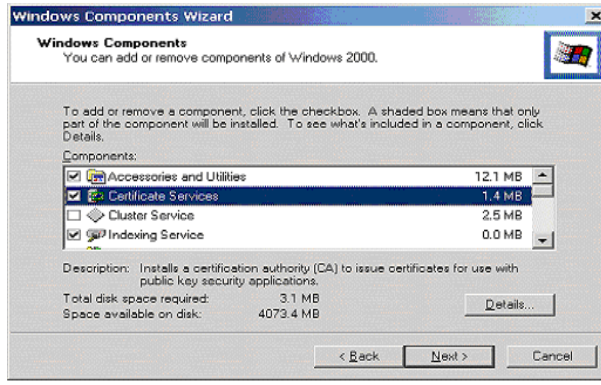
9. When a screen appears to inform you that you have successfully completed the procedure, click **Finish**.

Certification Authority Installation

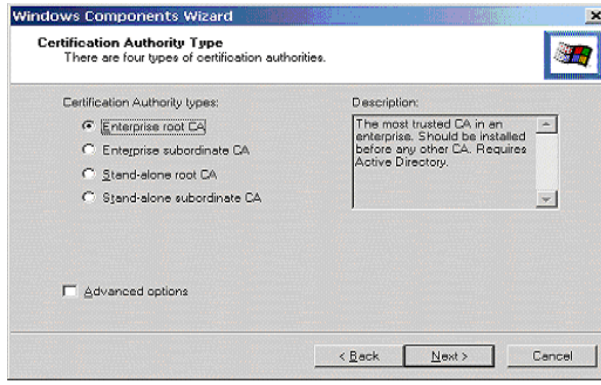
Note: The examples that follow show how to install Microsoft's CA. You may choose a different CA (RSA, VeriSign, e.g.), to install if you wish.

Windows 2000 Server

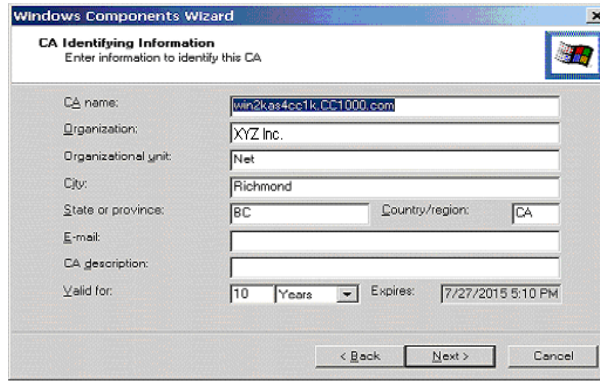
1. Open *Control Panel* → *Add/Remove Programs*.
2. In the left side panel, click **Add/Remove Windows Components**. The Windows Component Wizard appears.



3. Select *Certificate Services*, then Click **Next**. The *Certification Authority Type* dialog box appears:



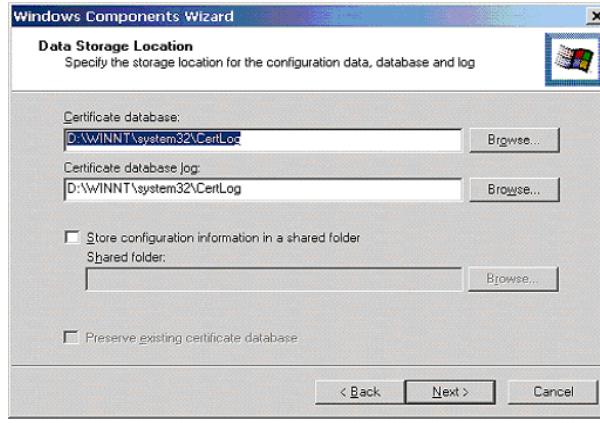
4. Select *Enterprise Root CA*, then Click **Next**. The *CA Identifying Information* dialog box appears:



5. Key in the ***full computer name*** in the *CA name* field.

Important! You must use the server's ***full computer name*** in this field. See *Getting the Full Computer Name*, page 195, for details.

Enter whatever suits your requirements for the validity period, then click **Next**. The following dialog box appears:



(continues on next page)

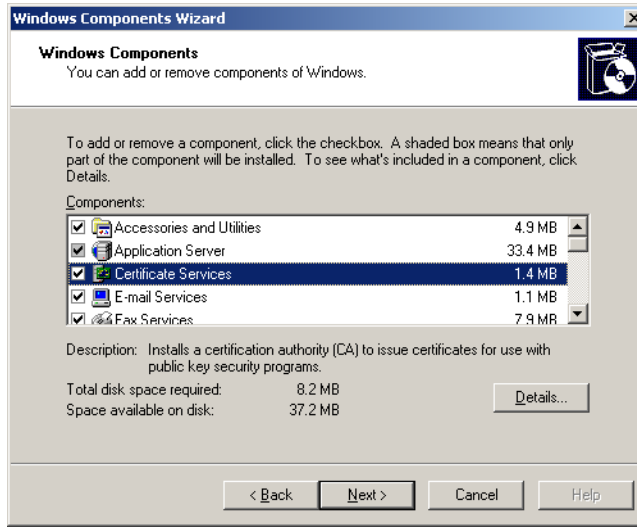
6. Keep the defaults for *Certificate Database* settings; click **Next**; and follow the instructions to complete the installation.

Note: At this time you may be asked to temporarily stop the Internet Information Services, and insert the Windows 2000 Server CD.

7. Click **Finish** to close the wizard.

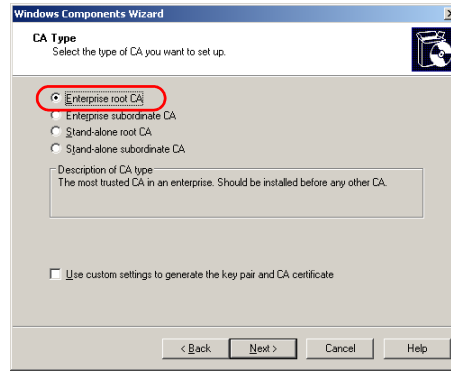
Windows Server 2003

1. Open *Control Panel* → *Add/Remove Programs*.
2. In the left side panel, click **Add/Remove Windows Components**. The Windows Component Wizard appears.

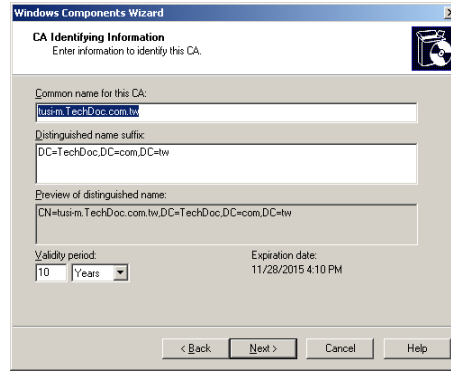


(continues on next page)

3. Select *Certificate Services*, then Click **Next**. The *CA Type* dialog box appears:



4. Select *Enterprise Root CA* for the *CA Type*, then click **Next**. The *CA Identifying Information* dialog box appears:



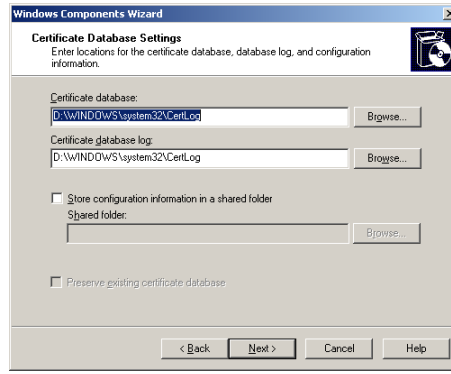
5. Key in the ***full computer name*** in the *Common name for this CA* field.

Important! You must use the server's ***full computer name*** in the *Common name for this CA* field. See *Getting the Full Computer Name*, page 195, for details.

Enter whatever suits your requirements for the validity period, then click **Next**.

(continues on next page)

6. In the *Certificate Database Settings* dialog box that appears, keep the default settings for the database and log locations.



Simply click **Next**, and follow the instructions to complete the installation.

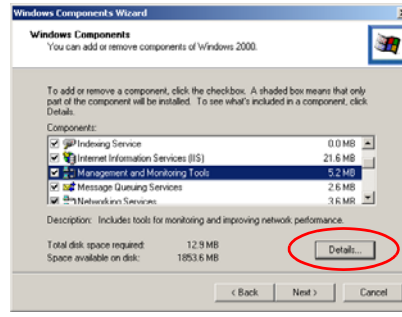
Note: At this time you may be asked to temporarily stop the Internet Information Services, and insert the Windows Server 2003 CD.

7. Click **Finish** to close the wizard.

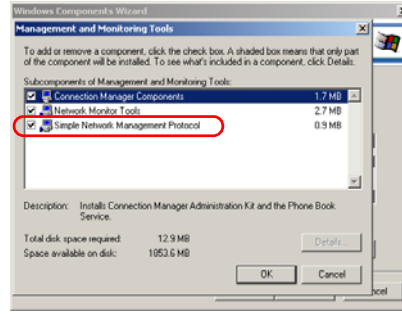
SNMP Installation

To be sure that SNMP is enabled on your server follow the procedures given in the following sections.

1. Under the Control Panel open *Add/Remove Programs*.
2. In the left panel, click **Add/Remove Windows Components**. The Windows Component Wizard appears:



3. Select *Management and Monitoring Tools*, then click **Details**. The following screen appears:



4. Make sure that *Simple Network Management Protocol* is checked, then click **OK** → **Next** → **Finish** to close the wizard.

Note: On Windows Server 2003, if you encounter any problems related to SNMP, make sure that *SNMP Service* and *SNMP Trap Service* have been started. (Control Panel → Administrative Tools → Services)

This Page Intentionally Left Blank

Chapter 8
CC1000 Server Setup

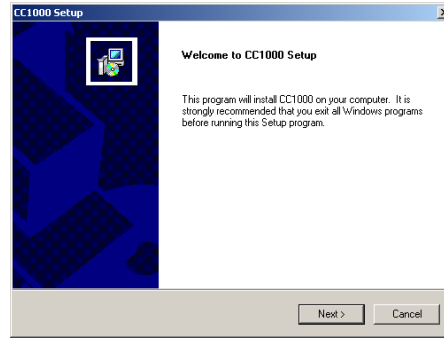
Installation

Before installing the CC1000 Server software, we strongly recommend that you download and install all the updates for the Windows 2000/2003 server.

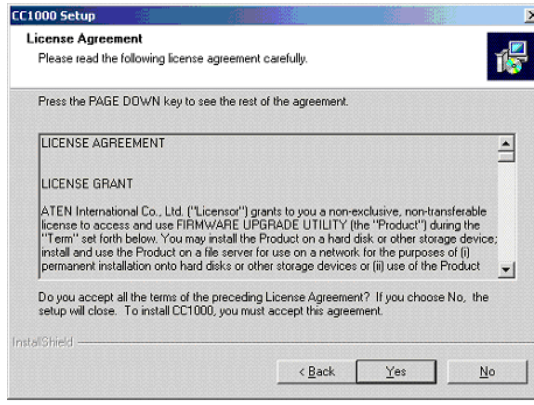
Note: The computer you are installing the CC1000 Server on must have CA, IIS, and SNMP services enabled. See pages 100, 97, and 105 for details.

In addition to containing the CC1000 Manager (discussed in Chapter 10), the CC1000 Server contains the CC1000 Web pages, and provides the entry point for users when they log in. To install CC1000 Server:

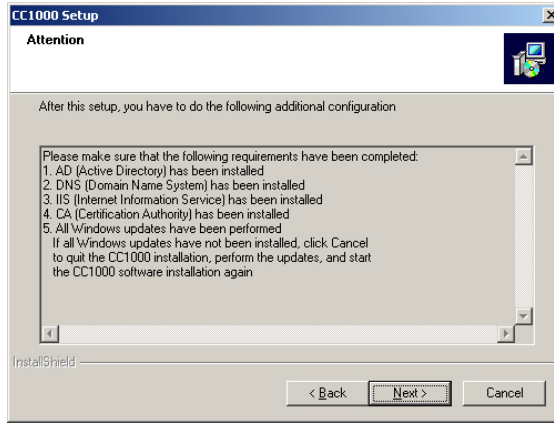
1. Plug the CC1000 USB Authentication Key into a USB port on the computer you are installing the CC1000 Server on. For security purposes, the key can be installed inside the case. See page 196 for details.
2. Copy *CC1KSetup.exe* from the software CD that came with your package to a convenient location on your server.
3. Go to the folder where *CC1KSetup.exe* is located, and execute it. The CC1000 Welcome screen appears:



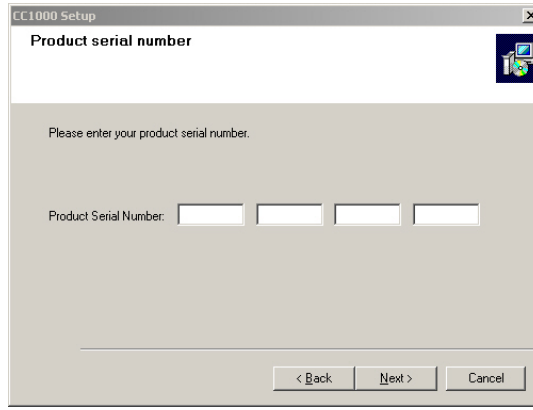
4. Click **Next** to continue. The License Agreement appears:



5. Click **Yes** to accept the License Agreement. In the *Attention* dialog box that comes up, make sure that the indicated requirements have been completed.

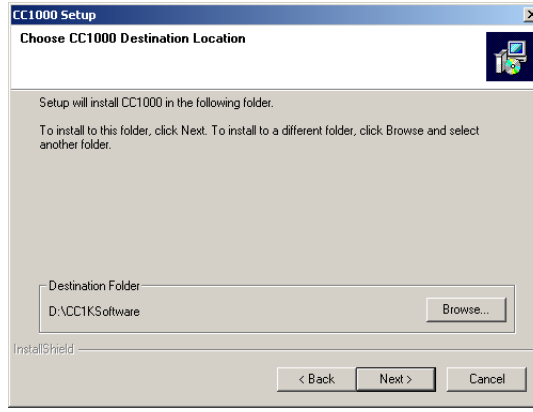


6. Click **Next** to continue. The *Serial Number* dialog box appears:



The serial number can be found on the CC1000's CD case. Key in the serial number.

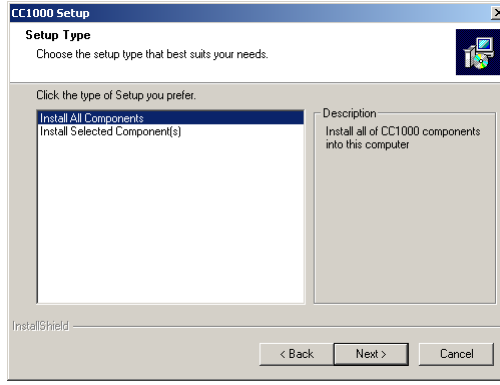
7. Click **Next** to continue. The following screen appears:



8. Select the destination folder for the CC1000 program, then click **Next** to copy files and install components.

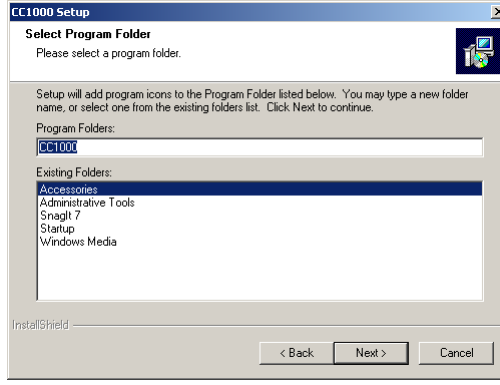
Important! CC1000 Web Pages are put in the *CC1Kweb* folder under the destination folder you selected. You must specify the full path to the CC1Kweb folder as the Home Directory of the CC1000 Website when you configure the CC1000 Website (see *Web Server Setup*, page 114).

After you click **Next**, the following screen appears:



9. Select *Install All Components*, then click **Next**.

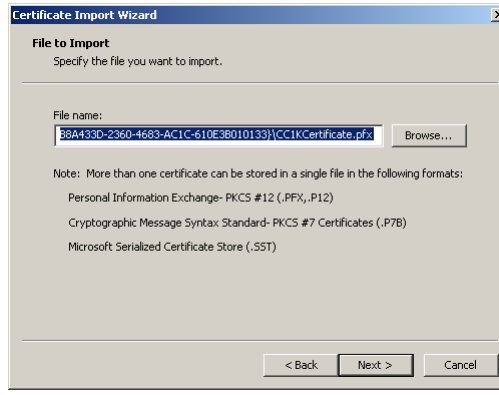
10. In the screen that comes up, accept the default choice for the location of the program icons, or choose another location, then click **Next** to complete this stage of the CC1000 Server software installation



Certificate Import

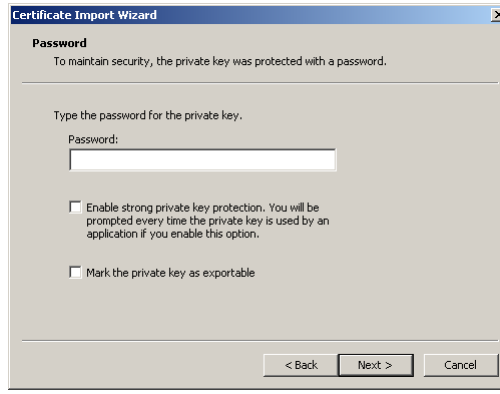
After the previous stage of the software installation ends, the *Certificate Import Wizard* appears:

1. Click **Next** to continue. The following dialog box appears:

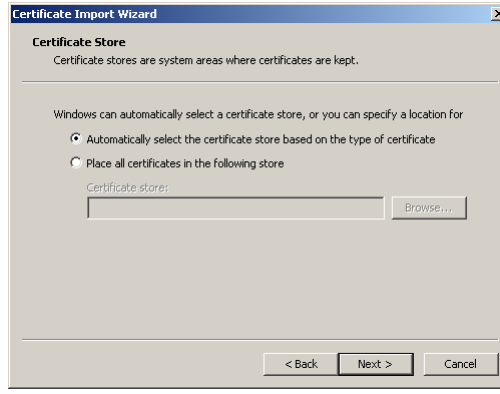


(continues on next page)

2. Keep the default settings; click **Next** to continue. The following dialog box appears:

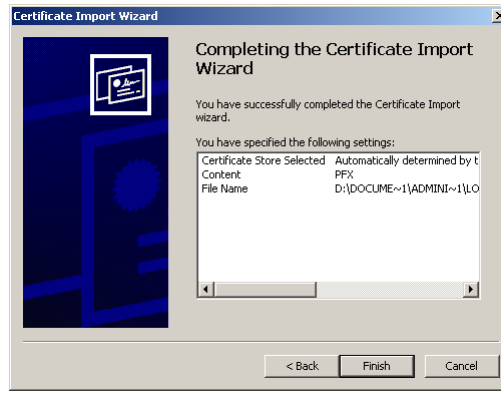


3. Keep the default settings; click **Next** to continue. The following dialog box appears:



(continues on next page)

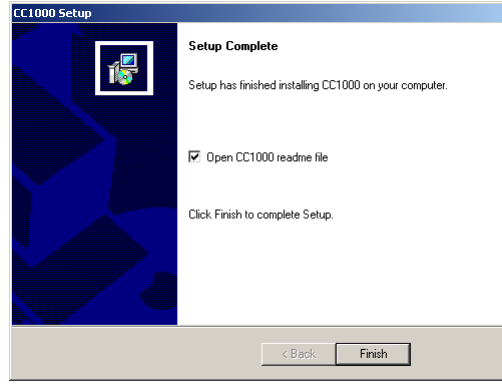
4. Keep the default settings; click **Next**. The following screen appears:



5. Click **Finish**. A window pops up to inform you that the procedure completed successfully:

   Click **OK** to move on.

6. When the following screen appears, Click **Finish** to close the Certificate Import Wizard and complete the CC1000 Server installation.



   After the screen closes, the CC1000 *readme* file comes up for your reference.

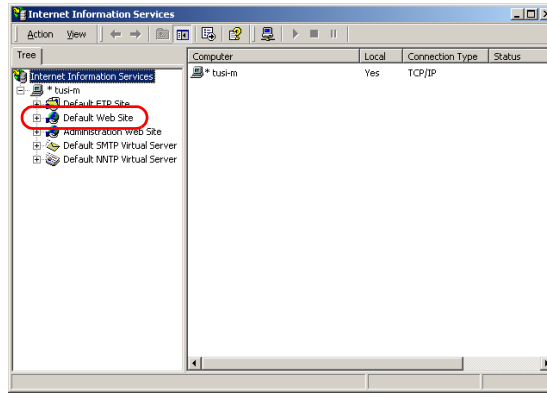
Web Server Setup

Configure the Default Web Site

When you installed IIS, it was preconfigured to serve as a default Website. You now need to change some of the settings, as follows:

1. For Windows 2000 Server, open *Control Panel* → *Administrative Tools* → *Internet Services Manager*. For Windows Server 2003, open *Control Panel* → *Administrative Tools* → *Internet Information Services (IIS) Manager*.

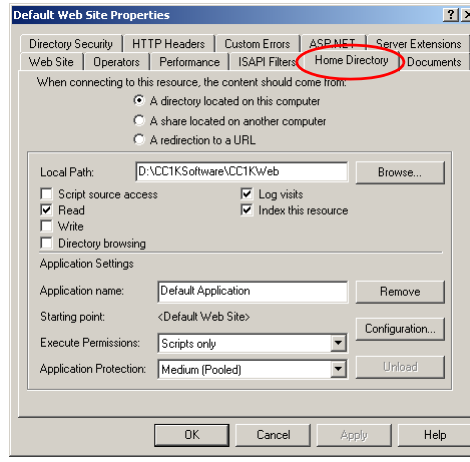
   A screen similar to the one below appears:



2. In the left panel, right click **Default Web site**. In the menu that pops up, click **Properties**.

(continues on next page)

3. In the *Default Web Site Properties* dialog box that comes up, select the **Home Directory** tab. A screen similar to the one below appears:



4. To use a folder on the local computer, select *A directory on this computer*; then click **Browse** to locate the folder that you want to use. This must be the *CC1Kweb* directory under the CC1000 destination folder that you specified when you installed the CC1000 program (refer to page 110, if necessary).

Note: The default directory is c:\CC1KSoftware\CC1kWeb.

---

5. Check **Read** to grant read access to the folder (required).*
6. For *Execution Permissions*, select **Scripts Only**.*

   To ensure that the program has been created, check the button to the right of the *Application name* field. If it displays *Remove*, then the Website has been set as a program. If it displays *Create*, click **Create** to create the program.

   If *Inheritance overrides* appears, select all except the *root _vti_bin* folder, any *subweb _vti_bin* folders, and any *cgi-bin* folders if they exist (these folders should have “execute” to work properly), and then click **OK**.

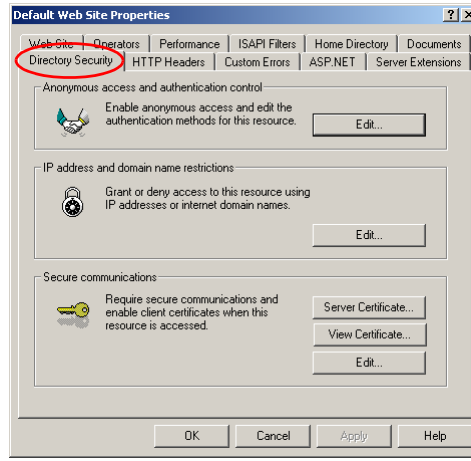
***** Steps 5 and 6 are for Windows 2000 Server Only.

---

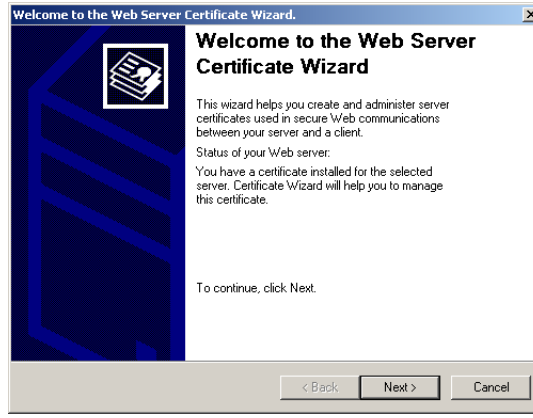
7. Click **OK** to accept the Website properties.

Configure Directory Security for Secure Communications

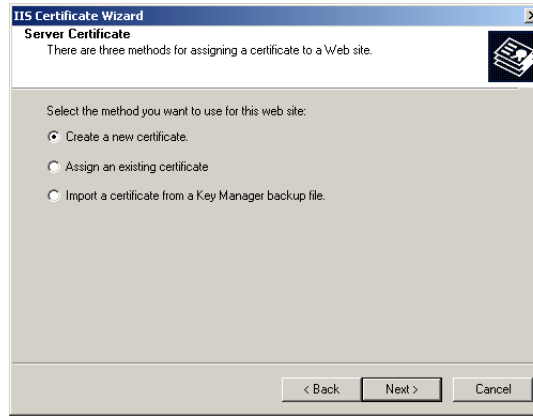
1. In the Control Panel, select *Administrative Tools* → *Internet Services Manager*. A screen similar to the one on page 114 appears.
2. In the left panel, right click **Default Web site**. In the menu that pops up, click **Properties**.
3. In the *Default Web Site Properties* dialog box that comes up, select the **Directory Security** tab. A screen similar to the one below appears:



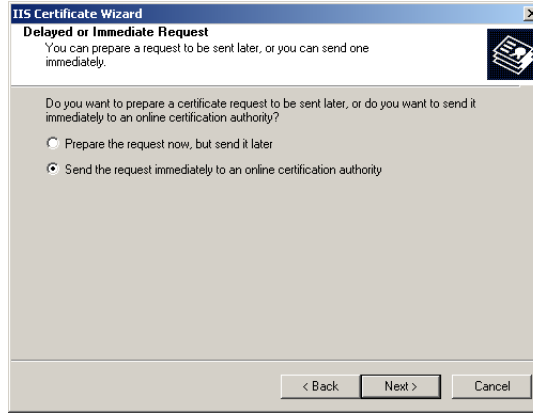
4. Click **Server Certificate...,** the Certificate Wizard comes up:



5. Click **Next** to continue, the following screen appears:

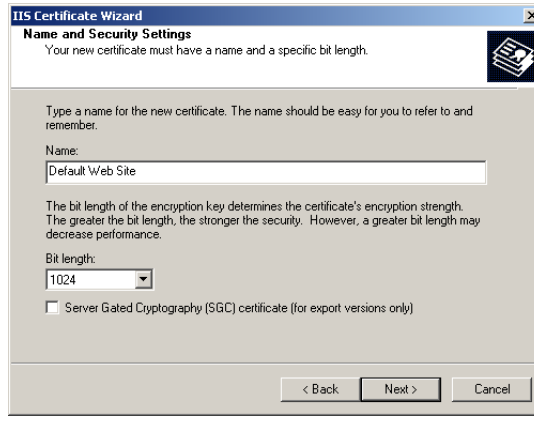


6. Select *Create a new certificate*, then click **Next**. The following screen appears:

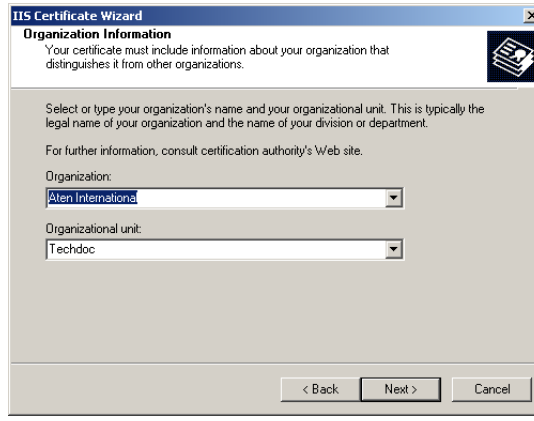


(continues on next page)

7. Select *Send the request immediately to an online certification authority,* then click **Next**. The following screen appears:

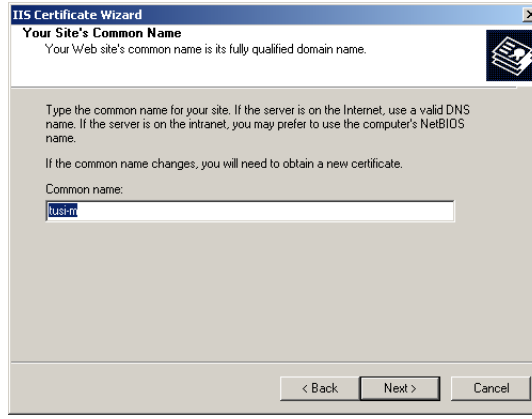


8. Make sure the *Bit length* is 1024; keep the other default settings; click **Next**. The following screen appears:

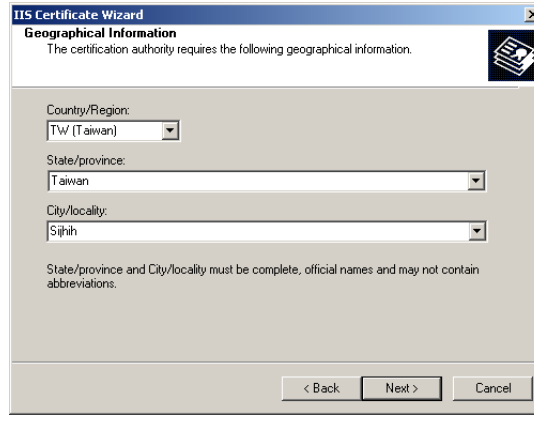


(continues on next page)

9. Key in the *Organization* and *Organizational unit* for the certificate, then click **Next**. The following screen appears:

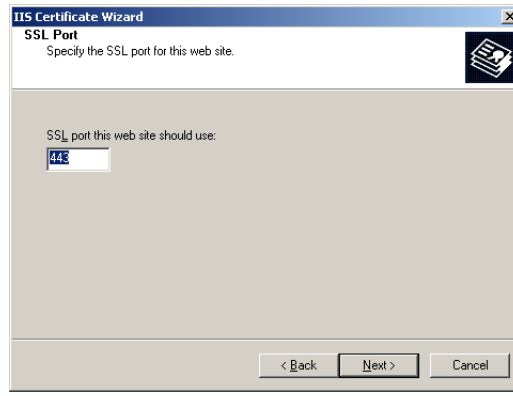


10. Key in the Common name for the certificate (it can be your server's IP address or your server's computer name). We recommend that you keep the default (the server's computer name - **not** the full computer name), then click **Next**. The following screen appears:



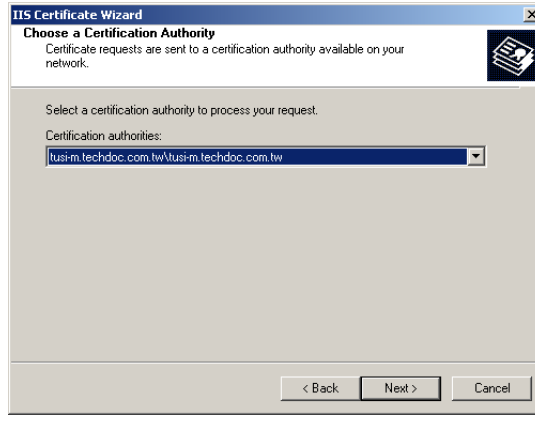
(continues on next page)

11. Key in your geographic information, then click **Next**. The SSL Port screen appears:



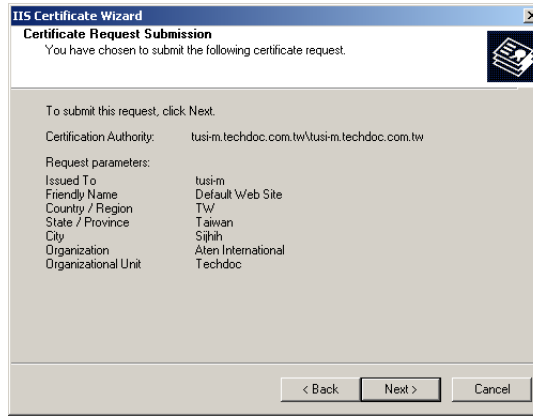
Note: The SSL Port screen is for Windows Server 2003 only. If you are running Windows 2000 Server, ignore this step and go on to the next screen.

12. Make sure to set 443 as the SSL port, then click **Next**. The following screen appears:

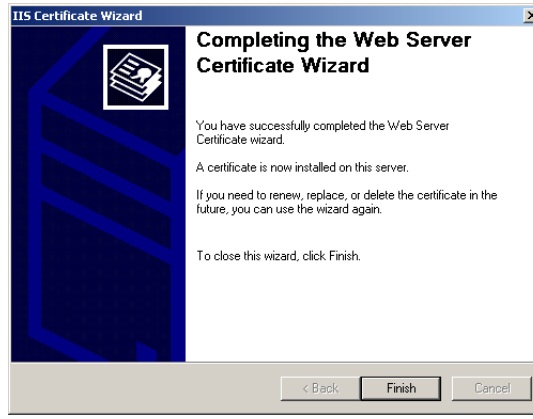


(continues on next page)

13. Keep the default settings; click **Next**. The following screen appears:



14. Click **Next** to submit this request. The following screen appears:

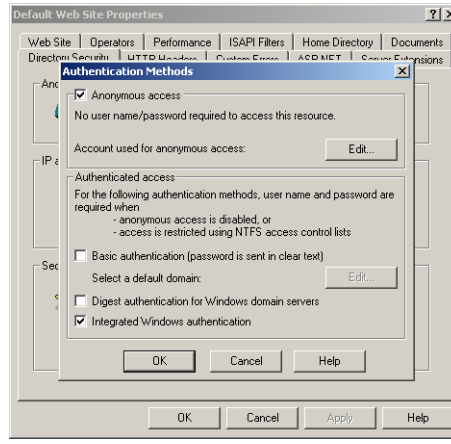


15. Click **Finish** to complete the Web Server Certificate Wizard.

16. When you return to the *Directory Security* screen, click OK to complete the operation.

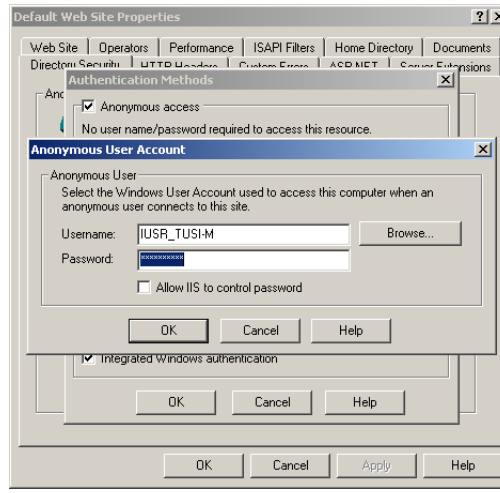
Directory Security Setup for Windows 2000 Server

1. In the Control Panel, select *Administrative Tools* → *Internet Services Manager*. A screen similar to the one on page 114 appears.
2. In the left panel, right click **Default Web site**. In the menu that pops up, click **Properties**.
3. In the *Default Web Site Properties* dialog box that comes up, select the **Directory Security** tab. A screen similar to the one on page 116 appears:
4. In the *Anonymous access and authentication control* panel, click **Edit**.



(continues on next page)

5. Make sure there is a check in the check box for *Anonymous access*, then click **Edit**.



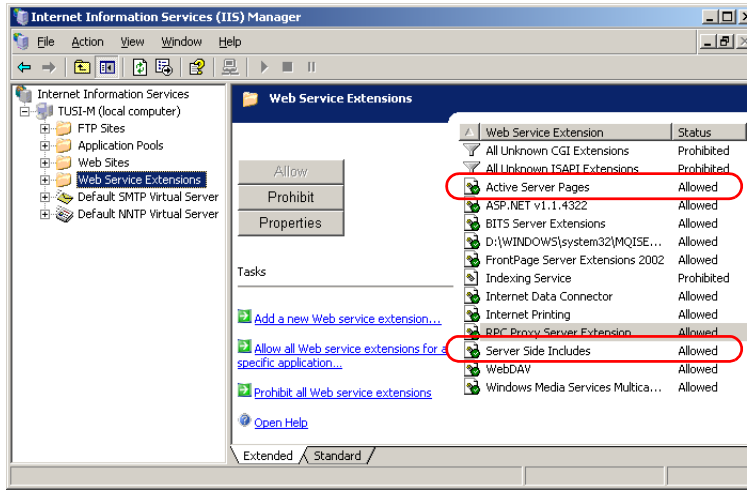
The default anonymous user username appears in the username field. Key in a new password for this account. The username and password must match what was specified for anonymous username and password information under *Password Setup* (refer to page 93). If the username is not correct, click the Browse... button to get the right anonymous username, such as *IUSR_XXX*.)

6. Make sure that the *Allow IIS to control password* check box is not checked.

7. Click **OK** to accept the Website properties.

Enable Web Service Extensions for Windows Server 2003

1. In the Control Panel, select Administrative Tools → Internet Services Manager.
2. In the left panel, drop down the list for the local computer; select **Web Service Extensions**:



3. In the right panel, select *Active Server Pages*, then click **Allow**.
4. In the right panel, select *Server Side Includes*, then click **Allow**.

Finishing Up

Before the CC1000 Server can function properly, the *CC1000 Log Server* and *CC1000 Manager Service* must be started. If they aren't already started, do the following to start them:

1. From the *Start* menu, open *Programs* → *CC1000* → *CC1000 Log Server*.
2. Click **CC1000 Log Server**.

Note: If the Log Server and CC1000 Server are installed on the same computer, the Log Server cannot start independently. The Log Server starts automatically when you start the CC1000 Manager.

3. From the *Start* menu, open *Programs* → *CC1000* → *CC1000 Manager*.
4. Click **CC1000 Manager**

To test the installation in order to make sure that everything is working properly:

1. Key the CC1000 Server's IP address in your browser.
2. When the CC1000 Login Screen comes up key in your Username and Password.

If all went well you should see the CC1000 Main Screen.

Note: 1. The CC1000 comes with a pre installed *superadmin* (Super Administrator) account. You can use this account to test the installation. The Username is *superadmin*; the password is *CC1KPassword*. The password is case sensitive. For security purposes, we strongly recommend changing the password to something unique.

2. If this is a first time login, or if your password was reset with the CC1000 Administrator Utility, you will need to change your password.
3. The CC1000 USB Authentication Key that was provided with your package must be plugged into the USB port of the computer that the CC1000 Server is running on in order for the program to come up successfully. For security purposes, the USB Authentication Key can plug in inside the case. See *USB Authentication Key Bracket Installation*, page 196 for details.

This Page Intentionally Left Blank

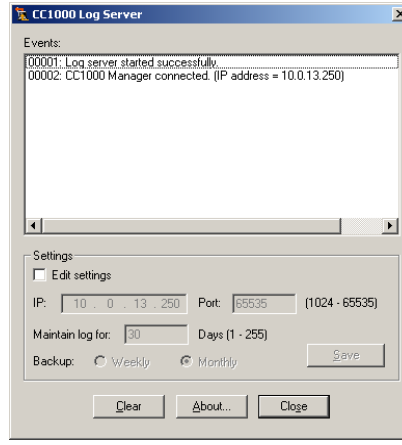
Chapter 9
The Log Server

Overview

The CC1000 Log Server records the events that take place on the CC1000 system and writes them to database file (CC1KLogs.mdb), which can be found in the same directory as the Log Server application. The Log Server automatically starts up when the CC1000 system starts.

To bring up the Log Server dialog box:

Open Start → Programs → CC1000, and click **CC1KLogServer**. The Log Server dialog box comes up:



Note: 1. If the Log Server is installed on the same PC that the CC1000 Manager is running on, the program cannot be executed independently. To bring up the Log Server dialog box, you must click the *Log Server* button in the CC1000 Manager dialog box (see page 131).

2. If the Log Server is not installed on the same PC as the CC1000 Manager, the *Close* button doesn't appear. An *Exit* button appears, instead (see *Close / Exit*, page 129).

Events

This panel displays information regarding the Log Server's operation (if the CC1000 Manager connected, for example). Clicking **Clear** clears the panel.

Fields

Initially, the fields are read only. To change the settings, enable *Edit Settings* (click to put a check in the checkbox).

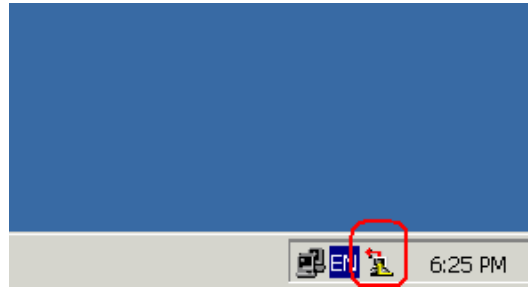
The meanings of the field headings are explained in the table, below:

Heading		Meaning
IP		This field contains the Log Server's IP Address. This address must match the IP address of the computer that the Log Server is running on.
Port		This is the port number of the port that the Log Server listens on. The valid port range is from 1024 to 65535.
Maintain log for		This setting determines the number of days that the working database file keeps a record before discarding it (it is still available in the backup file, however). The Log Server checks the records every hour and automatically deletes the ones that exceed the time limit. The valid time range is from 1 - 255 days.
Backup	Weekly	If *Weekly* is selected, when the Log Server writes a record, it also writes a copy to a backup file that is kept on a weekly basis and named for the week. For example a backup file named *CC1KLogs_W050717_050723.mdb* refers to a backup file that contains all the records for the week of July 17th to July 23rd.
	Monthly	Likewise, if *Monthly* is selected, the backup file is kept on a monthly basis and is named for the month — so that a backup file named *CC1KLogs_M2005_07.mdb* refers to a backup file that contains all the records for the month of July, 2005

3. After you have configured the fields, click **Save** to save your changes.

Close / Exit

- When the Log Server is installed on the same PC that the CC1000 Manager is running on, clicking **Close** closes the dialog box (but the program does not terminate).
- If the Log Server is installed on a PC that is separate from the one that the CC1000 Manager is installed on:
  - There is no *Close* button. There is an *Exit* button, instead. Clicking **Exit** closes the dialog box and also terminates the program.
  - When the dialog box is minimized a Log Server icon appears in the Windows system tray, as follows:



  - To restore the dialog box, double click the icon.
  - To bring up a context menu that allows you to either restore the dialog box or exit the program, right click the icon.

Backup

We strongly recommend backing up the log file on a regular basis.

This Page Intentionally Left Blank

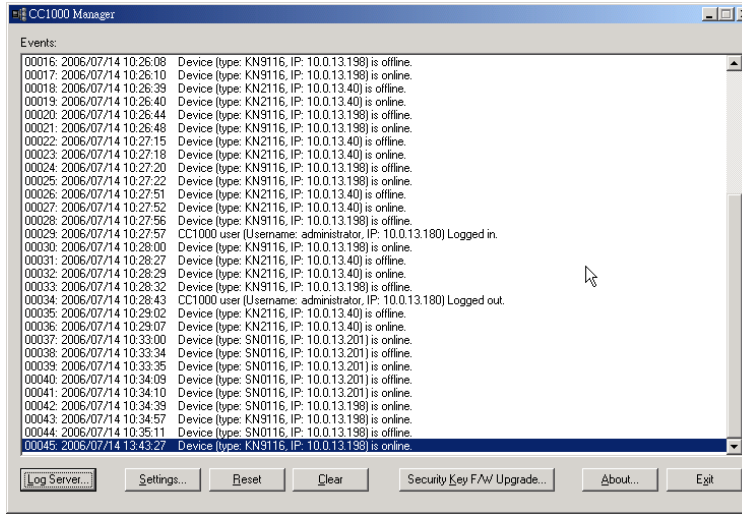
Chapter 10
The CC1000 Manager

Overview

The CC1000 Manager is the central component of the CC1000 system. It communicates with all the other components and presents status information about overall CC1000 operation. The CC1000 Manager automatically starts up when the CC1000 system starts.

Note: If the CC1000 Manager has been shut down, you can bring it up by opening Start → Programs → CC1000 → CC1000 Manager.

When the CC1000 Manager comes up, a screen like the one below appears:



- Messages concerning events that take place on the CC1000 appear in the *Events* panel.
- The functions of the buttons at the bottom of the screen are explained in the sections that follow.

Note: The *Log Server* button only appears when the Log Server is installed on the same PC that the CC1000 Manager is installed on.

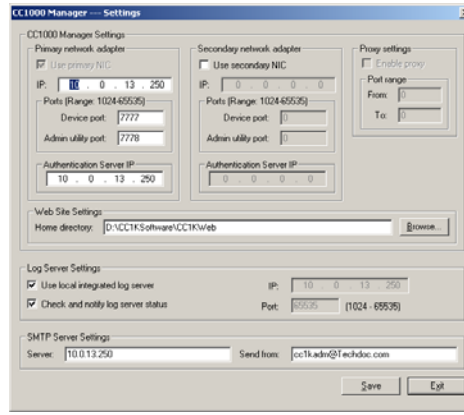
Button Functions

An overview of the button functions is given in the table below:

Button	Function
Log Server	The **Log Server** button brings up the Log Server dialog box. See page 127 for details.
Settings	The **Settings** button brings up a dialog box that lets you set configuration values for the CC1000 system. See page 133 for details.
Reset	The **Reset** button stops the program and then restarts it – saving you the trouble of having to close the window and go through the selection procedure again.
Clear	The **Clear** button erases the contents of the *Events* panel and starts over with a clean screen.
Security Key F/W Upgrade	The **Security Key F/W Upgrade** button brings up a dialog box that lets you upgrade the USB Security Key's firmware. **See** *Upgrading the USB Authentication Key Firmware*, page 138**.**

Configuration Settings

When you click the *Settings* button at the bottom of the CC1000 Manager's Main Screen, the following dialog box appears:



The dialog box is organized into the following main areas:

- CC1000 Manager Settings
- Log Server Settings
- SMTP Server Settings

The settings for each of these are discussed in the sections that follow.

CC1000 Manager Settings

Primary and Secondary Network Adapters:

The CC1000 makes use of one or two network adapters (two are recommended). If you use only one, it is the Primary adapter; its checkbox is enabled, and can't be disabled.

If you use two adapters – one for an Intranet (internal) and one for the Internet (external), for example – then you must enable the Secondary adapter (click to put a check in the *Use Secondary NIC* checkbox), and provide the appropriate IP address and port information.

The meanings of the fields are described in the following table:

Field	Meaning
IP	The IP address assigned to the network adapter of the computer that the CC1000 Server is installed on. (This is the computer that the CC1000 Manager is running on.)
Device port	The port is the port that the CC1000 Manager uses to communicate with the devices on the installation (CN-6000, PN9108, SN0116, etc.).
Admin utility port	The port that the CC1000 Manager uses to communicate with the Administrator Utility.
Authentication Server IP	The IP address of the computer that the Authentication Server is running on.

Note: 1. You cannot use 0.0.0.0 or 255.255.255.255 for the IP address of either the Primary or Secondary NIC.

2. No two ports on the same NIC can have the same value.

3. You cannot use 0.0.0.0 or 255.255.255.255 for the IP address of the the Primary Authentication Server.

4. You can use 0.0.0.0 for the IP address of the Secondary Authentication Server (it means ignore this IP), but you cannot use 255.255.255.255.

Some setting examples are given below:

1. CC1000 Manager and the Authentication Server are both installed on the same computer; the computer has two network adapters:

   The Primary Network Adapter's IP setting and the IP setting for the Authentication Server must be the same.

   Note: If you wish to download the Administrator Utility and access the Authentication Server via the Secondary Network Adapter, its IP cannot be 0.0.0.0.

(continues on next page)

(Continued from previous page.)

2. The CC1000 Manager and the Authentication Server are on separate computers; each computer has two network adapters (one for the Intranet; one for the Internet):
   - The IP of the Primary Network Adapter for both the CC1000 Manager computer and the Authentication Manager computer must both be on the same network segment.
   - The IP of the Secondary Network Adapter for both the CC1000 Manager computer and the Authentication Manager computer must both be on the same network segment.

Proxy Settings:

To allow users to access CC1000 managed devices over a WAN you have to enable the proxy function (put a check in the *Enable Proxy* checkbox). Since this function makes use of the Secondary Network Adapter, it only becomes available if the Use Secondary NIC function is enabled (refer to the discussion in the previous section).

After enabling *Proxy Setting*, specify a range of ports for the CC1000 Manager to use for this function. The valid range is from 1024 to 65535, with a minimum difference of 500.

Note: 1. If the CC1000 Server is behind a firewall, the proxy ports set here must be allowed by the firewall.

2. If you use this feature, when you Save the settings the program checks the *Secondary network adapter* and *Proxy settings* fields. If there is an error, it brings the cursor to the invalid field and asks you to re-enter the information for that field.

Web Site Settings:

This field specifies the location of the CC1000's web page directory. See *Important!* page 110 and *Note:* page 115 for details.

Log Server Settings

There are four settings for this section, as described in the table, below:

Field	Purpose
Use local integrated log server	This field lets you specify whether you are using a local or remote log server. A local log server refers to one that is installed on the same computer that the CC1000 Manager is installed on. A remote log server is one that is installed on an independent computer. **Note:** If you enable *Use local integrated log server*, the *IP* and *Port* fields are disabled since there is no need to set them.
Check and notify log server status	If this function is enabled, and the connection to the log server is lost, you are notified about the status in the *Events* panel. You will see either of the following messages: 1. No records were lost: "Failed to connect with Log Server (IP:xxxxx). No logs were lost. Will try again in 1 minute. 2. Some records were lost: "Failed to connect with Log Server (IP:xxxxx). A total of yy log(s) was (were) lost. Will try again in 1 minute. Where xxxxx represents an actual IP address, and yy represents a number indicating how many records were lost.
IP*	If you choose to use a remote log server (you do not enable *Use local integrated log server*), you have to specify the IP address of the computer that the log server is running on in this field.
Port*	If you choose to use a remote log server (you do not enable *Use local integrated log server*), you have to specify the Port that the log server on the remote computer is listening on.

***** The IP address and port settings of the Log Server entry must correspond to the ones you set when you configured the Log Server (see page 127).

SMTP Server Settings

The CC1000 sends email notification of emergency occurrences on installed devices to users of those devices.

Note: Recipients are designated in each device's configuration settings. See the device's User Manual for details.

Specify the IP address or the domain name of the computer running your SMTP server in the *Server* field. Specify the CC1000 administrator's email address in the *Send From* field.

Note: This field cannot be blank.

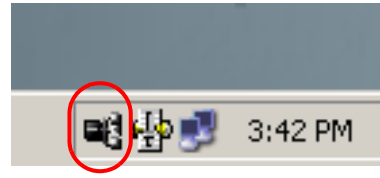
Finishing Up

To save your new settings and exit, click **Save**. If there is an error in any of the field entries, the pointer will move to the invalid field to indicate so. Change the entry to a valid one, then click **Save**, again.

To exit without saving any changes that you made, click **Exit**. A dialog box appears, asking you to confirm that you want to discard your changes. Click **Yes** to confirm and exit; click **No** to return to the Configuration dialog box.

Minimizing the Window

Once all CC1000 services have started successfully, the CC1000 Manager minimizes itself. When the main screen is minimized, an icon representing the CC1000 Manager appears in the Windows system tray, as follows:



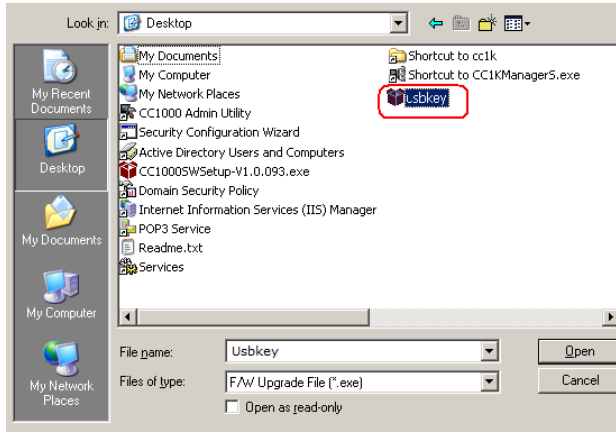
- To restore the main screen, double click the icon.
- To bring up a context menu that allows you to either restore the main screen or exit the program, right click the icon.

Upgrading the USB Authentication Key Firmware

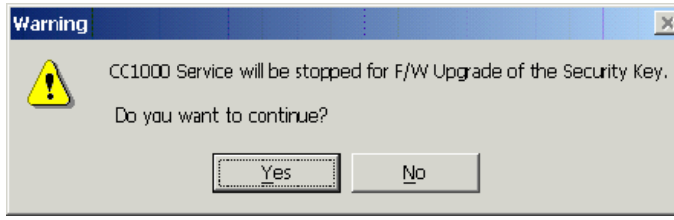
The USB Authentication Key's firmware can be upgraded as newer versions become available. New firmware versions are posted on our Website as they become available. Check the Website regularly to look for the latest versions and information relating to them.

To upgrade the USB Authentication Key's firmware, do the following:

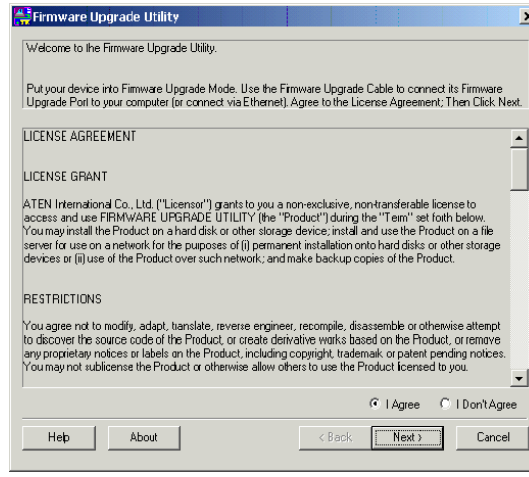
1. From the computer that the CC1000 Manager resides on, go to our Website and download the *usbkey* upgrade package.
2. At the bottom of the CC1000 Manager main screen, click **Security Key F/W Upgrade**.
3. In the dialog box that comes up, navigate to the directory that upgrade package is located in and select it.



4. Click **Open**. The following warning message appears:

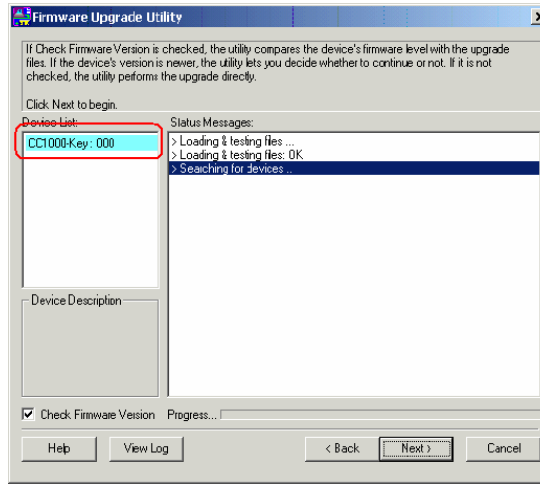


5. Click **Yes**. The License Agreement comes up:



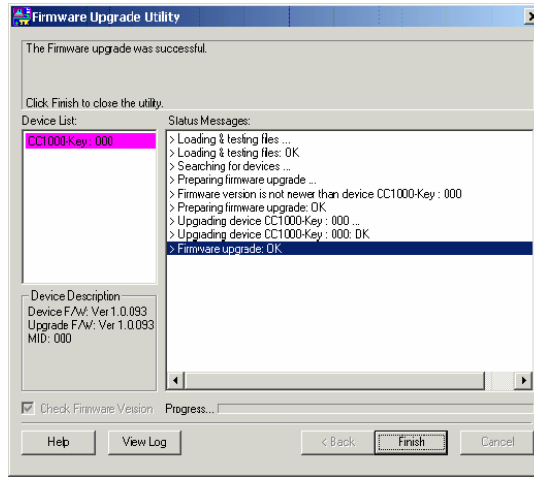
6. Read and agree to the License Agreement (enable the *I Agree* radio button).

7. Click **Next** to continue. The Firmware Upgrade Utility screen appears, with the CC1000 displayed in the *Device List*:



8. Click **Next** to start the upgrade. As the Upgrade proceeds status messages appear in the Status Messages panel, and the progress toward completion is shown on the *Progress* bar.

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



9. Click **Finish** to close the screen. The CC1000 Manager restarts automatically after the upgrade is complete.

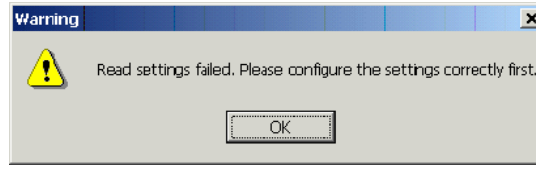
Chapter 11
The Administrator Utility

Introduction

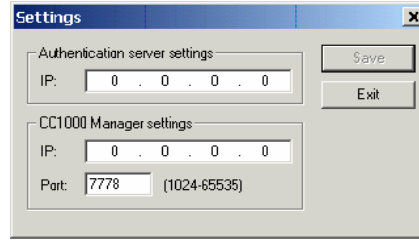
The CC1000 Administrator Utility (CC1KAdmin.exe) is a client utility that allows administrators to manage users and devices in the Active Directory. The utility provides four management functions: device management; user management; group management; and configuration data import/export. All nodes (device, folder, users, and groups) are managed from a tree view. Node-specific context menus can be accessed by right clicking on the node.

Getting Started

1. Double click the Administrator Utility icon on the desktop. If this is the first time that you are running the utility, a *Read settings failed* message appears:



2. Click **OK** to bring up the *Settings* dialog box



(continues on next page)

3. Key the Authentication Server's IP address in the *Authentication Server* settings field; key the CC1000 Manager's IP address in the *IP* field; key the port that the CC1000 Manager listens on in the *Port* field.

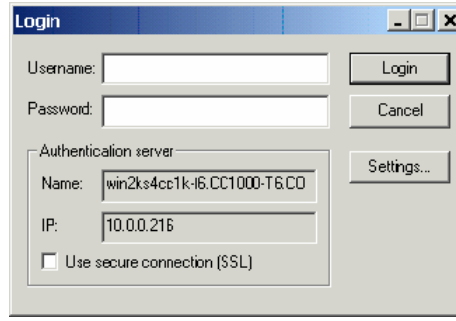
Note: 1. The latter two settings must correspond to the ones specified in the CC1000 Manager's *Configuration Settings* dialog box (see page 133).

2. In the future, you can bring up this dialog box by clicking the **Settings** button on the login page (see the screenshot below).

3. The *Settings* button doesn't appear in the dialog box if the program was obtained by downloading it from the web.

Logging In

After opening the,CC1000 Administrator Utility, a login dialog box (such as the one pictured below) appears.

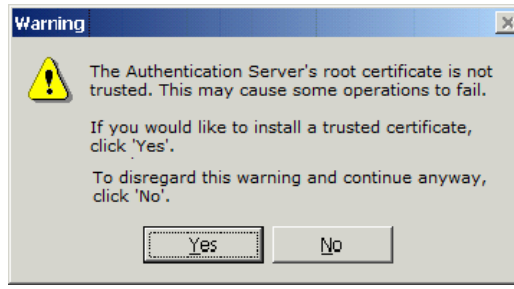


1. Type your Active Directory domain administrator's username and password in their respective fields.
2. To modify the settings for the Authentication Server and CC1000 Server (see *Getting Started*, page 141), click **Settings**.
3. If you would like to enable secure information exchange, select *Use secure connection (SSL)*.

Note: Before you can connect using a secure connection, you must install the root certificate. If you have not yet installed the root certificate on your computer, see *Installing the Root Certificate* in the next section. Otherwise, click **Login**, and skip to *The Main Screen*, page 146.

Installing the Root Certificate

Before you can log in to the Administrator Utility using a secure connection (SSL), a trusted *Authentication Server root certificate* must exist. If there is no trusted root certificate when you try to log in, the following dialog box appears:

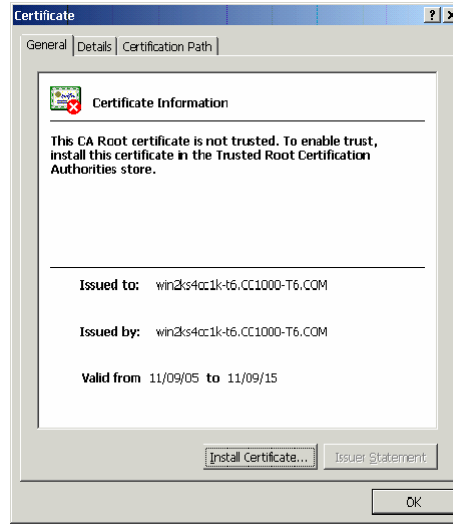


Note: If you don't install the trusted root certificate, you can still use the Administrator Utility to maintain all the data in the AD except you will not be able to set/reset user passwords.

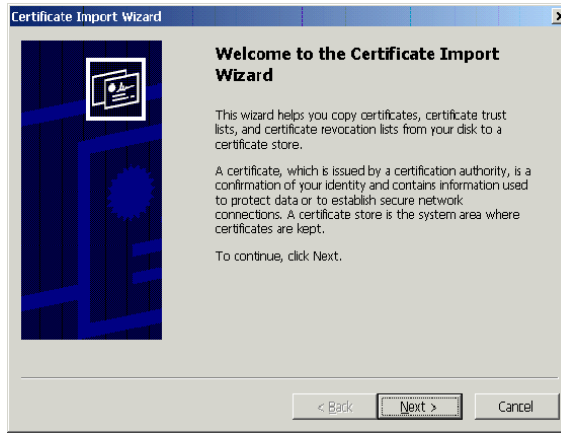
To install the root certificate, do the following:

1. Click **Yes**.

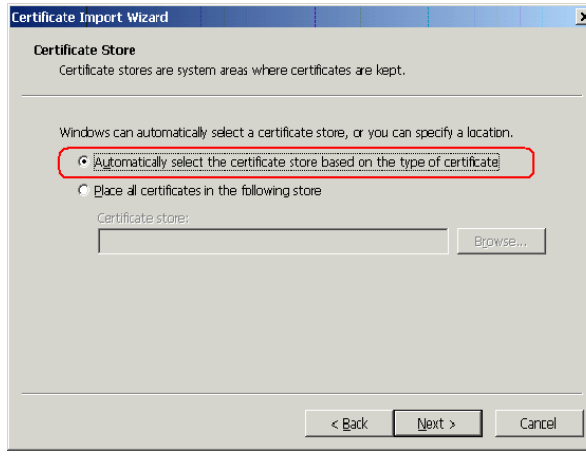
   The *Certificate* dialog box comes up:



2. Click **Install Certificate** to bring up the Certificate Import Wizard:

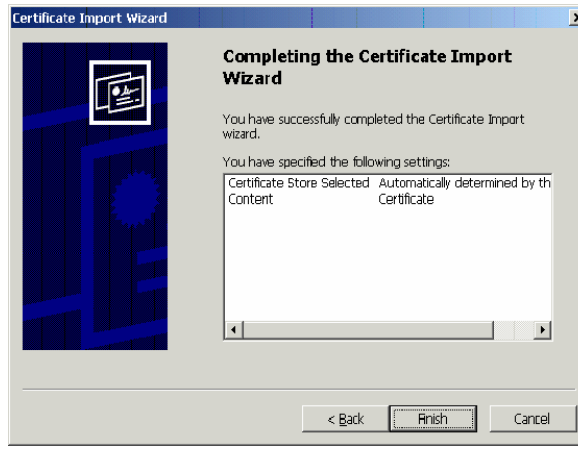


3. Click **Next** to continue. The following dialog box appears:



4. Choose *Automatically select the certificate store...*, then click **Next** to move on.

The following dialog box appears:



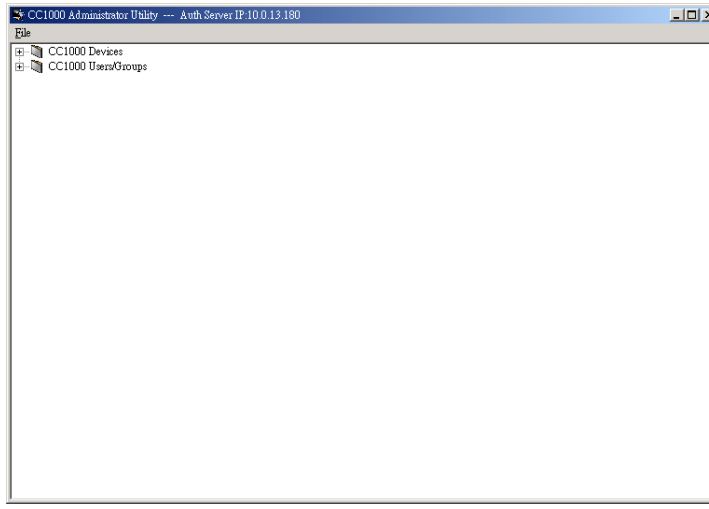
5. Click **Finish** to close the dialog box. A *Security Warning* dialog box comes up:

6. Click **Yes**. A confirmation dialog box appears:

7. Click **OK** to finish up.

The Main Screen

When you run the CC1000 Administrator Utility, the main screen appears, showing the Devices, and Groups/Users root nodes:



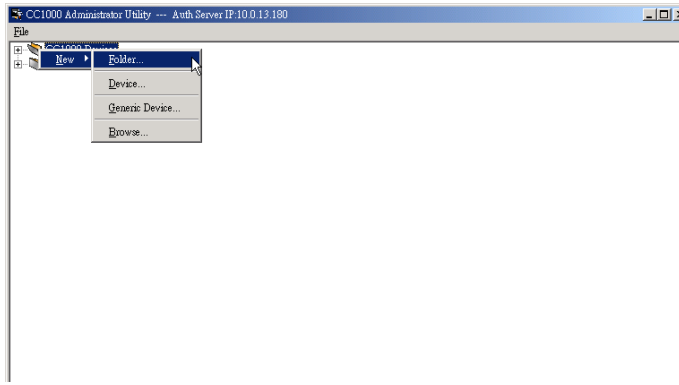
Devices, Users, and Groups are configured and managed from this screen. The first time you run the utility, except for a *Super Administrator* installed under the *Users* node, there are no device folders, devices, users, or groups listed under the root nodes. The following sections describe how to use the CC1000 Administrator Utility to create and manage Devices, Users, and Groups.

Device Management

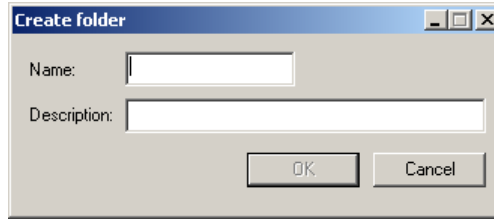
Creating Device Folders

Device folders allow you to organize your enterprise-wide devices into useful categories (location, department, etc.). To create a device folder, do the following:

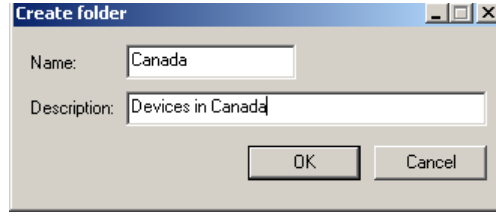
1. Right click on the *CC1000 Devices* folder.
2. In the pop up menu that appears, select New → Folder.



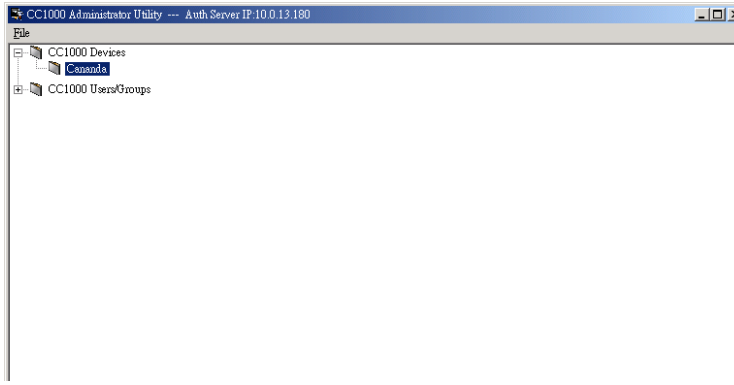
3. The *Create folder* dialog box appears.



4. Enter a name and a description for the folder.



5. Click **OK**. The folder appears as a subfolder of the CC1000 *Devices* root node:



Adding Devices

Devices are added to the device folders that are appropriate for them. For example, you would create a device node for a PN9108 that was in Canada, in the *Canada* device folder.

Note: You can nest device folders. For example, you could have a Vancouver device folder and a Toronto device folder as sub folders under the Canada folder.

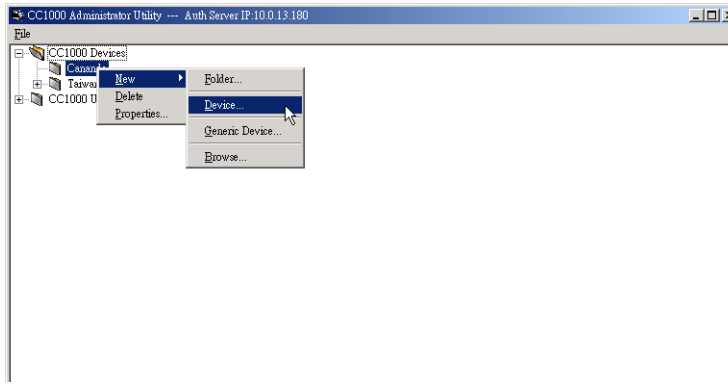
There are two methods to add a device node. The first is to manually add the device. The second is to use the CC1000 Manager to browse the device list.

Browsing the device list (see page 151), is the simplest way to add a device to a folder, because the device provides information about itself, such as its name, type, and MAC address. In this way, you ensure the accuracy of the device information and save the time normally required to gather and type in the information.

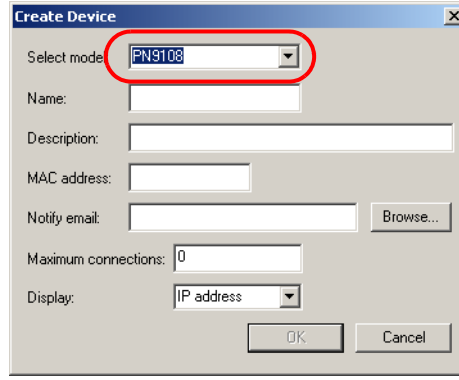
Adding Device Nodes Manually:

To manually add a device node, do the following:

1. Right click on the folder node that you want to add the new device node to.
2. In the pop up menu that appears, select New → Device.



3. In the dialog box that appears, drop down the *Select Model* list and select the device type that you want to add:



Note: In this example we are adding a PN9108. The procedure for adding other devices is the same.

4. Enter a name, description, and MAC address for the device in the appropriate fields.

5. Enter an email address for the person that the device will send messages to when important events (such as SNMP traps) occur in the *Notify email* field.

Note: 1. This step is optional.

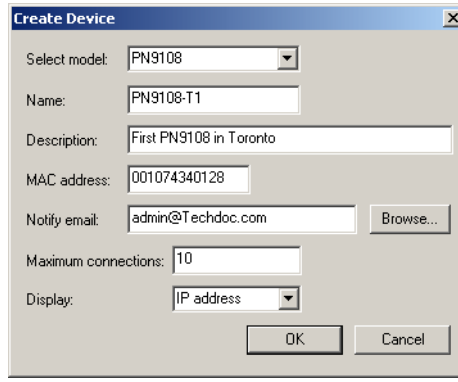
2. You can use the *Browse* button to select the address from a list of users rather than inputting the address manually. See *Email*, page 158 for details.

6. Specify the maximum number of simultaneous connections to the device that you want CC1000 to allow.

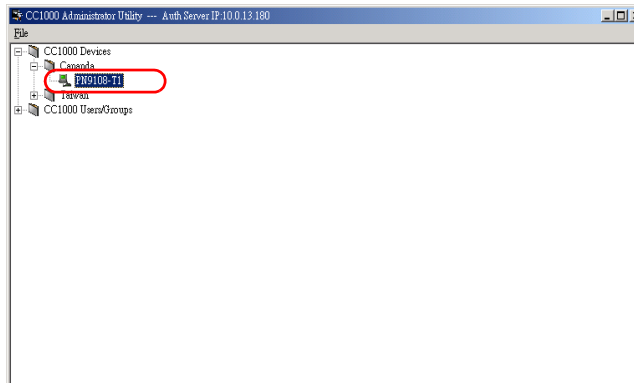
Note: 1. A number of 0 (zero) means unlimited connections (up to the maximum number of connections set in the device, itself).

2. If the number specified here is greater than number of connections allowed by the device itself, the number allowed by the device takes precedence over this number. More connections than the ones allowed by the device will not be accepted.

7. Select whether the device name or IP address appears when users log in via their browsers. As a security precaution, selecting the device's name keeps its IP address from being visible under the *Operation Notes* in the browser screen's main panel.



8. Click **OK**. The new device node is created and submitted to Active Directory.



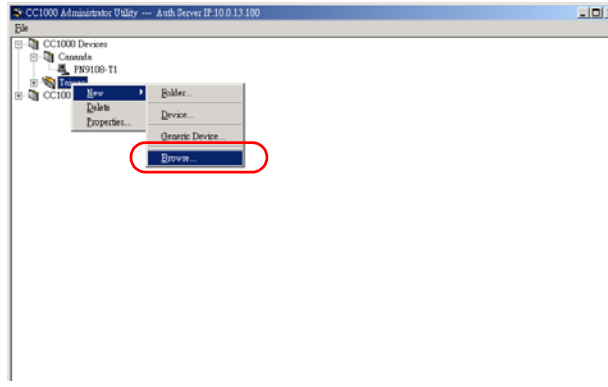
Adding Device Nodes by browsing:

Browsing is the most convenient way to add devices, since most of the device information is automatically inserted, rather than having to be keyed in.

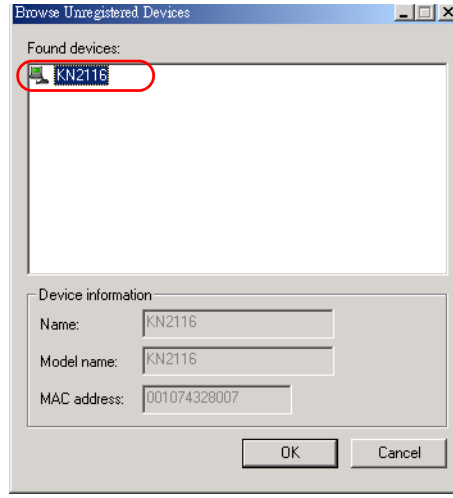
Note: Devices to be added by browsing must be powered on and have CC management enabled and configured in their settings.

To add a device node by browsing, do the following:

1. Right click on the folder node that you want to add the new device node to.
2. In the popup menu that appears, select New → Browse:



3. In the *Browse unregistered device* dialog box that appears, select the device you want to add from the *Found device* list, then click **OK**.



4. In the dialog box that appears, the *Model Name* and *MAC address* fields are already filled in.
5. Give the device a more descriptive name, and fill in the *Description* field, if you like.
6. Enter an email address for the person that the device will send messages to when important events (such as SNMP traps) occur on it in the *Notify email* field.

Note: 1. This step is optional.

2. You can use the *Browse* button to select the address from a list of users rather than inputting the address manually. See *Email*, page 158 for details.

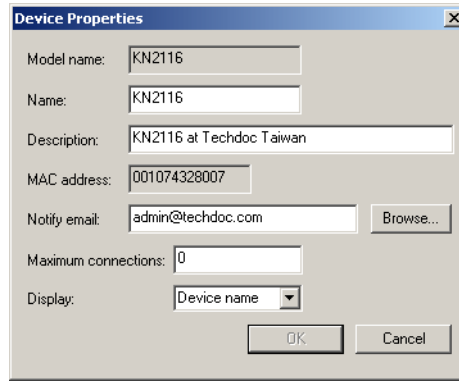
---

7. Specify the maximum number of simultaneous connections to the device that you want CC1000 to allow.

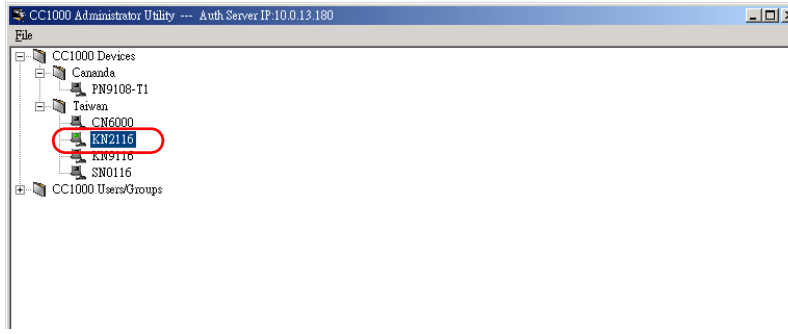
Note: 1. A number of 0 (zero) means unlimited connections (up to the maximum number of connections set in the device, itself).

2. If the number specified here is greater than number of connections allowed by the device itself, the number allowed by the device takes precedence over this number. More connections than the ones allowed by the device will not be accepted.

8. Select whether the device name or IP address appears when users log in via their browsers. As a security precaution, selecting the device's name keeps its IP address from being visible under the *Operation Notes* in the browser screen's main panel.



9. Click **OK** to finish up. The device is added to the folder:



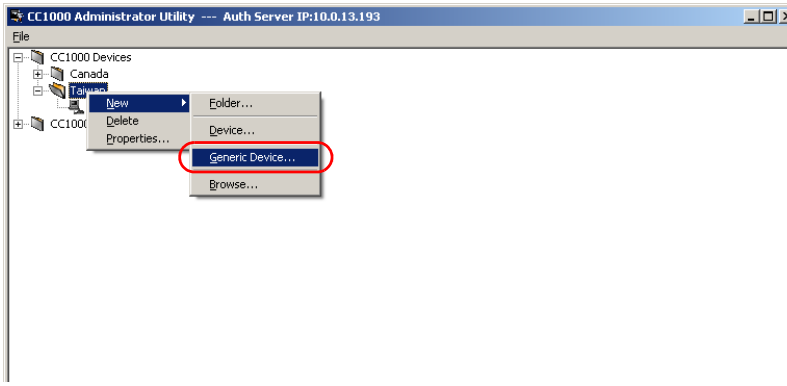
Adding Generic Device Nodes:

The CC1000 supports the creation of a *Generic* device type. This refers to a device that is not part of the Aten / Altusen *On the Net*™ / *Over the Net*™ line of products.

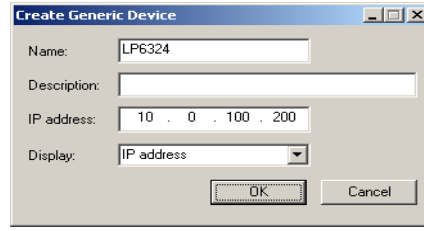
Since generic devices have no provision for CC management support, they cannot be added by browsing, and they cannot be authenticated through the CC1000. Although they can be accessed through the CC1000, you must log in to them with their own Username/Password authentication procedure.

To add a generic device node, do the following:

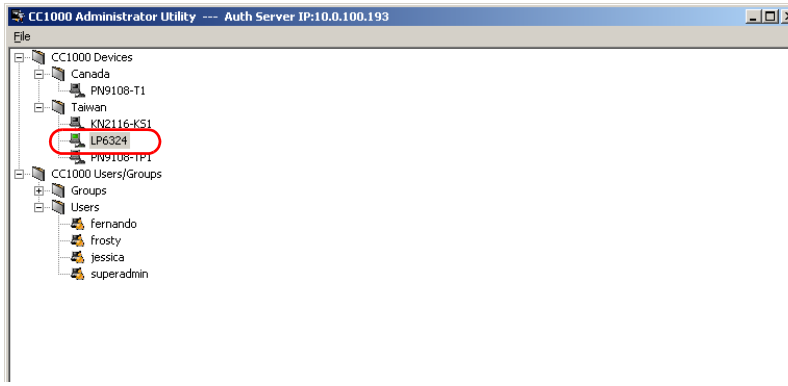
1. Right click on the folder node that you want to add the new device node to.
2. In the popup menu that appears, select New → Generic Device:



3. In the dialog box that appears, key in a name and description (optional) for the device. Select whether the device name or IP address appears when users log in via their browsers. As a security precaution, selecting the device's name keeps its IP address from being visible under the *Operation Notes* in the browser screen's main panel.



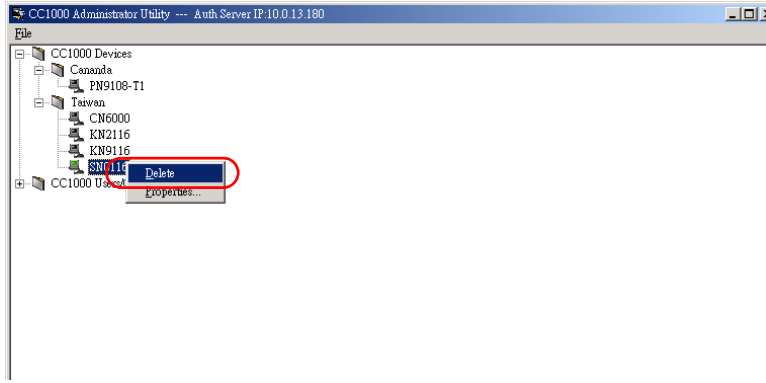
4. Click **OK** to finish up. The device is added to the folder:



Deleting Device Nodes

With the exception of the *CC1000 Devices* root folder node, all folder and device nodes can be deleted by doing the following:

1. Right click on the node you want to delete. A popup menu similar to the one below appears:



2. Click **Delete** to remove the folder/device.

Note: When you delete a folder node, all subfolders and device nodes contained in it are also deleted.

Moving Folder/Device Nodes

Folders and devices can be moved to other folders by dragging and dropping.

Folder/Device Node Properties

To view and/or edit the properties of any folder or device node, right click on the node and click **Properties** on the popup menu that appears.

User Management

The CC1000 Administrator Utility allows administrators to create, delete and modify users and user attributes.

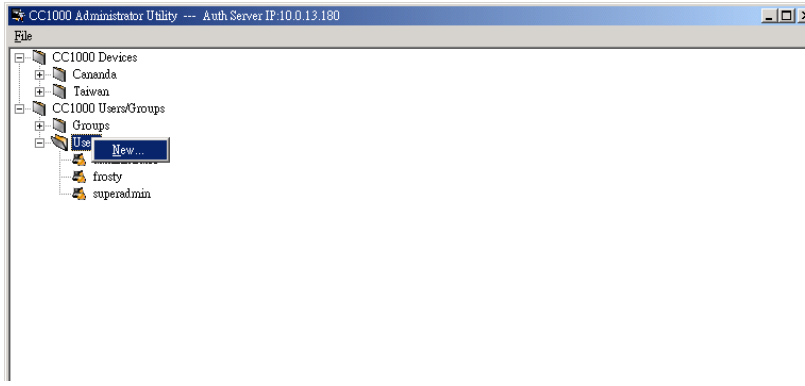
Note: The Administrator Utility comes with a pre installed *superadmin* (super administrator) account. This account can be used to download the Administrator Utility via browser to a remote site for remote administration purposes. See *Download Administrator Utility*, page 161, and *Download*, page 185, for details).

The Username for this account is *superadmin*; the password is *CC1KPassword*. The password is case sensitive. For security purposes, we strongly recommend changing the password to something unique.

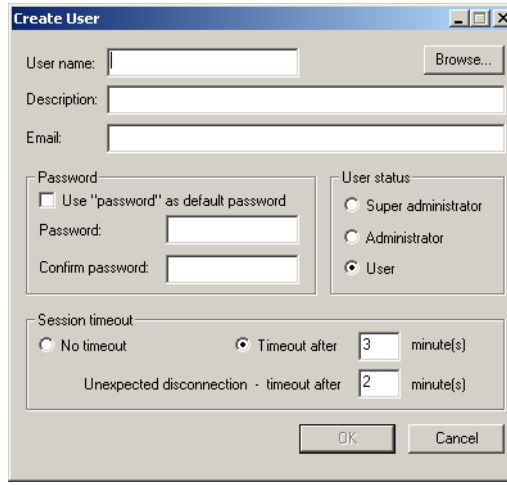
Adding Users

To add a user, do the following:

1. Expand the *CC1000 Users/Groups* folder (click the plus sign).
2. Right click on the *Users* folder. In the pop up menu that appears, click **New**:



3. The *Create User* dialog box appears.



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

Field	Description
User name	Enter a username here.
Description	Additional user information you may wish to include.
Browse	The information for the User name and Description fields can be filled in automatically by clicking Browse and selecting the user from a list of users registered in AD.
Email	The user's email address. If the email address is entered here, it will show up in a device's *Notify email* list. (See *Adding Device Nodes Manually:*, page 149).
Use "password" as default password	Selecting this sets "password" as the user's password.
Password	You must set the password unless you select *Use "password" as default password*. **Note:** The password must match the Authentication Server's password policy (see *Password Setup*, page 93)
Confirm password	To be sure there is no mistake in the password you are asked to enter it again. The two entries must exactly match.

(Continues on next page.)

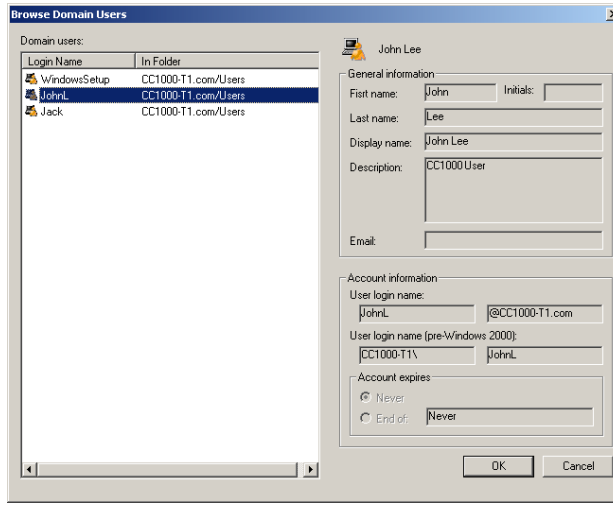
(Continued from previous page.)

Field	Description
User status	There are three categories: Super Administrator, Administrator and User (see page 161 for details). There is no limitation on the number of accounts that can be created in each category. **Note:** 1. The Super Administrator is not allowed to access devices from a browser login to the CC1000. 2. If the User status you want to choose is already selected, click to select it again to bring up the *User Type Options* dialog box.
Session timeout	1. If there is no online device connected to the CC1000, and there is no operator input for the amount of time specified here, the CC1000 session is ended. The Super Administrator timeout interval is from 1–1440 minutes; default is 3 minutes. The timeout interval for Administrators and Users can either be 1–1440 minutes or no timeout; default is 3 minutes. 2. If an operator is connected to a device and that device has its own timeout interval, the CC1000 time-out interval won't begin until the operator is first timed out of the device session.
Unexpected disconnection timeout	If the user unexpectedly disconnects (i.e. closes the browser), the CC1000 times out the user's session after the amount of time specified here. The timeout interval is from 2 - 10 minutes; default is 2 minutes.

(Continues on next page.)

(Continued from previous page.)

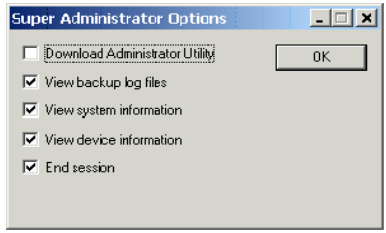
Note: If you click the Browse button (see *Browse*, page 158), to add the Username and Description, a *Browse Domain Users* dialog box appears:

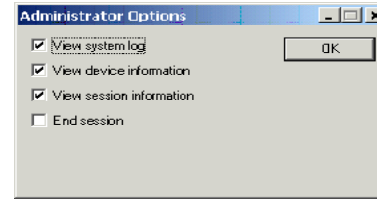


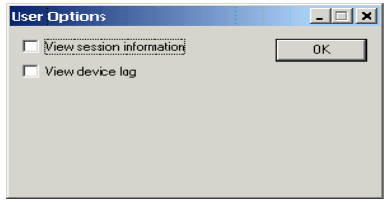
1. Select the user in the *Domain Users* column. The user's information displays in the fields to the right of the column.
2. Click **OK**

4. Click one of the *User Status* options that is appropriate for the User.

   Depending on the *User status* that you selected in the *Create User* dialog box, one of the following *User Options* dialog boxes appears.







A description of the options is given in the table, below:

Option	Description
Download Administrator Utility	This option allows a Super Administrator to download the Administrator Utility executable file from the CC1000 Servers site. The Administrator Utility can run as an independent module on Windows 2000 and higher systems.
View backup log files	Selecting this option allows the Super Administrator to view and query the backup log files.
View system information	Selecting this option allows the Super Administrator to view system information – such as the number of Licenses and Connections available to the system.
View device information	Selecting this option allows the Super Administrator to view information for all online devices on the installation. Administrators can view information for the online devices that they have access rights to.
End session	Selecting this option allows the Super Administrator to end Administrator and User CC1000 sessions. Administrators can end User CC1000 sessions.

(Continues on next page.)

(Continued from previous page.)

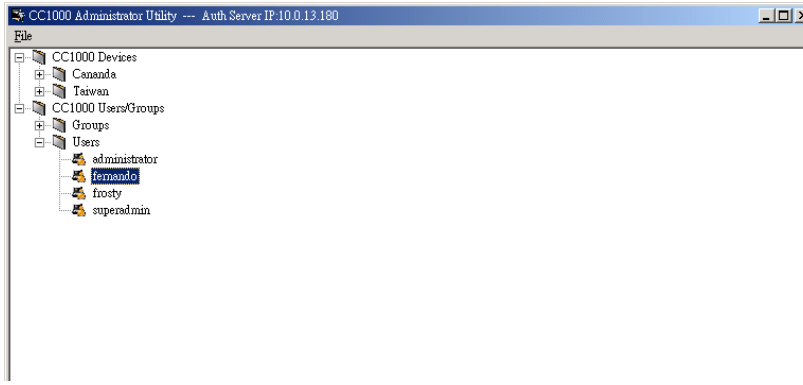
Option	Description
View system log	Selecting this option allows the Super Administrator or Administrator to view and query the system log files.
View session information	Selecting this option allows the Super Administrator, Administrator, or User to see information regarding the sessions currently taking place online.
View device log	Selecting this option allows the Super Administrator, Administrator, or User to view and query the device logs for the devices they have access rights to.

Note: 1. *View system log*, *View session information*, and *View device log* are the defaults for the Super Administrator; *View device log* is the default for Administrators.

2. See *Main Page Links*, page 184 for screenshots and more details regarding these selections.

5. Place a check in the boxes to enable the options that you want to allow, then click **OK**.

6. When you return to the *Create User* dialog box, click **OK**. The new user is added to the *Users* folder.



7. Repeat steps 2–6 for each new user you want to add.

Deleting Users

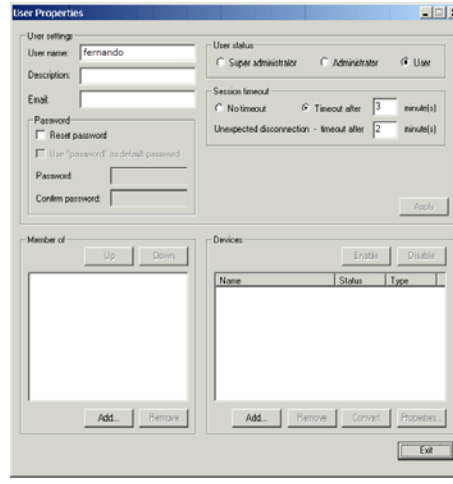
To delete a user, do the following:

1. Navigate to the *Users* folder (CC1000 Users/Groups → Users) and right click on the username.
2. When the pop up menu appears, click **Delete**.

Managing Users

User accounts are managed through the *User Properties* dialog box:

1. Navigate to the *Users* folder (CC1000 Users/Groups → Users) and right click on the name of the user whose properties you want to access.
2. In the menu that pops up, click **Properties**. The *User Properties* dialog box appears.



- With the exception of *Reset password* (discussed below), the upper dialog box fields are similar to the ones discussed under the *Adding Users* section, page 157.
- The *Member of* panel lets you add the user to a group. See *Group Management*, page 164 for details.
- The *Devices* panel lets you assign devices to the user. See *Device Assignment*, page 170 for details.

3. To modify a user's properties, make the desired changes in each of the panels. When all changes have been made, Click **OK**.

Resetting Passwords:

To reset a user's password, do the following:

1. In the *User Properties* dialog box check **Reset password**. This enables the *Password* fields.
2. Enter the new password; then enter it again to confirm it. (Refer back to *Adding Users*, page 157, for password information, if necessary.)
3. Click **OK** to finish.

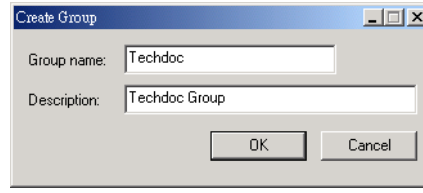
Group Management

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 those devices.

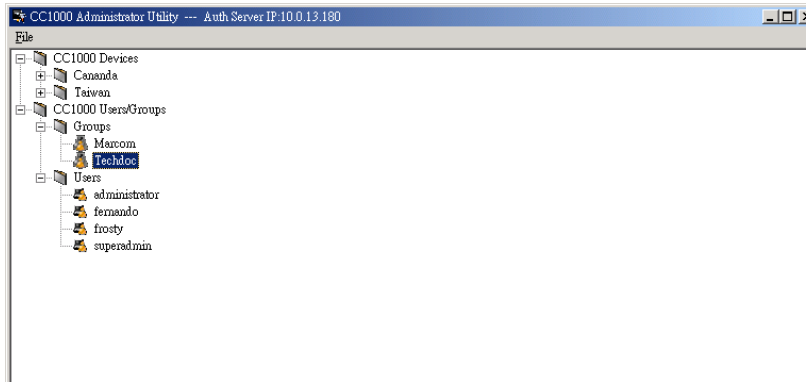
Creating Groups

To create a group, do the following:

1. From the CC1000 Administrator Utility main screen, navigate to the *Groups* folder (CC1000 Users/Groups → Groups).
2. Right click the *Groups* folder.
3. In the pop up menu that appears, choose **New**.
4. In the *Create Group* dialog box that appears, enter a group name and description, then click **OK**.



5. The new group is added to the *Groups* folder node.



Deleting Groups

To delete a group, do the following:

1. From the CC1000 Administrator Utility main screen, navigate to the *Groups* folder (CC1000 Users/Groups → Groups).
2. Right click on the Group's name.
3. In the pop up menu that appears, choose **Delete**. The group is automatically removed.

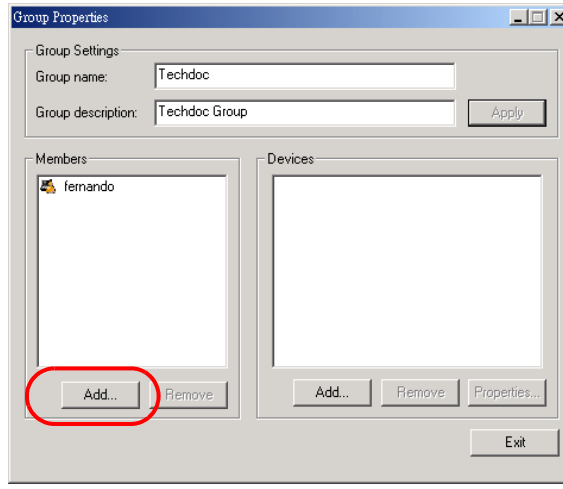
Adding Users to Groups

Note: Before you can add users, you must first create them. See *User Management*, page 157 for details.

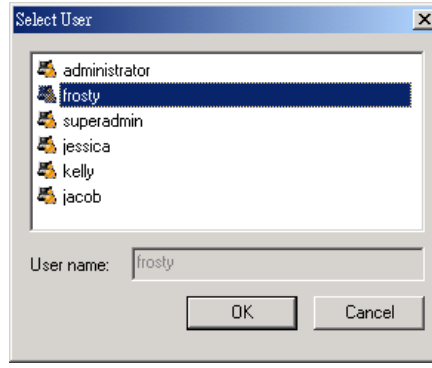
To add a user to a group, do the following:

1. Navigate to the Groups folder (CC1000 Users/Groups → Groups), and right click on the name of the group that you want to add a user to.
2. In the pop up menu that appears, choose **Properties**.

3. In the *User Group Properties* dialog box that appears, go to the bottom of the *Members* panel and click **Add**

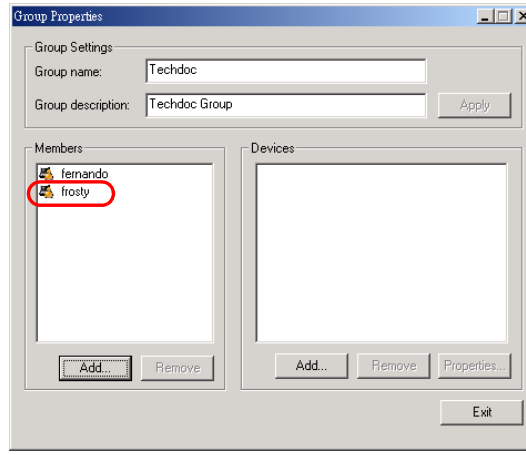


4. In the *Select User* dialog box that appears, select the user you want to add to the group from the list of users.



(Continues on next page.)

5. Click **OK**. The user is added to the group's *Members* list.



6. Click **Exit** to close the dialog box.

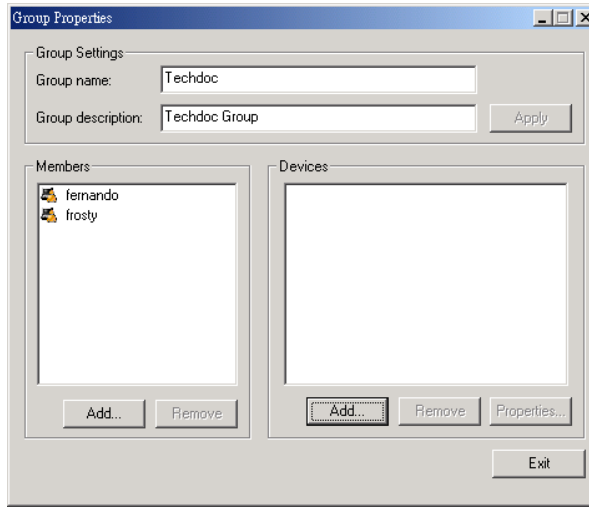
Removing Users from Groups:

To remove a user from a group, select the group in the *Member of* panel, then click **Remove**.

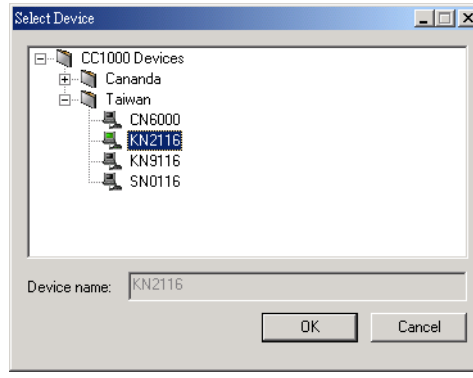
Adding Devices to Groups

To add a device to a group, do the following:

1. Open the *User Group Properties* dialog box. (See *Adding Users to Groups*, page 165.)
2. At the bottom of the *Devices* panel, click **Add**.

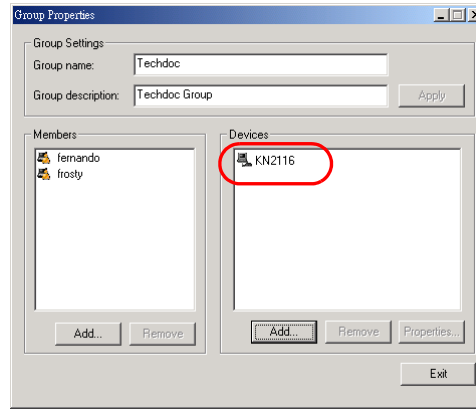


3. Select the device that you want to add to the group.



4. Click **OK**.

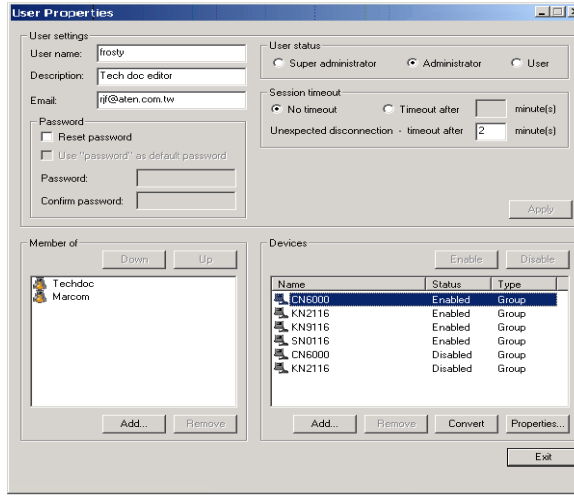
5. In the *Access Configuration* dialog box that appears, set the access rights for the device. (See *Device Access Rights*, page 172 for information about *Access Configuration* dialog boxes.)
6. The device is added to the group's *Devices* list.



7. Click **Exit** to close the dialog box.

Device Assignment

All devices that a user accesses privately, or through a group, are listed in the *Devices* panel of the *User Properties* dialog box:



Device Panel Headings

The headings at the top of the Device panel are described in the table, below:.

Heading	Description
Name	Lists the name of the device.
Status	Indicates whether the device is set as enabled or disabled. If it is set as enabled, it shows up in the user's tree view. If it is set as disabled, it doesn't show up in the user's tree view – even though it is on line. The administrator can use this function to temporarily deny a user access to a device without having to delete it and then reinstall it.
Type	Indicates whether the device is accessed privately or as part of a group.

Device Button Functions

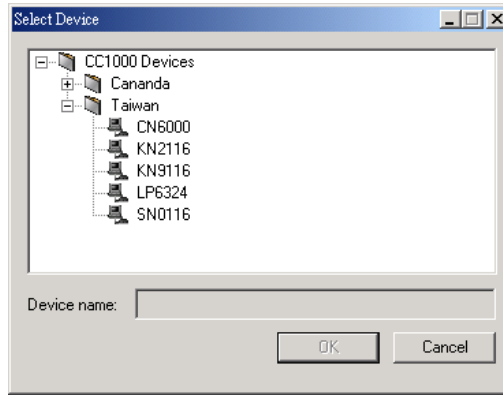
The functions of the buttons associated with the panel are described in the table, below:

Heading	Description
Enable	Highlight a device in the list box and click **Enable**, to allow the user to access the device. This function only works for devices that are accessed privately.
Disable	Highlight a device in the list and click **Disable**, to disable user access to the device. This function only works for devices that are accessed privately.
Add	Allows the administrator to add devices to the list of devices that a user can access.
Remove	Highlight a device and click **Remove**, to remove a device from the list. This function cannot be used to remove a device that the user accesses through a group.
Convert	This function converts a device that is accessed through a group to device that is personal to the user. To convert a *group* device in the list to a *personal* one, select it and click **Convert**. The status of the new, personal, device is **Enabled**; the status of the old group device is now **Disabled**. If the private device is removed, however, the status of the original group device automatically reverts to being **Enabled**. **Note:** A personal device cannot be converted to a group device.
Properties	To view and change device properties, select the device and click **Properties**,. **Note:** Properties of devices belonging to groups can only be viewed, not changed.

Device Access Rights

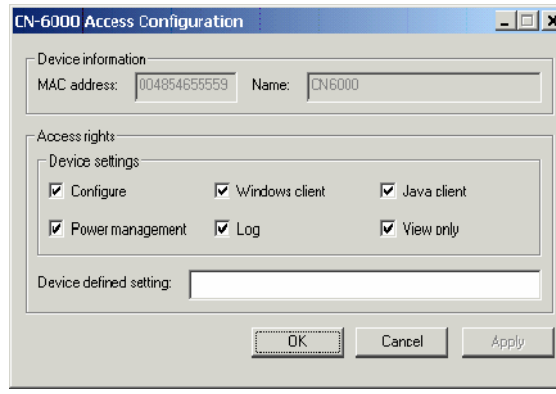
Before a user can access a device, access rights to the device must first be granted. To grant a user access rights to a device, do the following:

1. Open the *User Properties* dialog box (see page 163).
2. In the *Devices* panel, click **Add**.
3. When the *Select Device* dialog box appears, Select the device that you want to grant the user access to, then click **OK**.



Note: You may have to expand the folders to get to the device.

An *Access Configuration* dialog box that allows you to set user access permissions for the device appears:



Note: 1. The screenshot shows a dialog box for the CN-6000. Each Administrator Utility device has its own *Access Configuration* dialog box. The makeup of the dialog boxes vary, reflecting the device's function. Refer to each device's User Manual for information about setting its user access rights.

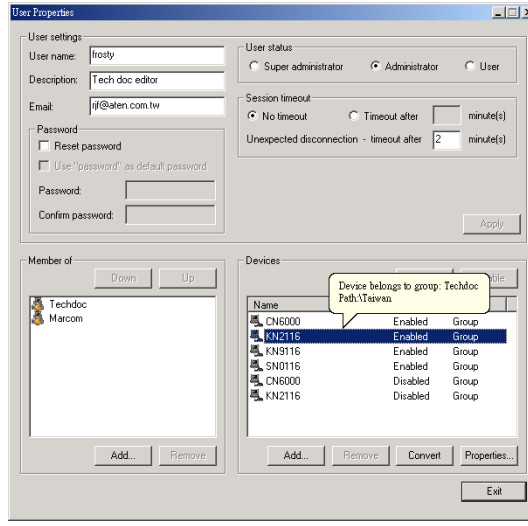
2. The CC1000 supports the creation of a *Generic* device type (a non-Administrator Utility product), such as the LP6324 in the screenshot on page 172. This type of device doesn't have an *Access Configuration* dialog box.

3. The *Device defined setting* field is reserved at the current time, and should be left blank. It may be given a particular function in future versions.

Group Membership

If a user is a member of more than one group and each group has access to the same device, the device's name will appear more than once in the *Devices* panel. Only the first entry of the device is enabled, however. Users are only able to access the device from the group that the first instance of the device is pointing to.

To ascertain which group a device is pointing to, hover the mouse pointer over the device's name in the *Devices* list. The balloon that appears displays which group (if any), the device points to – as shown in the screen, below.



In order for a user to access the device, the group that it points to must have first priority.

The group at the top of the list has the highest priority; the second in the list has second priority, etc. To change a group's priority, do the following:

1. In the *Member of* list, select the group that you want to change.
2. Click **Down** to move it lower in the list (and thereby decrease its priority); click **Up** to move it higher in the list (and thereby increase its priority).

Note: Devices for which there is only one entry, or that are accessed privately, are always enabled. They do not need to be prioritized.

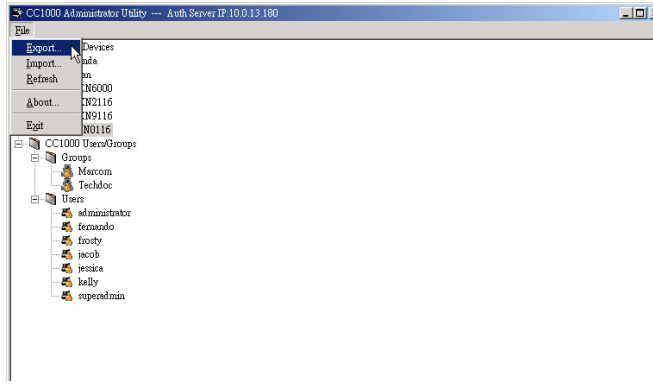
Export / Import Configurations

The Administrator Utility can export CC1000 user and device configurations contained in Active Directory to a file. It can also import CC1000 user and device configurations from previously generated configuration files and incorporate the data into Active Directory.

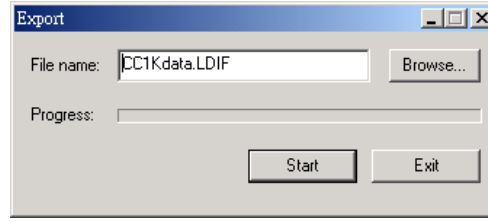
Exporting Configurations

To export configurations to a file, do the following:

1. From the CC1000 Administration Utility *File* menu, choose **Export**.



The Directory Export dialog box appears.



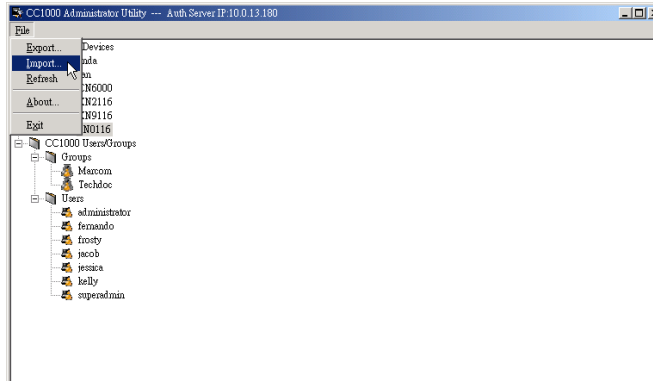
2. Key in a filename for the output configuration file, then click **Start**. The configurations are exported to the specified file.

Note: By default, the file is saved in the *\CC1KSoftware\CC1KApp* folder., but you can key in, or browse, to a different folder.

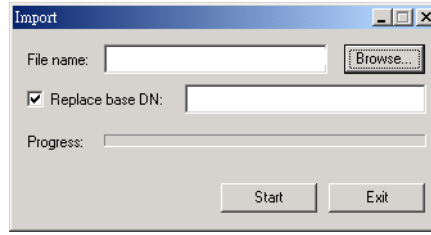
Importing Configurations

To import configurations from a file, do the following:

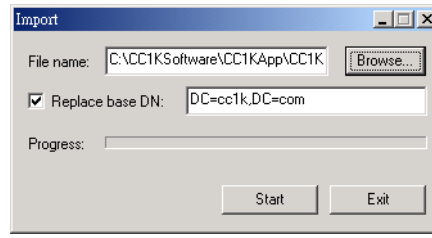
1. From the CC1000 Administration Utility *File* menu, choose **Import**.



The *Import Directory* dialog box appears.



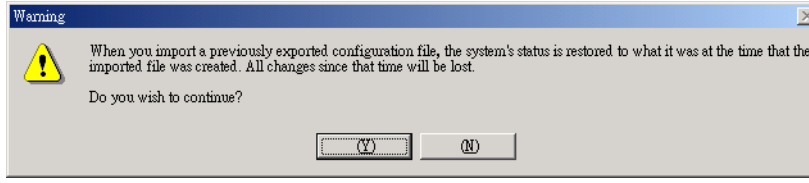
2. Key in, or browse to, the path and filename where the import file is located. If the file was originally exported by the Administration Utility, its DN (Domain Name) configuration data appears in the text box to the right of the *Replace base DN* entry.



3. Choose whether to enable or disable the *Replace base DN* entry.
   - By default, the *Replace base DN* checkbox is enabled. That means that the import file's DN configuration data (the entries in the text box to its right), will be replaced by the AD's DN configuration.

     If you are importing a file that was not created by exporting it from this Administrator Utility (running on this computer), you must key in this computer's DN configuration in the text box.
   - If the *Replace base DN* checkbox is not enabled, only the data in the import file that matches the Active Directory DN will be imported.
4. Click **Start**.

   A cautionary message appears:



5. Click **Y** to import the configuration file's information; click **N** to abort the operation.

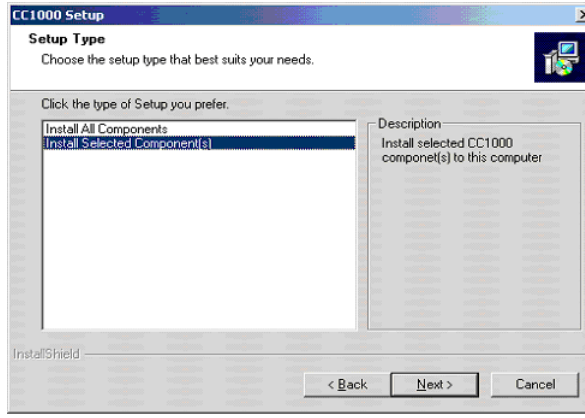
After the file is successfully imported, a message appears on screen to inform you of the fact.

Additional Installation Options

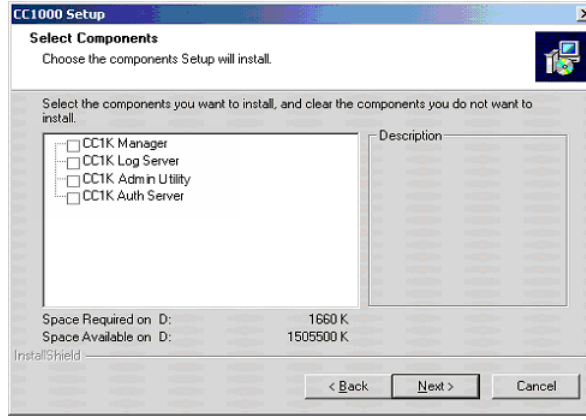
Installing the Administrator Utility Separately

In the previous sections, it has been assumed that you are installing all of the CC1000 components on the same host. The Administrator Utility can be installed and run separately on a stand-alone host, however. To install the Administrator Utility separately, do the following:

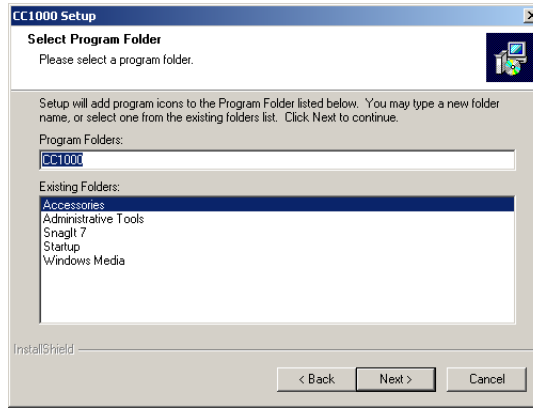
1. Follow steps 1-5 in the *Installation* chapter for installing the CC1000 (see *Installation*, page 107). The following screen appears:



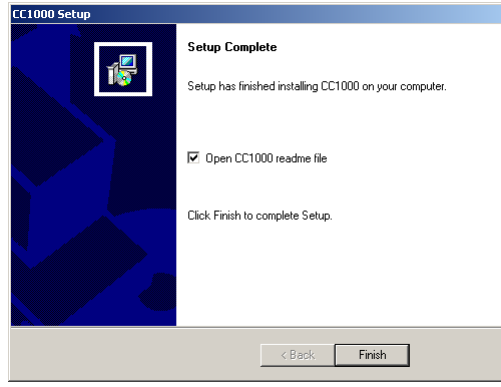
2. In the list box, select *Install Selected Components*, then click **Next**. The following screen appears:



3. In the list, select *CC1K Admin Utility*, then click **Next**. The following screen appears:



4. Click **Next**. The following screen appears to indicate that the stand alone installation of the Administrator Utility installed successfully:



This Page Intentionally Left Blank

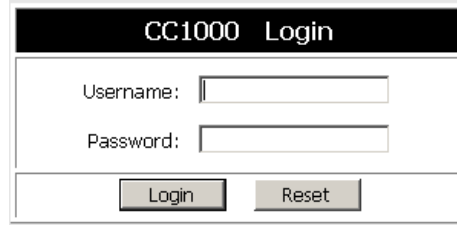
Chapter 12
Browser Operation

Devices on a CC1000 installation are accessed from a browser based GUI. Only a single login to the CC1000 Server is required to access any of them. An expandable tree view lets you locate and access any device on the entire installation - no matter where in the world - with just a few clicks of the mouse.

Logging In

To log into the CC1000, do the following:

1. Open the browser and specify the IP address of the CC1000 in the browser's URL location bar.
2. When the Security Alert dialog box appears, accept the certificate – it can be trusted. (See *Trusted Certificates*, page 200, for details.) The Login page appears:



3. Provide your CC1000 Username and Password, then click **Login**.

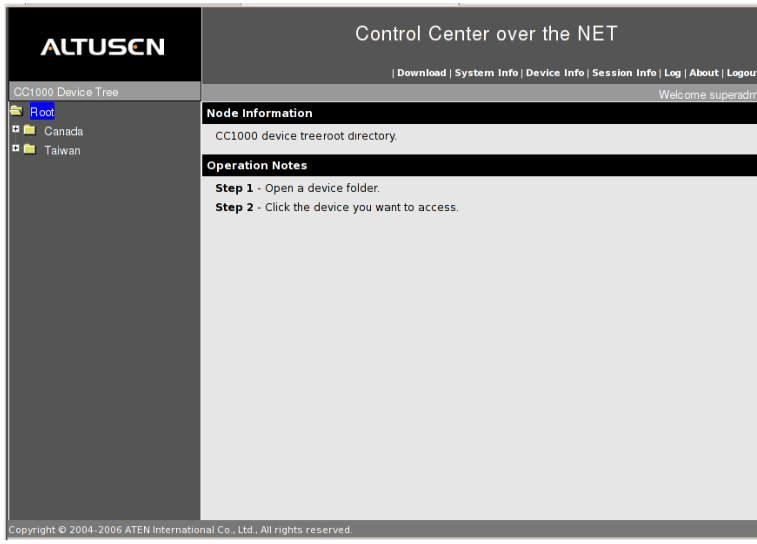
   If this is the first time you are logging in, or your password was reset, a dialog box comes up for you to set up your password again. Reenter and confirm your password. You can keep your original password if you like.

Note: 1. The CC1000 provides a limited number of login licenses. If no licenses are available, a window informing you that there are no more licenses available appears instead of the login screen.

2. If a message saying that the *CC1000 Service is not available*, make sure that the CC1000 Manager is running and that its settings are correct.
3. The CC1000 supports multiple logins for Administrators and Users; Super Administrators are restricted to a single login.

Main Page Layout

After you have successfully logged in, the CC1000 Main Web Page appears:

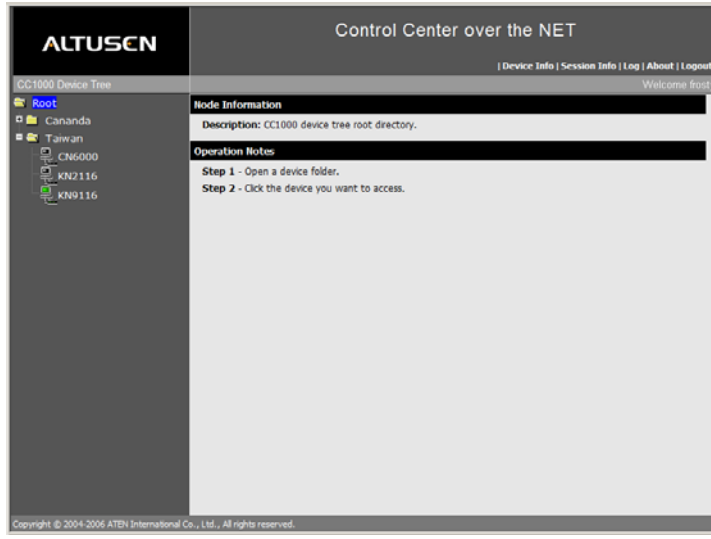


The CC1000 Main Page is divided into three major sections: a left panel; a right panel; and a row of links at the top.

- The left panel displays a tree view of all the device folders on the installation that the user is authorized to access. The Tree View is discussed in the next section.
- The main panel provides information about the node in the Device Tree that is currently selected.
- Clicking a link on the row at the top, brings up additional screens. The number and type of links displayed, are determined by the user's type (Super Administrator, Administrator, User) and the options selected when the user was created. The links are discussed in the *Main Page Links* section, page 184.

Tree View

- Only devices the user is authorized to access are listed in the Tree View (See *Device Access Rights*, page 172 for details.)
- A plus (+) sign in front of a folder means that there are items nested inside of it. Click the plus sign to expand the view and show the nested items.
- To access a device, navigate through the folders to select it. A screen similar to the one below appears:



- If the device is on line, its icon lights green, and its IP address appears under the *Operation Notes* heading in the main panel when you select it.
- Usually, there are two choices available to access a device:
  - Accessing it directly and logging in manually
  - Accessing it via the CC1000 – which doesn't require another log in.

  If the device cannot be accessed directly, however, only the CC1000 access method appears.
- Click the IP address to bring up a new browser window with the device's web page displayed.

Note: The device must be configured to operate with the CC1000, or its status will be displayed as *Off Line*. Refer to the device's User Manual for information on how to configure and operate it.

Main Page Links

Overview

Clicking a link on the main page's top row at the top, brings up additional screens. The number and type of links displayed, are determined by the user's type (Super Administrator, Administrator, User) and the options selected when the user was created.

The table below shows the relation between the User Type and link type:

Link	Accessible By	Access
Download	Super Administrator	Optional
System Info	Super Administrator	Optional
Device Info	Super Administrator	Optional
	Administrator	Optional
Session Info	Super Administrator	Default
	Administrator	Optional
	User	Optional
Log (System)	Super Administrator	Default
	Administrator	Optional
Log (Device)	Super Administrator	Default
	Administrator	Default
	User	Optional
Log (Backup)	Super Administrator	Optional
About	All	Default
Logout	All	Default

- If a link is designated as *Default*, it is always available on the web page.
- If a link is designated as *Optional*, it is only available if it has been selected as an option in the user's configuration.
- For further details regarding configuration of User Types, see *User Management*, page 157.

Each link is explained in detail in the sections that follow.

Download

Download provides a way for the Super Administrator to download the Administrator Utility executable file from the CC1000 Web Server – thereby allowing the Super Administrator to manage the CC1000 from anywhere on the Internet.

Note: The operating system that the Administrator Utility runs on must be Windows 2000 or higher.

To download and run the Administrator Utility, do the following:

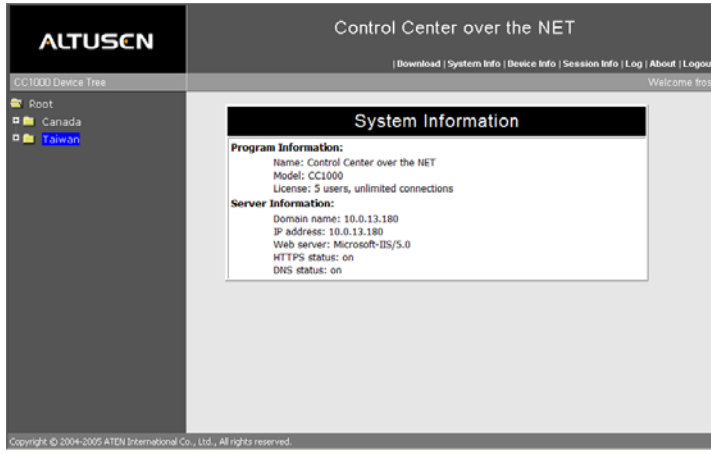
1. Click the **Download** link. The following screen appears:

2. Click the *CC1KAdmin.exe* link.
3. When the confirmation screen comes up, click **Save**.
4. In the dialog box that comes up, pick a location on your computer to save the file to.
5. To run the program, navigate to the directory where it resides, and double click the program icon.

See Chapter 11, *The Administrator Utility* for details on using the program.

System Info

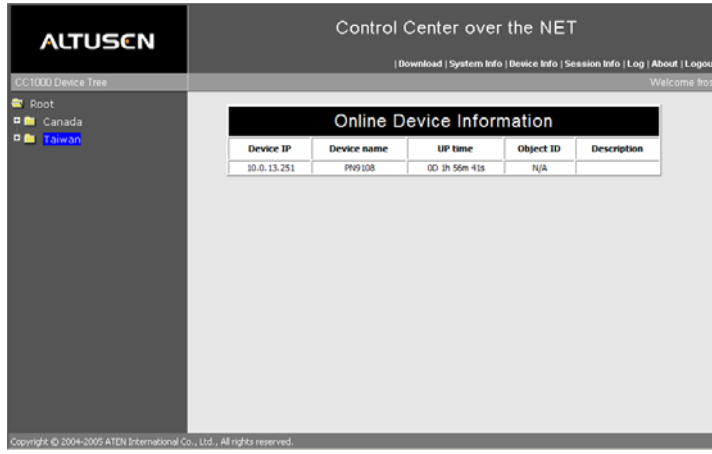
When the Super Administrator clicks the *System Info* link, a screen, similar to the following appears:



System Info shows system information – such as the number of Licenses and Connections available to the system. This information is set and stored in the USB Authentication Key.

Device Info

When the Super Administrator or Administrator clicks the *Device Info* link, a screen, similar to the following appears:

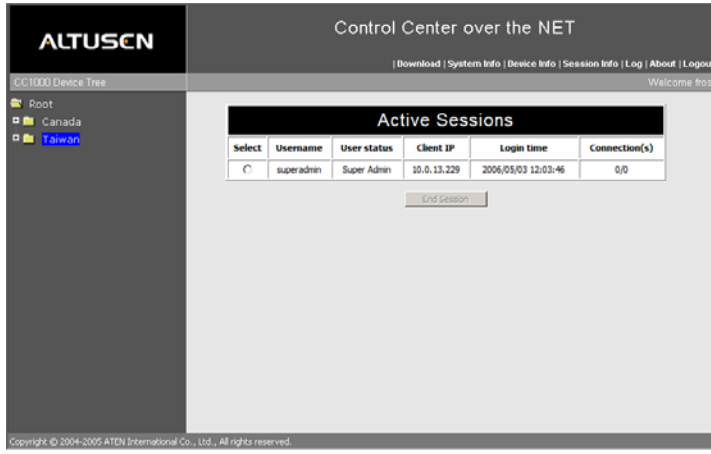


The screen provides information regarding all online devices.

- The *Object ID* entry represents the SNMP related OID (Object Identifier). If the device doesn't support SNMP, **N/A** will appear in this field.
- *UP Time* refers to the amount of time the device has been powered on (up).

Session Info

Session Info provides information regarding online active sessions. When you click the *Session Info* link, a screen, similar to the following appears :

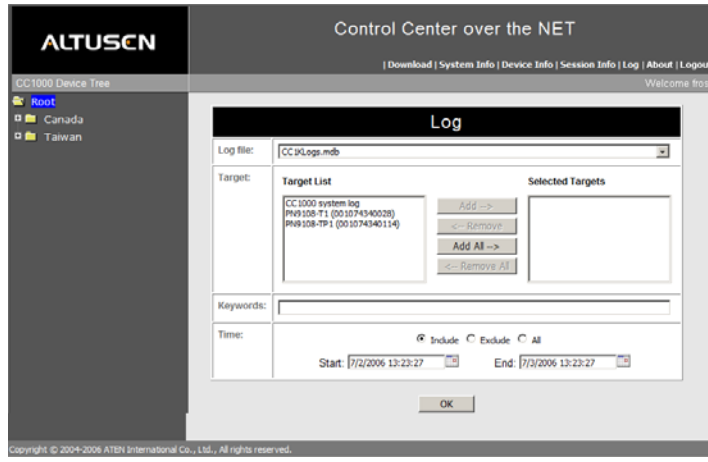


- The Super Administrator can end any Administrator or User session by selecting the desired Username and clicking **End Session**.
- The numbers under the *Connections* heading represent the number of connections to installed devices and the number of subconnections to them.

  For example, if the entry under the heading were 2/5, it would mean that the user was connected to two devices through the CC1000, and that there were a total of five connections under those devices (the subconnections).

Log

When you click the *Log* link, a screen, similar to the one below appears:



To query a log record, do the following:

1. Click the arrow at the right of the *Log File* field to drop down a list of available log files. Only the log files that you have rights to view are available.

   Note: If you have rights to query the system log, it will appear in the list.

2. Select the items that you want to perform a query on in the *Target List*, and add them to the *Selected Targets* list. If you are searching on more than one item, the order of the search will follow the order of your selection.

   Note: If you have rights to query backup log records, you may need to select the main log file in the *Log File Select* field in order to have the backup log file appear in the Target List.

3. If you want to search on a keyword, enter it in the *Keywords* field – otherwise leave the field blank.

   Note: The keyword can be a single word, a phrase, or even a sentence.

(Continues on next page.)

4. In the *Time* panel, if you want to search the entire record regardless of the time frame, select *All*.

   If you want to search a particular time range, click the calendar icons at the right of the *Start* and *End* fields to bring up a dialog box to choose the dates and times for the search, then choose whether the search will *include* or *exclude* the date/time range.

5. When all your choices have been made, click **OK** to perform the search.

About

The About page provides information regarding the current version of the CC1000.

Logout

Clicking this button logs you out of your CC1000 session.

Appendix A
Technical Information

Safety Instructions

General

- Read all of these instructions. Save them for future reference.
- Follow all warnings and instructions marked on the device.
- Do not place the device on any unstable surface (cart, stand, table, etc.). If the device falls, serious damage will result.
- Do not use the device near water.
- Do not place the device near, or over, radiators or heat registers.
- The device cabinet is provided with slots and openings to allow for adequate ventilation. To ensure reliable operation, and to protect against overheating, these openings must never be blocked or covered.
- The device should never be placed on a soft surface (bed, sofa, rug, etc.) as this will block its ventilation openings. Likewise, the device should not be placed in a built in enclosure unless adequate ventilation has been provided.
- Never spill liquid of any kind on the device.
- Unplug the device from the wall outlet before cleaning. Do not use liquid or aerosol cleaners. Use a damp cloth for cleaning.
- The device should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.
- The device is equipped with a 3-wire grounding type plug. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your obsolete outlet. Do not attempt to defeat the purpose of the grounding-type plug. Always follow your local/national wiring codes.
- Do not allow anything to rest on the power cord or cables. Route the power cord and cables so that they cannot be stepped on or tripped over.
- If an extension cord is used with this device make sure that the total of the ampere ratings of all products used on this cord does not exceed the extension cord ampere rating. Make sure that the total of all products plugged into the wall outlet does not exceed 15 amperes.

- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables and power cables carefully; Be sure that nothing rests on any cables.
- When connecting or disconnecting power to hot pluggable power supplies, observe the following guidelines:
- Install the power supply before connecting the power cable to the power supply.
- Unplug the power cable before removing the power supply.
- If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.
- Never push objects of any kind into or through cabinet slots. They may touch dangerous voltage points or short out parts resulting in a risk of fire or electrical shock.
- Do not attempt to service the device yourself. Refer all servicing to qualified service personnel.
- If the following conditions occur, unplug the device from the wall outlet and bring it to qualified service personnel for repair.
  - The power cord or plug has become damaged or frayed.
  - Liquid has been spilled into the device.
  - The device has been exposed to rain or water.
  - The device has been dropped, or the cabinet has been damaged.
  - The device exhibits a distinct change in performance, indicating a need for service.
  - The device does not operate normally when the operating instructions are followed.
- Only adjust those controls that are covered in the operating instructions. Improper adjustment of other controls may result in damage that will require extensive work by a qualified technician to repair.

Rack Mounting

- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.
- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Make sure that the rack is level and stable before extending a device from the rack.
- Use caution when pressing the device rail release latches and sliding a device into or out of a rack; the slide rails can pinch your fingers.
- After a device is inserted into the rack, carefully extend the rail into a locking position, and then slide the device into the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Ensure that proper airflow is provided to devices in the rack.
- Do not step on or stand on any device when servicing other devices in a rack.

Technical Support

International

Email Support	Email your questions and concerns to: support@aten.com
Online Support ◆ Technical Support ◆ Troubleshooting ◆ Documentation ◆ Software Updates	1. Online technical support is available to ALTUSEN customers through our e-Support Center: **http://support.aten.com** 2. Online troubleshooting that describes the most commonly encountered problems and offers possible solutions to them; online documentation (including electronically available manuals); and the latest drivers and firmware for your product are available at our website: **http://www.aten.com**
Telephone Support	886-2-8692-6959

North America

Email Support	Email your questions and concerns to: support@aten-usa.com
Online Support ◆ Technical Support ◆ Troubleshooting ◆ Documentation ◆ Software Updates	1. Online technical support is available to ALTUSEN customers through our e-Support Center: **http://www.aten-usa.com/support** 2. Online troubleshooting that describes the most commonly encountered problems and offers possible solutions to them; online documentation (including electronically available manuals); and the latest drivers and firmware for your product are available at our website: **http://www.aten-usa.com**
Telephone Support	1-888-999-ATEN

When you contact us, please have the following information ready beforehand:

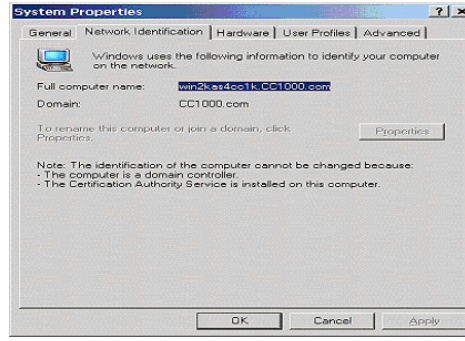
- Product model number, serial number, and date of purchase.
- Your computer configuration, including operating system, revision level, expansion cards, and software.
- Any error messages displayed at the time the error occurred.
- The sequence of operations that led up to the error.
- Any other information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

Getting the Full Computer Name

When you install the CA (Certification Authority) function, and configure the CC1000 Authentication Server, you will need to specify the full computer name. The following sections show you how to get the full computer name.

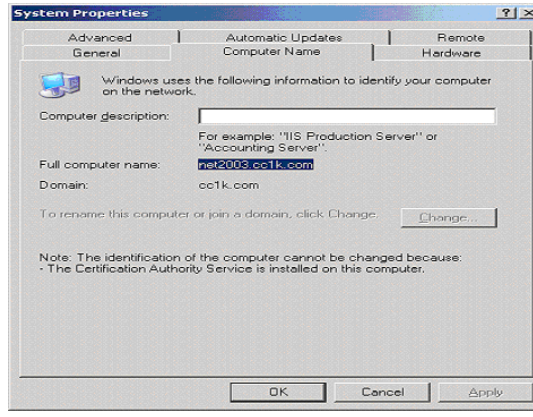
For Windows 2000 Server

1. In the Control Panel, Double click **System**.
2. Click the **Network Identification** tab. In the screen that appears, the full computer name is displayed in the *Full computer name* field:



For Windows Server 2003

1. In the Control Panel, Double click **System**.
2. Click the **Computer Name** tab. In the screen that appears, the full computer name is displayed in the *Full computer name* field:



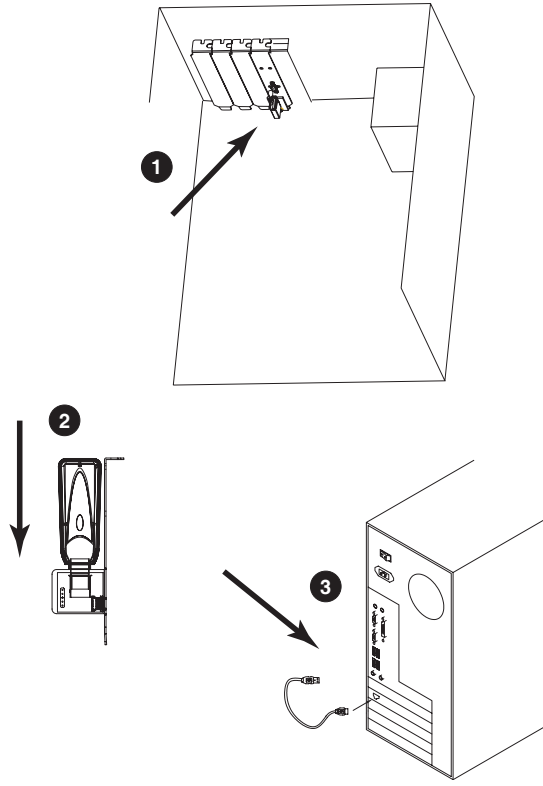
USB Authentication Key Bracket Installation

For security purposes, the USB Authentication Key can be installed inside the case. The key can either connect to an external USB port or, if your computer has an internal USB connector on the mainboard, you can connect to the internal port.

External Cable Installation

To connect to an external USB port, refer to the diagram below as you perform the following steps:

1. Install the USB Authentication Key bracket that came with your CC1000 package into one of the computer's expansion slot openings.
2. Plug the USB Authentication Key into the USB socket on the bracket.
3. Plug the "B" end of the USB cable into the bracket's USB port; Plug the "A" end of the cable into one of the computer's USB ports.

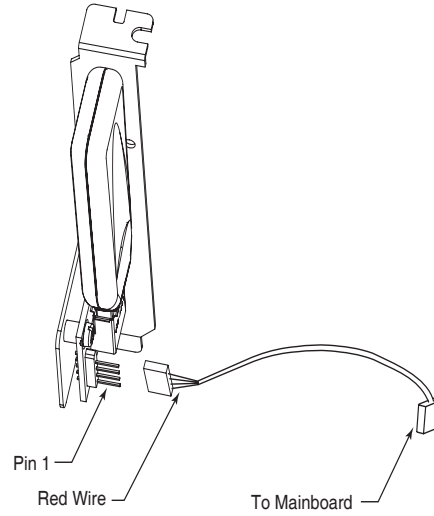


Internal Cable Installation

If your computer has a USB connector on the mainboard and you would prefer to connect to it rather than to an external USB port, do the following:

1. Install the USB Authentication Key bracket according to steps 1 and 2 of the External USB Installation procedure, described above.
2. Plug one end of the USB internal connector cable onto the bracket's connector pins.

Note: The red wire goes to pin 1 (at the bottom of the bracket).



3. Plug the other end of the cable into a USB connector on the mainboard. See your mainboard manual for the connector's location.

Internal Cable Pin Assignments

The internal connector cable's pin assignments are as follows:

Pin	Signal	Color
1	USB +5V	Red
2	D-	White
3	D+	Green
4	GND	Black

USB Authentication Key Specifications

Function		Key	Bracket
Environment	Operating Temp.	0–40° C	
	Storage Temp.	-20–60° C	
	Humidity	0–80% RH	
Physical Properties	Composition	Metal and Plastic	
	Weight	14 g	32 g
	Dimensions	8.36 x 1.37cm	1.209 x 2.14 x 4.65 cm

CC1000 Capable ALTUSEN/ATEN IP Products

The following is a list of ALTUSEN/ATEN IP products that are capable of being managed in a CC1000 Control Center Over the NET™ installation:

- CN5660; CN6000
- IP8000
- KH1516i
- KL8108; KL9116
- KN2108; KN2116; KN9108; KN9116
- PN9108
- SN0108; SN0116

Running CC1000 on 64-bit Windows

To run CC1000 on a 64-bit Windows system, you must run ASP.NET 2.0 in 32-bit mode – not 64-bit mode.

Note: You must use a CC1000 version that is higher than V1.0.094. CC1000 V1.0.094 and lower do not run properly on 64-bit Windows.

To run ASP.NET 2.0 in 32-bit mode, follow these steps:

1. Click **Start → Run**
2. Key in **cmd**, then click **OK**
3. Key in the following command (all on one line) to enable 32-bit mode:

   ```
   cscript %SYSTEMDRIVE%\inetpub\adminscripts\adsutil.vbs
   SET W3SVC/AppPools/Enable32bitAppOnWin64 1
   ```

   Note: There is a space between *adsutil.vbs* and *SET*

4. Key in the following command (all on one line) to install the 32-bit version of ASP.NET 2.0, and to install the script maps at the IIS root and under:

   ```
   %SYSTEMROOT%\Microsoft.NET\Framework\v2.0.40607\aspnet_
   regiis.exe -i
   ```

   Note: There is no space between *aspnet_* and *regiis.exe*

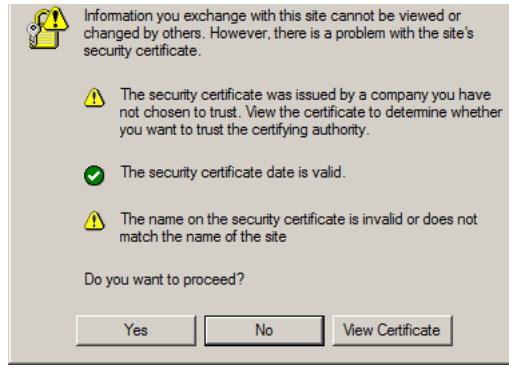
5. Make sure that the status of ASP.NET version 2.0.40607 (32-bit) is set to **Allowed** in the Web service extension list in Internet Information Services Manager.

   Note: The build version of ASP.NET 2.0 shown above (40607), is for example purposes. The build number on your version may differ depending on what the currently released build version is.

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.



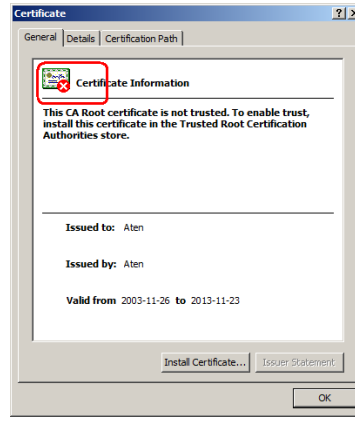
The certificate can be trusted, but the alert is triggered because the certificate's name is not found on Microsoft list of Trusted Authorities. You have two options: 1) you can ignore the warning and click **Yes** to go on; or 2) you can install the certificate and have it be recognized as trusted.

- If you are working on a computer at another location, accept the certificate for just this session by clicking **Yes**.
- If you are working at your own computer, install the certificate on your computer (see below for details). After the certificate is installed, it will be recognized as trusted.

Installing the Certificate

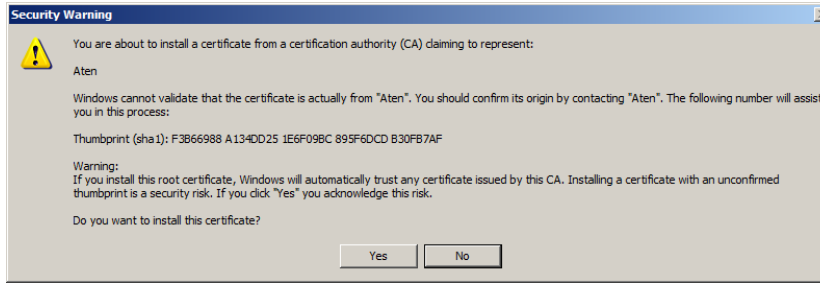
To install the certificate, do the following:

1. In the *Security Alert* dialog box, click **View Certificate.** The *Certificate Information* dialog box appears:



Note: There is a red and white **X** logo over the certificate to indicate that it is not trusted.

2. Click **Install Certificate**.
3. Follow the Installation Wizard to complete the installation. Unless you have a specific reason to choose otherwise, accept the default options.
4. When the Wizard presents a caution screen:



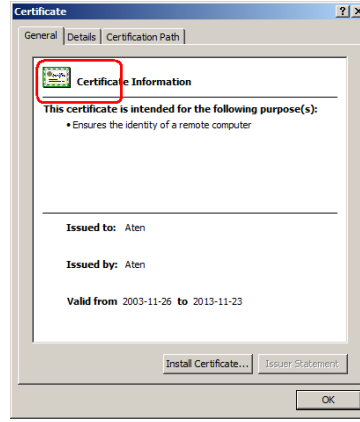
Click **Yes**.

5. Next, click **Finish** to complete the installation; then click **OK** to close the dialog box.

Certificate Trusted

The certificate is now trusted:

When you click *View Certificate*, you can see that the red and white **X** logo is no longer present – further indication that the certificate is trusted:



Troubleshooting

Installation

Problem	Resolution
While installing the CC1000 software, I get the following error message: “The Active Directory is not installed properly. Setup failed.”	The Active Directory may not be installed yet. Finish installing the CC1000 software, install the Active Directory, then run CC1KSetup.exe to successfully complete the CC1000 software installation.
While installing the CC1000 software, I get the following error message: “Setup failed to complete successfully. Error code:0003”	Finish installing the CC1000 software, then run CC1KSetup.exe to successfully complete the CC1000 software installation.

CC1000 Server

Problem	Resolution
An error occurred and the CC1000 Manager no longer seems to be providing authenticaton services.	A USB Authentication Key error occurred. This happens if an illegal operation is performed, or the CC1000 Manager ends abnormally. When this happens, the key automatically locks for about 10 minutes. You can wait until the key automatically unlocks itself, or else you can unlock it by simply unplugging and replugging it.
I am not receiving email notifications of event trap situations	1. Check that the email server settings have been specified correctly in the CC1000 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.

CC1000 Browser Operation

Problem	Resolution
I key in the IP address for the CC1000 Website, but I can't bring up the CC1000 login page.	The CC1000 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 CC1000'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`
I cannot log in to the CC1000.	Make sure your Username and Password are correct.
	If the login dialog box title (CC1000 – Login) is in a color other than white, the total number of User licenses has been reached. Only the Super Administrator is allowed to log in at this point. You must wait until a license becomes available (i.e., another users logs out) before you can log in.
When I try to log in, I get the following message: "Login failed. You are attempting to log in from a computer that already has a browser session open."	Netscape and Firefox (as well as other Mozilla based browsers), share the same session ID for multiple connections to the same server. The CC1000 will deny a login request once there already is a session open with the same session ID. Either: end the currently open session and log in again; log in from a different computer; or log in with a non-Mozilla based browser. **Note:** This condition occurs in some versions of IE running on Windows98, as well.
When I log in, the browser generates a *CA Root certificate is not trusted*, or a *Certificate Error* response.	The certificate's name is not found on Microsoft's list of Trusted Authorities. The certificate can be trusted, however. See *Trusted Certificates*, page 200, for details.
After I log in to the CC1000, I cannot bring up the page for the device I want to access.	Check with your CC1000 administrator to find out whether you are authorized to access that device.

(Continues on next page.)

(Continued from previous page.)

Problem	Resolution
When I try to access my Generic device from the Tree View nothing happens.	Generic devices are accessed directly by clicking 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.
I could not change passwords after a first-time browser login.	1. Make sure you have installed the a root certificate in the CC1000 Server (the server that CC1000 Manager is running on). 2. If the CC1000 Server uses a firewall, make sure port 445 (Microsoft-DS), or port 139 (NETBIOS), or port 636 (LDAPS) is allowed. 3. Make sure that your new password matches the Authentications Server's (AD Server's) password policy (Domain Security Policy → Account Policies → Password Policy).

CC1000 Authentication Server

Problem	Resolution
Even though I give the CC1000 a proper username and password, I cannot log in.	1. Make sure that the username has not been changed or deleted. 2. Make sure that the password has not been reset. 3. Do not use third party LDAP tools to add or change CC1000 configuration data in AD.

CC1000 Control Center Over the NET

Problem	Resolution
I cannot log in to the CC1000 Control Center Over the NET with my CC1000 username and password.	You must log in with your domain administrator's username and password as set in the Active Directory. If your CC1000 username and password is different from this, then you will not be able to log in to the CC1000 Control Center Over the NET with it.
I cannot log in to the Authentication Server with the CC1000 Control Center Over the NET even though I enter the correct Username and Password.	If *Use secure connection* is enabled, the Authentication Server's root certificate must be installed. Make sure that the root certificate has been properly installed. Install the Authentication Server root certificate, if necessary.
The device I want to add cannot be found.	1. Make sure the CC1000 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.
The Administrator Utility that I downloaded could not connect to the CC1000 Server.	1. The CC1000 Server settings may have changed after you downloaded the Administrator Utility. Download the utility again. 2. If you are behind a firewall, make sure that the LDAP and LDAPS ports (389 and 636) are allowed. 3. If you are using LDAPS, make sure you have installed the server root certificate.
I could not reset/change a password using the Administrator Utility.	1. Make sure that you have installed the root certificate in the computer that the Administrator Utility is running on. 2. If you access the AD Server remotely and it uses a firewall, make sure port 445 (Microsoft-DS), or port 139 (NETBIOS), or port 636 (LDAPS) is allowed. 3. Make sure that your new password matches the Authentications Server's (AD Server's) password policy (Domain Security Policy → Account Policies → Password Policy).

CC1000J

Problem	Resolution
I cannot log in to the CC1000J.	1. Make sure your Username and Password are correct. 2. If the login dialog box title (CC1000J – Login) is in a color other than white, the total number of User licenses has been reached. Only the Super Administrator is allowed to log in at this point. You must wait until a license becomes available (i.e., another users logs out) before you can log in.
After I log in to the CC1000J, I cannot bring up the page for the device I want to access.	Check with your CC1000J administrator to find out whether you are authorized to access that device.
The device I want to add cannot be found.	Make sure that CC Management has been enabled and specified correctly in the device's ANMS settings.
I am not receiving email notifications of event trap situations	1. Check that the email server settings have been specified correctly in the CC1000 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.
USB Authentication Key errors.	Stop the CC1000J Manager; unplug the key; replug the key; restart CC1000J Manager.
The CC1000J Manager reports "System settings - Tomcat HTTP port:8080 conflict."	Tomcat did not finish loading: 1. Wait a few moments and try again. 2. Try using a different port for Tomcat.

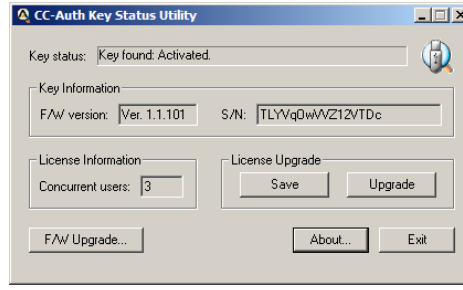
Appendix B
Authentication Key Utility

Overview

The Authentication Key Utility (CCAuthKeyStatus.exe), is a program for accessing and updating the information and data contained in the CC1000 Authentication Key. C*CAuthKeyStatus.exe*, can be found on the CD that comes with the CC1000 package. This file should be copied to a convenient location on your computer.

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

When you run the program, a screen, similar to the one below, appears:



Key Status Information

Three sections of the screen provide information about the key's status:

Section	Purpose
Key Status	Informs you whether or not the key has been found and whether or not it has been activated. If the key has not been found, or if it has not been activated, contact your dealer
Key Information	Displays the key's current firmware version and serial number.
License Information	Displays the number of concurrent users currently allowed to access the CC1000

Key Utilities

The remaining two sections offer utilities that allow you to upgrade the number of user licenses (License Upgrade), and to upgrade the key's firmware (F/W Upgrade...).

Key License Upgrade

The CC1000 has a feature that allows user licenses to be added to an authentication key. Although key license upgrades are usually handled by a distributor/dealer, there may be times when users have to perform the upgrade themselves. In case of that eventuality, the necessary procedures are described in this section.

To add licenses to a key, an order is placed with an ALTUSEN sales representative, specifying the number of licenses to be added. Upgrades can be requested for as many keys as desired in the same order.

After a Key License upgrade order has been placed, a confirmation email, similar to the example below, is sent:

```
Your order is ready to be processed. Please go to
http://192.168.3.100 to upgrade your key's license.

Login Information:

   * Username: test207@aten.com.tw
   * Password: test_032307062634_MA_780a_e00a

Order Information:

   * Order ID: 1017000125, This order requests 30 more
     license(s)

   * Order ID: 1017000124, This order requests 30 more
     license(s)

   * Order ID: 1017000127, This order requests 30 more
     license(s)
```

From here, there are two methods for upgrading the key:

- **Off Line:** A Windows-based authentication key utility (CCAuthKeyStatus.exe) is used to generate a key information data file (CC1KAUpload.dat). This file is then used to obtain an upgrade file (Keyupgrade.dat), that gets loaded into the key. A step-by-step procedure for this is given in the next section.

  Note: C*CAuthKeyStatus.exe*, can be found on the CD that comes with the CC1000 package. This file should be copied to a convenient location on your computer.

- **On Line:** The key license gets upgraded "live", over the internet. A step-by-step procedure for this is given after the *Off Line* section.

Offline Upgrade

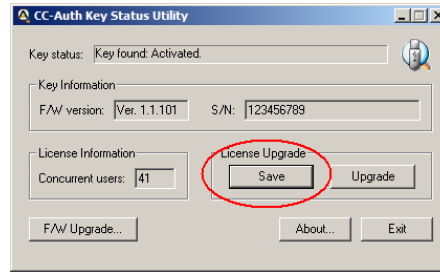
Preliminary Steps

To perform an offline upgrade, the user must generate a *Key Information Data File* (CC1KAUpload.dat). To do that, follow these steps:

1. With the authentication key plugged in, run the *Key Status Utility* (CCAuthKeyStatus.exe).

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

2. In the *License Upgrade* panel of the dialog box that comes up, click **Save**.



   The Key Information Data File (CC1KAUpload.dat) is created in the same directory that the Key Status Utility resides in. You will use that file to perform the Offline upgrade.

Performing the Upgrade

To perform the upgrade, follow these steps:

1. Open a browser and log into the URL indicated in the email (refer to page 210), with the Username and Password provided.

   Note: Accept the certificates when asked.

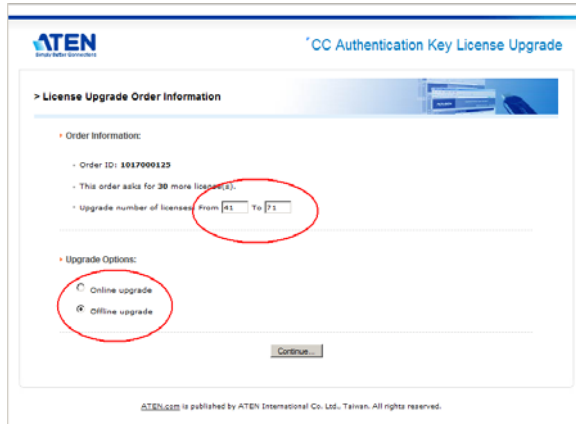
2. In the screen that comes up, key in the order number indicated in the email that applies to the upgrade (refer to page 210), then click **Continue**.

3. In the License Upgrade Order Information screen that comes up:

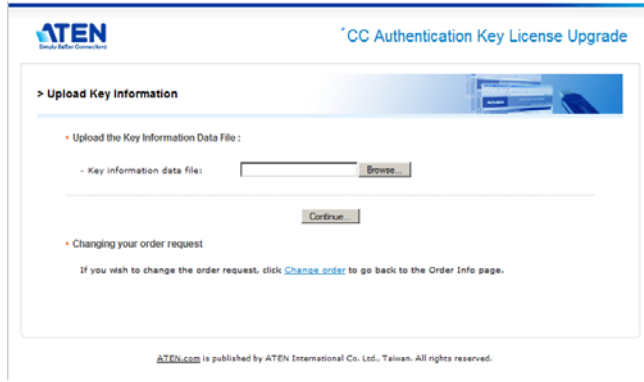
   a) Key in the current number of licenses in the *From* field. If you don't know what the current number is, ask your customer. It appears in the *License Information* panel when *CCAuthKeyStatus.exe* is run (see page 211). The *To* field is automatically filled when you click in it.

   b) Select that this is to be an *Offline* upgrade

   c) Click **Continue** to move on.

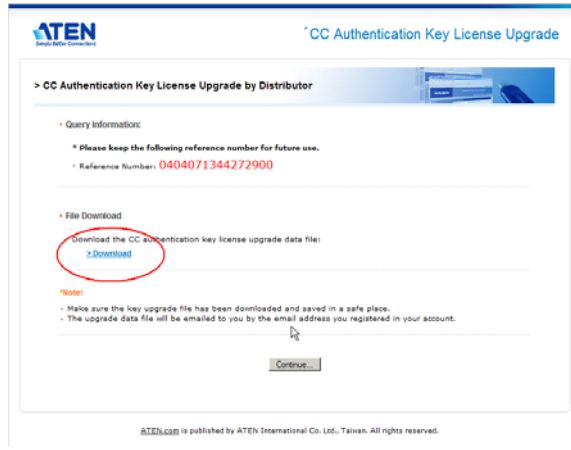


4. When the Upload Key Information screen comes up, click **Browse** and load the CC1KAUpload.dat file that was generated in the *Preliminary Steps* section (see page 211), then click **Continue**.



5. The next screen that comes up summarizes the transaction so far. Click **Continue** to move on.

6. In the screen that appears next, click **Download** to download the key license upgrade data file (Keyupgrade.dat).



7. 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.

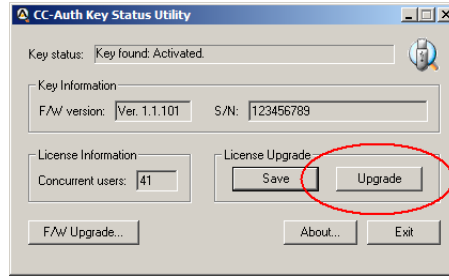
8. In the confirmation popup that appears click **Yes**. A summary page confirming the order appears:

9. Click **Logout** to exit, or **Continue** to process another order.

Final Steps

To finish the upgrade, follow these steps:

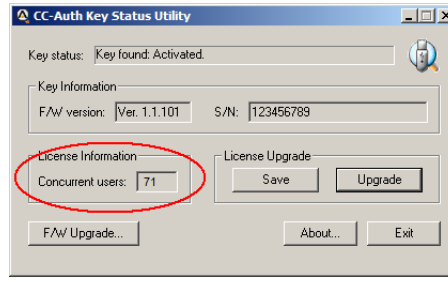
1. With the authentication key plugged in, run the *Key Status Utility* (CCAuthKeyStatus.exe) again.
2. In the License Upgrade panel, click **Upgrade**.



3. 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 concurrent users in the License Information panel changes to reflect the upgrade.



Note: When the upgrade file is downloaded, an email is sent containing the particulars, along with a copy of the upgrade file in case there was a problem with the downloaded file – as shown in the example, below:

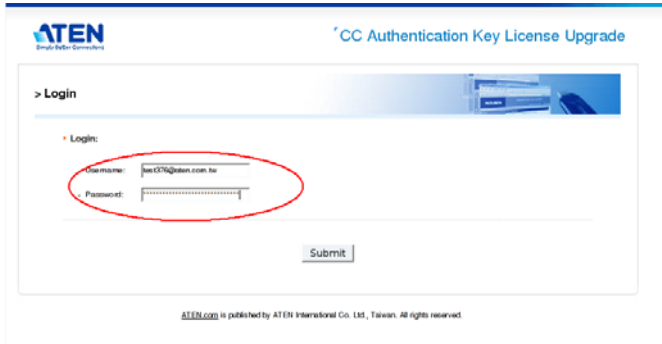
```
Offline upgrade email response:

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: 1.1.101

   * Serial number: 123456789

License Upgrade Info:

   * From 31 to 61 concurrent users

Confirmation Info:

   * Username: CC-Auth-Key-123456789

   * Password: 0404071455055016

If you have any problem with upgrading your CC-
Authentication key's license, please confirm it online
at http://192.168.3.100 using the username and
password above.
```

Online Upgrade

To perform an online upgrade, follow these steps:

1. Plug the authentication key into a USB port on your computer.
2. Open a browser and log into the URL indicated in the email (refer to page 210), with the Username and Password provided.

Note: Accept the certificates when asked.



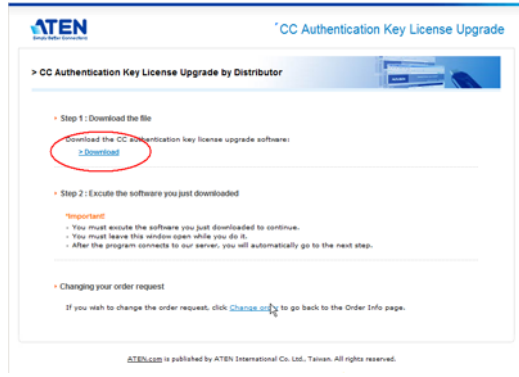
3. In the screen that comes up, key in the order number that applies to the upgrade (refer to page 210), then click **Continue**.

4. When License Upgrade Order Information screen comes up, key in the number of licenses information in the From and To fields.

Note: 1. If necessary, you can use the Windows-based Key status utility (CCAuthKeyStatus.exe) to see the current number of licenses. The To field is automatically filled in when you click in it.

2. Select that this is to be an Online upgrade, then click **Continue**.

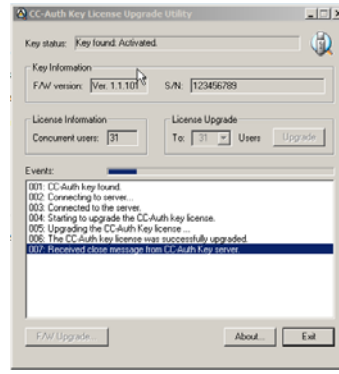
5. When the CC Authentication Key License Upgrade screen comes up, click Download.



6. When the browser asks what to do with the file (KeyUpgrade.exe), select *Save to disk.*

7. Leave the browser open, exactly as it is; go to where you downloaded the file and execute it.

   The upgrade utility comes up and starts the upgrade. The actions it performs are reported in the main panel:



8. 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:

9. Click **Logout** to exit, or **Continue** to process another order.

Firmware Upgrade

The CC1000 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:

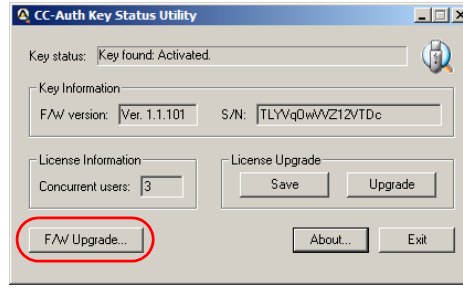
1. Go to our website and download the new firmware file to a convenient location on your computer.
2. With the authentication key plugged in, run the *Key Status Utility* (CCAuthKeyStatus.exe).

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

2. C*CAuthKeyStatus.exe*, can be found on the CD that comes with the CC1000 package. This file should be copied to a convenient location on your computer.

---

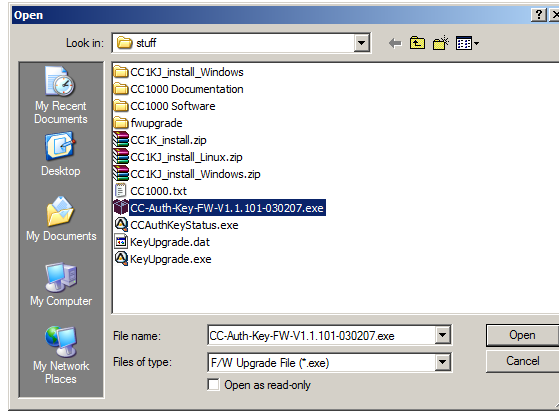
3. In the screen that appears, click **F/W Upgrade...**



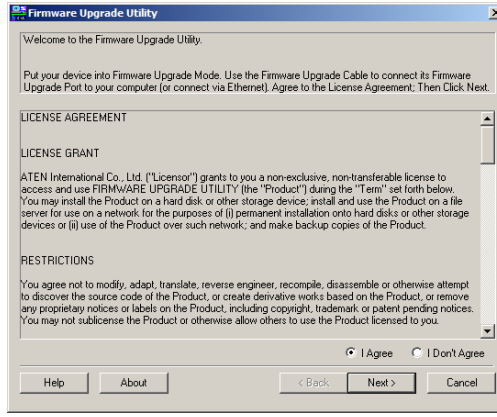
(Continues on next page.)

(Continued from previous page.)

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



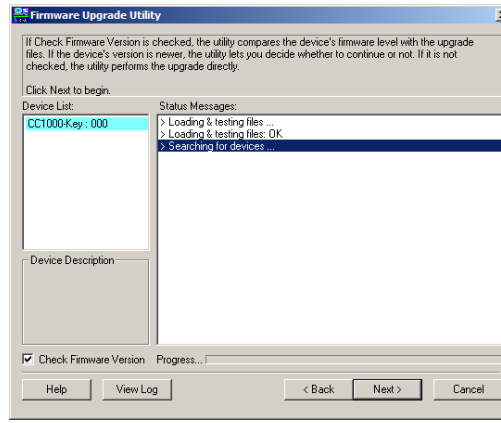
5. Read and *Agree* to the License Agreement (enable the *I Agree* radio button).



(Continues on next page.)

(Continued from previous page.)

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



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

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

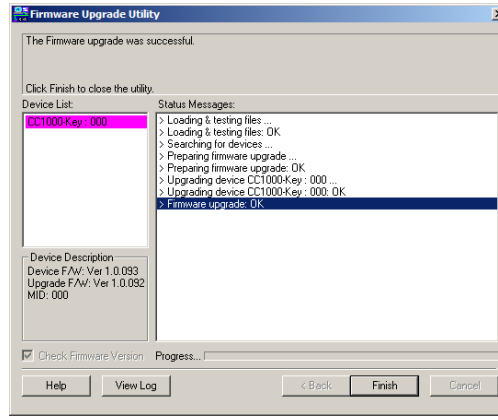
Click **Next** to continue.

(Continues on next page.)

(Continued from previous page.)

Upgrade Succeeded

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



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

Index

U

V

W