CC2000 Control Center Over the NET™

用户说明书

www.aten.com.cn

FCC 信息

美国联邦通信委员会干扰声明

本产品是通过 FCC 认证的 A 级产品。在居住环境下使用可能会对通讯造成干扰，因此建议用户可采取适当的防护措施。

本产品已经过测试，完全符合 A 级电子设备要求和 FCC 验证的第 15 部分规范。这些规范是为了在商业环境下使用本设备，而能避免有害干扰，并提供有效保护所规范的规定。本设备会产生并辐射电磁波，如果用户未能按照用户手册的说明进行安装和使用，将可能对通讯造成有害干扰，如果在居住区域使用而造成此种情况，用户将自行解决并负相关责任。

FCC 警告: 非经负责合格方对该设备所做的变更及修改会导致用户丧失操作该设备的权限。

RoHS

本产品符合 RoHS 标准。

SJ/T 11364-2006

以下内容与中国市场销售相关：

用户信息

在线注册

请一定要在我们的在线支持中心注册您的产品：

全球	http://eservice.aten.com

电话支持

如果您需要电话支持，请拨打：

全球	886-2-8692-6959
中国	86-400-810-0-810
日本	81-3-5615-5811
韩国	82-2-467-6789
北美	1-888-999-ATEN ext 4988
英国	44-8-4481-58923

用户注意事项

制造商有修改与变更手册所包含的信息、文件和规格表的权利，且不需事前通知。制造商不会保证、明示、暗示或法定声明其内容或特别否认其对于特殊用途的可销售性和适用性。本手册所描述的任何被销售与授权的制造商软件亦同。如果在购买后发现软件程序有瑕疵，购买者（及非制造商、其经销商或其购买商家）将需承担所有因软件瑕疵所造成的必要服务费用、维修责任及任何偶然事件或间接损害。

制造商并不担负任何未经授权调整本设备所造成的收音机及/或电视干扰的责任，用户必须自行修正干扰。

操作前如未选择正确操作电压设置而进行操作，制造商将不担负因此所导致任何损害的责任。**使用前请务必确认电压设置为正确的。**

包装明细

CC2000 包装明细如下：

1 个 CC2000 许可证密钥

1 套软件 CD

1 本用户说明*

请检查确保所有部件齐全，排放整齐。如果任何部件丢失，或者在装运时受损，请联系经销商。

请仔细阅读本手册，认真遵循安装和操作步骤，以免损坏切换器或 CC2000 设备中的其它设备。

*自本说明书中文化完成后，新的产品功能可能日后陆续增加，如需知道更新的产品特性，请至我们的网站参考最新版说明书。

说明书日期：2017-07-26

目录

关于本手册

本用户手册帮助您充分地使用 CC2000 系统。手册包含安装、设定和操作各个方面，内容大致如下。

一般来说，普通用户使用第一、三和四章就已足够。其它章和各附录仅供特殊类型用户使用。例如，系统管理员应阅读整个手册；设备管理员应阅读第六、八章；用户管理员应阅读第七章。自定义类型用户可阅读对应其分配权限的各章。

概述

第一章　介绍

本章向您介绍 CC2000 系统，包括其目的、特性和优势，并描述其前后面板组成部件。

第二章　CC2000 服务器安装

本章提供在 Windows 和 Linux 系统上安装 CC2000 的步骤说明。

第三章　浏览器操作

本章描述如何用浏览器登录 CC2000，并描述如何操作 CC2000 的浏览器 GUI 界面。

第四章　端口访问

本章描述如何访问和控制可通过 CC2000 网络进行管理的设备。

第五章　用户管理

本章说明如何添加、修改及删除用户帐户；创建用户群组及向其分配用户；为用户和群组指定访问权；指定用户验证方式。

第六章　设备管理

本章描述如何添加、设定和管理通过 CC2000 网络进行管理的设备。

第七章　系统管理

本章概述 CC2000 的架构概念，并演示如何部署、设定和管理设备中 CC2000 主、从服务器。

第八章　日志

本章说明 CC2000 的日志功能，及如何访问、过滤和搜索 CC2000 保存的多种日志文件。

附录 A　技术资讯

本章提供技术资讯和故障排除信息。

附录 B　CC2000 工具

本章描述如何无需激活浏览器 GUI，从 CC2000 运行的电脑桌面设定 CC2000 的诸多参数。

附录 C　验证密钥工具

本章描述如何使用和更新 CC2000 验证密钥包含的信息。

附录 D　外部验证服务

本章讨论通过外部第三方服务进行的验证，本章也提供如何设定 OpenLDAP 以进行 CC2000 验证，及在 Linux 环境下设定 RADIUS 以进行 CC2000 验证。

常规用语

本用户手册使用下列常规用语：

Monospaced	表示需要键入的文本信息。
[ ]	表示需要按的键。例如，[Enter]表示按 **Enter**(回车)键。需要同时输入的键，就放在同一方括号内，各键之间用加号连接，例如，[Ctrl+Alt]。
1.	数字表示操作步骤序号。
◆	表示提供信息以供参考，与操作步骤无关。
→	表示下一选项(例如，在菜单或对话框中)。例如，Start→Run，表示打开*Start*菜单，然后选择*Run*。
⚠	表示极其重要的信息。

产品资讯

如果您想了解所有宏正产品资讯及如何更有效地使用这些产品，请随时访问宏正的网站或联系宏正授权的经销商，请访问如下网站以获取更多资讯：

全球	http://www.aten.com
中国	http://www.aten.com.cn

固件重要提示

由于此固件版本(V2.3.222)已发布，数据库已更新，所以此版本 CC2000 不兼容之前任何版本的 CC2000。CC2000 固件 V2.7.264 支持 Java Web Start (JNLP)。

第一章
介绍

概述

CC2000 Control Center Over the NET™远程集中管理软件提供对整个网络－本地及全球－的单一入口、单一登录、安全集中、随时随地的访问和管理。

CC2000 提供单一、整合的浏览器界面，以管理所有设备。用户无需学习各设备的不同界面，使系统管理更简洁高效。

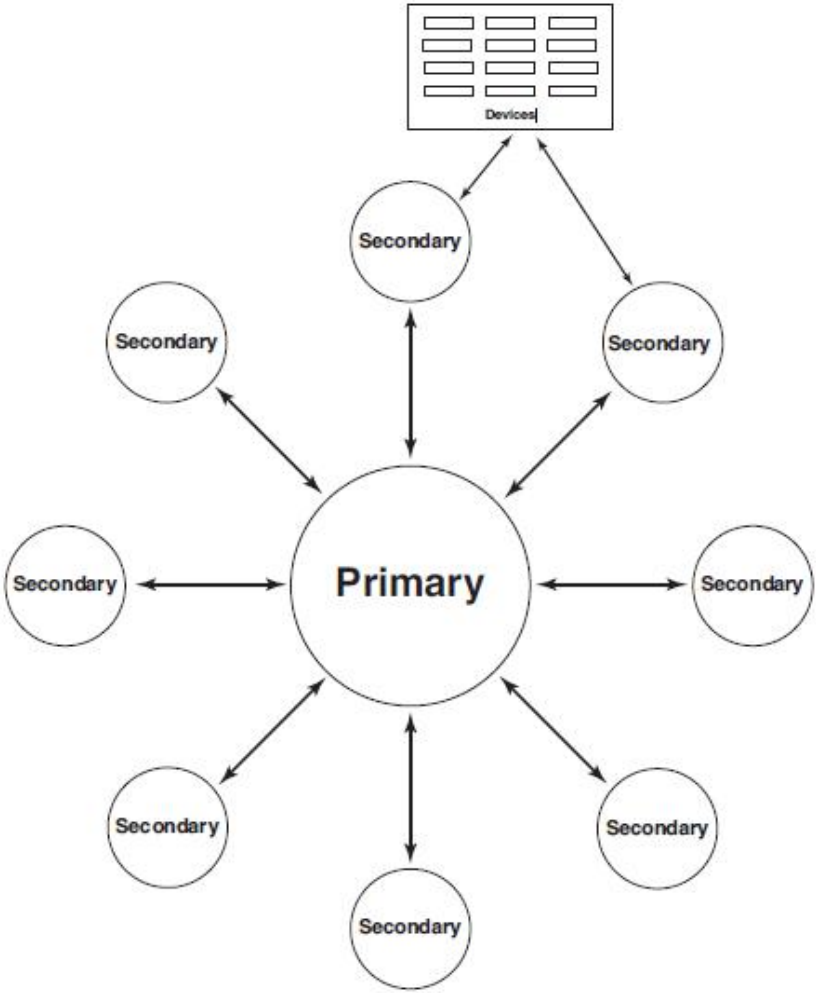
CC2000 的*主/从*架构允许多台 CC2000 设备连接于通讯网络，以创建设备的一体网络－从网络浏览器通过单一登录即可访问所有设备。(下一页提供 CC2000 部署示例图。)

主-从架构通过内建的冗余机制，包括自动备份主、从和其它设备的数据、以及实时更新数据，保障数据传输的安全。冗余机制确保任何一台 CC2000 服务器发生故障时，CC2000 管理系统仍保持运作，因为冗余从设备会接替并提供所需服务，直到故障设备恢复正常。通过此双重冗余功能，各从服务器都可拥有自己的冗余从，从而确保顺畅、持续地管理所有设备。

CC2000 整合管理 ATEN/Altusen 设备，允许通过单一 IP 地址安全访问和控制所有设备。CC2000 将服务器和网络设备整合于单一树形视图，对于拥有跨地区数据中心和分支办公室的企业来说，CC2000 是理想之选。

CC2000 的 Java 软件识别诸多电脑环境，可与启用 Sun Java 运行环境(JRE)的操作系统搭配使用－确保多平台的整合性和彼此间的互通性。

部署示例图：


Devices
Secondary
Secondary
Secondary
Secondary
Primary
Secondary
Secondary
Secondary
Secondary

特性

安全集中管理

- 可全面控管企业－整合管理所有 ATEN/Altusen 设备
- 通过单一入口、单一登录和单一 IP 地址安全访问设备中的所有设备
- 所有设备整合于一个树形视图，以随时随地集中访问和管理分布世界各地的设备的网络
- 主/从架构提供了冗余能力-包括数据库更新
- 双冗余功能－CC2000 不仅为数据中心的主服务器提供一个冗余能力，每个从服务器同时也可拥有一个冗余从服务器
- 聚合设备－可将一个 IT 设备上的 KVM 连接端口、串口连接端口与电源插座组合在一起，显示在同一 web 界面，使 IT 管理员从单一用户界面完整地控制该 IT 设备。
- 支持多平台安装- Windows/Linux
- 支持多平台客户端(Windows、Mac OS X、Linux、Sun)
- 支持多种浏览器– Internet Explorer, Chrome, Firefox, Safari,Opera, Mozilla, Netscape
- 邮件通知特殊系统事件
- 自动进程系统、设定和维护任务
- 记录和审查 CC2000 及其管理的设备的系统事件
- 会话日志提供串口设备的历史记录
- 自动搜索 ATEN/Altusen 设备，并提供设备状态与警示信息
- 能实时浏览、管理与终止在线用户会话
- 用户层级管理认证
- 浏览器 GUI 提供不同语言界面，以减少用户学习时间并提高工作效率
- 支持通用设备(Generic Device)－可将用户从 CC2000 转向第三方数据中心的设备
- 弹性化的纪录与报告选项功能

- 支持整合刀片式服务器以集中管理服务器，及管理服务器电源 - 开关服务器，并通过 Service Processor Management 读取传感器及日志信息
- 支持 APC PDU (AP79xx, AP89xx, AP86xx)
- 支持单一登入 Dell DRAC 5, iDRAC 6 (标准机架服务器(monolithic)及刀片服务器(modular)),IBM RSA II, HP iLO 2, Dell CMC, IBM AMM 与 HP OA
- 支持机架型智能 PDU
- 整合所有目标设备的 SSH/Telnet, VNC/RDP, IPMI/SPM, KVM, 串口与电源的访问权限
- VMware 虚拟架构包括 Center Servers, ESX Servers 与虚拟机器(Virtual Machines)及 Citrix XenServer
- 画面同步分割模式(Panel DynaArray™)–可让 IT 管理员在同一个屏幕浏览来自不同连接端口的画面输出
- 可与 ATEN/Altusen PDU 电源分配器整合，整合 KVM 多电脑切换器连接端口与 PDU 电源分配器的电源插座，以利从 KVM 多电脑切换器进行服务器电源的远程管理
- Web-based 软件安装精灵，可协助迅速完成安装
- 主服务器可访问从服务器设备连接端口名称
- 先进的登入搜寻功能
- 强大的联机管理(session management)/整合不同的联机功能(包括 ATEN iKVM, 刀片服务器, VMware, PDU 电源分配器与其它设备)
- 节省使用许可数–通过整合设备可整合不同连接端口至单一节点许可
- 远程或本地端服务器的数据可实时或排定时程进行导出/导入。数据导出支持 AES/DES
- 支持 OOBC, PAP 与 CHAP 验证
- 支持 IPv6
- 支持 NTS–可精准显示管理者所指定的服务器上的设备时间

强大的安全机制

- 强大的安全机制包括内部与外部验证－外部验证支持包括 LDAP、LDAPS、Kerberos、Active Directory、RADIUS、TACACS+、及 NT Domain－只有通过验证的用户才可以访问设备
- 可选择强制所有 CC2000 管理的设备的用户都进行 CC2000 验证－用户不能直接登入这些设备
- 符合 X.509 数字证书标准
- 支持 TLS 1.2 数据加密和 RSA 2048 位认证，以确保用户从浏览器登录
- 灵活的会话超时注销功能
- 基于角色的访问和控制权机制，可设定用户和群组访问与控管服务器的权限
- 支持强大的密码保护机制－符合 SAS70 认证，可设定用户登录失败次数和用户 ID 自动锁定参数
- 在浏览器中，可通过名称、MAC 地址、或 IP 进行设备识别－KN/SN/PN 设备的 IP 地址可隐藏以维护其安全性
- 通过 IP 与 Mac 进行过滤
- 支持 CA 私钥

服务器管理功能

- 支持 BIOS 层级管理
- 弹性的加密设计允许用户选择 56 位 DES、168 位 3DES、256 位 AES、128 位 RC4 或 Random 的任意组合，分别加密键盘/鼠标、显示器与虚拟媒体数据
- 支持虚拟媒体
- 支持退出宏
- 支持鼠标动态同步
- 支持画面分割模式–可同时监看服务器的影像输出
- 信息板功能可让远程使用者进行沟通
- 画面可随着窗口大小自动调整

系统要求

服务器要求

安装 CC2000 服务器的系统应达到如下要求：

- 硬件要求
  - CPU：Pentium 4,2.60 GHz 或更高
  - 内存：至少 512MB (建议 1GB 或更高)
  - 硬驱：500MB 或更多可用空间
  - 以太网：至少 1 个以太网适配器 (100Mbps 或更高) – 建议 Giga LAN
- 操作系统要求
  - Windows： 2000、XP、2000 Server、Server 2003、Server 2008，或配备 Java 运行环境(JRE) 6，Update 11 或更高的 Windows Vista (针对各安装版本有最新服务包)
  - Linux (配备 Java 运行环境(JRE) 6，Update 11 或更高)
    - Red Hat Enterprise Linux V. 4 和 5
    - Novell SUSE Enterprise Server 9 和 10
    - Ubuntu 15.10 x64
    - Ubuntu 15.10 x86
    - Debian 8.2 x64
    - Fedora 23 x64
    - Fedora 23 x86
    - OpenSUSE 13.1 x64
    - CentOS 7 x64

客户端要求

硬件要求

- CPU：为取得最佳效果，我们建议访问切换器的电脑至少配有 P III 1 GHz 处理器，屏幕分辨率设为 1024 × 768。
- 内存：至少 512MB (建议 1GB 或更高)
- 以太网：至少 1 个以太网适配器 – 10Mbps 或更高 – 建议 100Mbps
- 浏览器必须支持 128 位 SSL 加密。
- 对于基于浏览器的 Java Applet 浏览器，必须安装 Sun Java 运行环境(JRE)的最新版本。
- 从浏览器登录后，第一位浏览者必须要有至少 205M 内存可用，此后各附加浏览者有 100 MB 内存可用。

操作系统

- 对于连接 CC2000 的客户端工作站，支持的操作系统如下表所示：

操作系统		版本
Windows		2000 或更高
Linux	RedHat	7.1 或更高
	Fedora	Core 2 或更高
	SuSE	9.0 或更高
	Mandriva(Mandrake)	9.0 或更高
UNIX	AIX	4.3 或更高
	FreeBSD	4.2 或更高
	Sun	Solaris 8 或更高

- 对于登录 CC2000 的用户使用的操作系统，支持的包括 Windows2000 或更高，以及可运行 Sun Java 运行环境(JRE) 6，Update 11 或更高的操作系统。

注意： Windows 2000 Client不支持WinClient浏览器

浏览器

对于登录 CC2000 的用户使用的浏览器，支持的包括：

◆

操作系统		版本
IE		6及以上版本
Chrome		8.0及以上版本
Firefox	Windows	3.5及以上版本
	Linux	3.0及以上版本
Safari	Windows	4.0及以上版本
	Mac	3.1及以上版本
Opera		10.0及以上版本
Mozilla	Windows	1.7及以上版本
	Sun	1.7及以上版本
Netscape		9.0及以上版本

注意：针对更新版本的Chrome浏览器，您可能需要启用NPAPI（Netscape浏览器插件应用程序编程界面）在地址栏手动键入命令 "chrome://flags/#enable-npapi" 或者，您可以去Java.com（https://java.com/en/download/faq/chrome.xml）了解更多详情。

设备要求

所有 ATEN/Altusen IP 产品的固件必须要包含 CC 管理功能，且必须启用 CC 管理功能。如有必要，请从我们的网站下载并安装相关固件的最新版本。关于更新固件的详情请见第 197 页的*更新所选设备的固件*。

注意：1. 必须设定设备通讯的端口与为CC2000的设备端口所设的端口相同 (见第15页的*设备端口*)。

2. 关于支持的设备的列表，见第243页的*支持CC2000的*ATEN/Altusen *IP产品*。

许可证

CC2000 许可证控制 CC2000 服务器设备中允许的从服务器和节点的数量。许可证信息包含在购买 CC2000 时附带的 USB 许可证密钥中。

完成 CC2000 服务器软件安装后，将自动提供对一台主(不带从)和 16 个节点的默认验证。要添加更多(从服务器及节点)，您必须更新许可证。详细说明请见第 188 页的*更新许可证*。

节点

- 一个节点可以是一个物理端口，也可以是一个虚拟设备。每个节点要求有一个许可证。

  当 CC2000 管理的一台设备(路由器、服务器、以太网切换器等)能够通过几组 ATEN/Altusen™端口被访问时，即可创建虚拟。通过将这些端口整合到单一虚拟设备，此虚拟设备算作视为一个节点，因此仅需要一个许可证。

  ATEN/Altusen™设备上的端口，当不属于虚拟设备时，必须解锁这些端口(见 108 页的*解锁端口*)才可使用这些端口。解锁的各端口视为一个节点。
- 通用设备(路由器、切换器等)不算在内。
- 直接网络访问的设备不算在内。
- 群组设备不视为节点。群组由组在一起的、被解锁的物理端口组成。同一物理端口可添加到不只一个群组设备，但是，不论添加到多少个群组设备，它只需要一个节点许可证。
- 和群组设备一样，文件夹也不视为节点，但是文件夹中的各物理端口视为一个节点。另外，包含于文件夹中的各虚拟设备视为一个节点。

注意：各设备类别的详细说明，请见第88页的*设备*。

从服务器

许可证指定可在主 CC2000 上注册多少从服务器。关于在主上注册从的详细说明，请见第 23 页的 *CC2000 从服务器*。

此页刻意留白

第二章
CC2000 服务器安装

概述

认识到 Linux 在服务器环境中越来越重要，CC2000 远程集中管理软件使 CC2000 管理可用于 Windows 和 Linux 两种平台。本章描述如何在各平台安装 CC2000 服务器。

CC1000 考虑事项

更新 CC1000

已有 CC1000 USB 许可证密钥(针对最少 2 位用户)的用户，可以更新至 CC2000-LE (CC2000 Lite)版本，此版本提供一个允许 1 个主和 128 个节点的许可证。更新 CC1000 密钥固件为 CC2000 密钥固件(见 264 页的*密钥固件更新*)即可获得此许可证。执行更新后，许可证密钥变为 CC2000 许可证方式。

注意：如果您决定回到CC1000许可证方式，则必须用CC1000密钥固件(V 1.2.111)“更新”密钥，此时CC1000密钥许可证－保有原先的用户数－被恢复。

卸载 CC1000

如果已安装了先前的CC1000而您又尝试安装标准CC2000版本，屏幕出现一条信息，通知您必须先卸载 CC1000，以便安装 CC2000：

注意：如果选择不卸载CC1000(因此会损失其所有信息)，您必须将CC2000安装在不同系统及不同网段上。如果将其安装在同一网段，您必须关闭其中一个

系统。

安装 Windows 版本

安装前

运行安装程序之前，请确保系统已安装 Sun 的 Java 运行环境(JRE)6, Update 11 或更高。如果未安装，则需要下载并安装。您可以从 Java 网站获得最新版本：

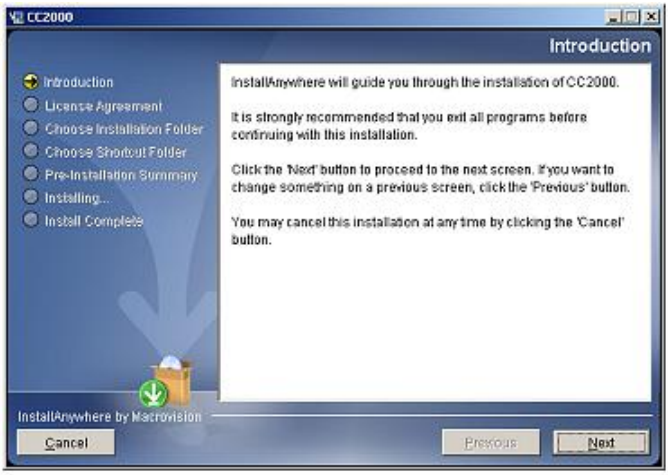
`http://java.com`

在系统上安装 JRE 之后，即可随时安装 CC2000。

开始安装

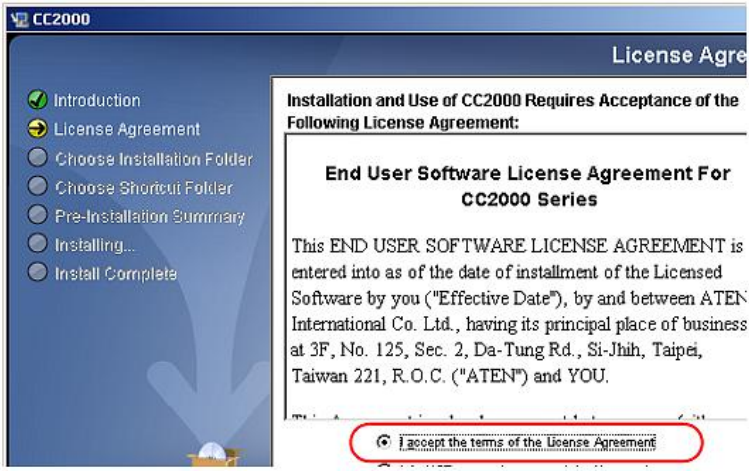
在Windows系统上安装CC2000，请按如下操作：

1. 将包装附带的软件CD放入电脑的CD或DVD驱动器。
2. 到*CC2000Setup_Win.exe*所在的文件夹，执行此文件。如下窗口出现：



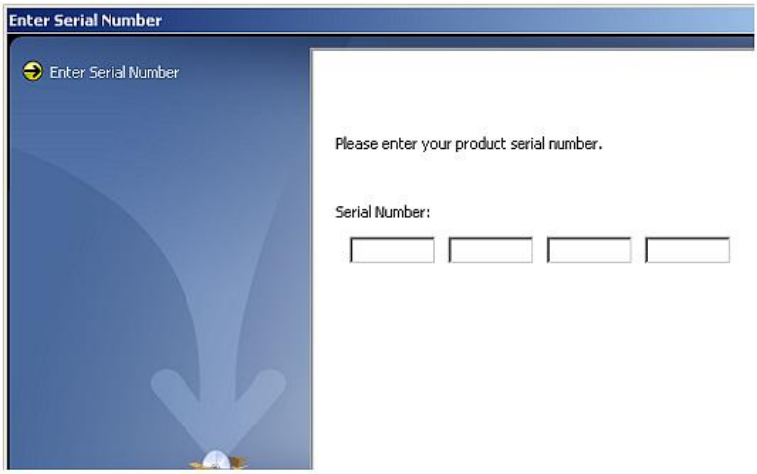
点击**Next**以继续操作。

3. 在出现的窗口中，请阅读*许可证协议*，然后点击勾选*I accept…*单选按钮：



4. 点击**Next**以继续。

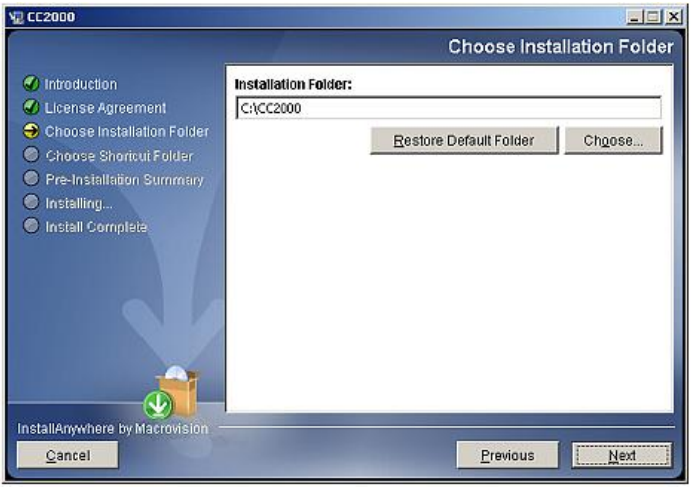
5. 如下对话框出现：



6. 键入CC2000的软件序列号(序列号可在CD盒上找到)，点击**Next**以继续。

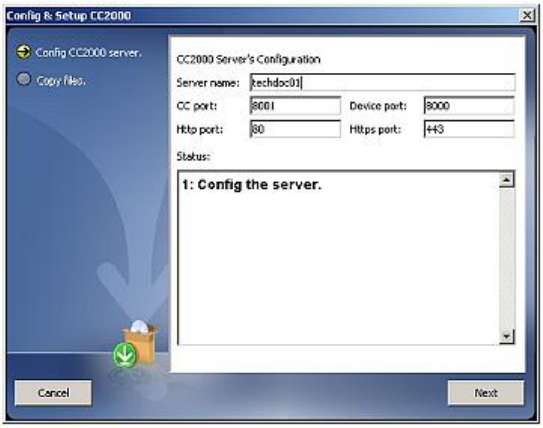
注意：我们建议您将软件序列号保存在安全的地方，以备重装之需。

7. 在*Choose Installation Folder*对话框中，指定CC2000的安装文件夹。如果您不想使用默认条目，点击**Choose...**以浏览到您需要的位置，然后点击**Next**以继续。



8. 在*Choose Shortcut Folder*对话框，点击一个单选按钮，指定要创建产品图标的地方，然后点击**Next**以继续。

9. 在出现的Configuration对话框，根据下表提供的信息填写各区。



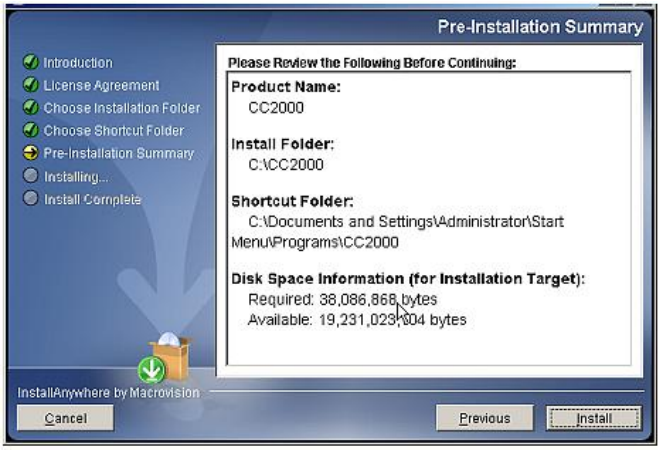
标题	说明
Server name (服务器名)	此对话框显示服务器的默认名称－在 Windows *Computer Name* 设置中指定的。您可以选择其它名称，以在 CC2000设备中识别此服务器。名称可以是2-32字节的任何支持的语言。 **注意**：1. 不能用如下字符："'\。 2. 此名称仅针对 CC2000服务器所用－它不改变电脑的实际名称。
CC port (CC端口)	CC2000用此端口与其它 CC2000服务器通讯。默认为8001。 **注意**：1. 这就是 *This Server* 网页上所指的 **CC Port**(见第148页的*服务器信息*)。 2. 尽管系统中的各 CC2000服务器可使用自己的端口设置，但是为了方便管理，我们建议所有 CC2000服务器使用同一端口设置。
Device port (设备端口)	CC2000用此端口与设备中其它设备(ATEN/Altusen 产品)通讯。默认为8000。 各 CC2000可有不同设备端口号，但是为了与其网段所连设备通讯，这些设备必须设定使用在此设定的同一端口。
HTTP port (HTTP端口)	CC2000用此端口进行网络通讯。默认为80。如果您使用不同的端口，用户必须在其浏览器的地址栏指定端口号。
HTTPS port	CC2000用此端口进行安全网络通讯。默认为443。如果您使用不

(THHPS端口)	同的端口，用户必须在其浏览器的地址栏指定端口号。

10. 填写各区后，点击**Next**以继续。

注意：安装后您可以修改这些设置。详情请见第148页的*服务器信息*。

11. 对话框变为通知您，文件已拷贝到安装文件夹。一旦这些文件被拷贝完，点击**Continue**以继续。
12. *Pre-Installation Summary*(安装前信息概述)窗口出现：



如果要修改某项，点击**Previous**以回到上一窗口，如果信息正确，点击**Install**。

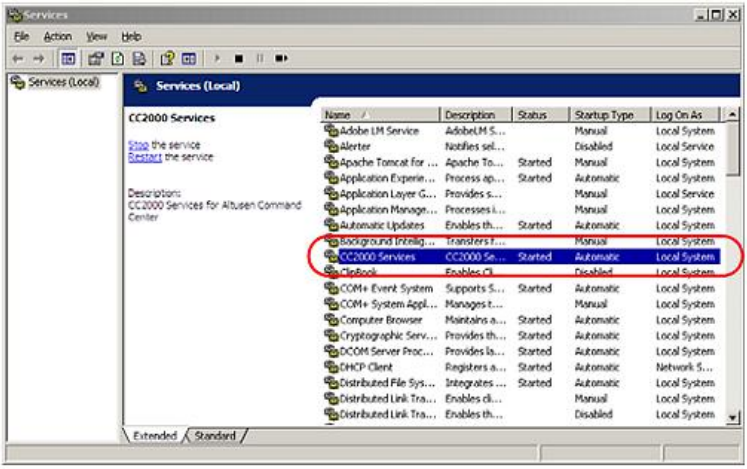
13. 当安装工具调出一个窗口通知您安装成功完成时，点击**Done**以退出安装器。

14. 安装完成后，一个CC2000条目创建在Windows*开始*菜单中。

安装后检查

安装成功完成后，CC2000程序自动运行(随每次启动自动运行)。

检查CC2000是否运行，导航经过如下文件夹：Control Panel → Administrative Tools → Services。在列表中查找CC2000条目。如果CC2000正在运行，其则出现于servieces列表。您可以看到一个类似如下的窗口：



Status区应该显示*Started*。如果未显示，右击CC2000条目行的任何地方，从弹出菜单中选择**Start**。

安装 Linux 版的 CC2000

安装前

在 Linux 系统上安装 CC2000 的步骤与在 Windows 系统上安装 CC2000 相似，但是首先要注意的是 Java 事项。

- 如果您的系统尚未安装 Java，请从 Java 网站进行下载：

  `http://java.com`

  安装说明在 Java 下载页提供。

- CC2000要求安装JRE6, Update 11或更高，而某些Linux发行套件装有的版本早于CC2000这一要求。要测定您系统上的Java版本，打开一个终端，输入如下信息：

  Java –version

  如果其显示的Java版本早于JRE6, Update 11，您必须安装JRE6, Update 11或更高的版本。(参见前一条关于下载和安装Java的信息。)

- 请确保在您的*/root/.bash_profile*文件中，PATH和JAVA_HOME环境变量指向新版本。例如：

```
PATH=/usr/java/jre1.6.0_0-b11/bin:$PATH:$HOME/bin:./
JAVA_HOME=/usr/java/jre1.6.0_0-b11
BASH_ENV= $HOME/.bashrc
USERNAME= "root"
export USERNAME BASH_ENV PATH JAVA_HOME
```

- 即使安装了适当的Java版本并设置了新PATH和JAVA_HOME环境变量后，发行套件可能仍不识别新版本，并继续使用原先的Java版本。如果您的设备存在此问题，按如下步骤纠正此问题：

  1. 从发行套件CD复制CC2000*Setup_Linux.bin*文件到您硬盘上的文件夹。
  2. 打开一个终端，到CC2000*Setup_Linux.bin*文件所在的目录。
  3. 输入如下明令：

     `export LAX_DEBUG=1`

```
sh CC2000-Setup-ForLinux.bin
```

注意：如果安装程序运行，取消运行。

4. 在出现的窗口，寻找以如下开头的一行(以粗体显示)：

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

   以查看您的Java发行套件的默认值。

5. 如果*Using VM*条目显示一个名为*java*的文件的路径在旧Java版本目录中，则到此目录，或是删除、或是重命名此*java*文件。

6. 退出并重新登录。

开始安装

确保安装了适当JRE版本后，请按如下操作：

1. 将包装附带的软件CD放入电脑的CD或DVD驱动器。
2. 到*CC2000Setup_Linux.exe*所在的文件夹，执行此文件。

注意：1. 您必须以系统管理员的身份运行安装程序。
2. 确保安装文件有可执行权限。
3. 对于某些Linux版本，程序必须在终端运行。

如下窗口出现：

点击**Next**以继续。

3. 从此步骤，安装步骤与Windows版的安装步骤相同。关于如何继续安装的详细说明，请参考Windows版的CC2000安装步骤(见第12页)。

安装后检查

1.安装成功完成后，CC2000程序自动运行(随每次启动自动运行)。

要检查CC2000是否已运行，从一个终端控制端发布如下命令(以系统管理员身份)，运行、停止并重运行service命令：

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

2. 如要检查您的系统运行的Java版本，请执行以下操作：

1.打开开始菜单。

2.导航至CC2000条目（程序→CC2000），并选择Java版本检查。

安装后设置

CC2000软件附带一个默认演示版许可证，其允许服务器作为一个无从却有16个节点(所有节点必须与服务器在同一网络) 主服务器。要超出此限制，您需要一个允许从和附加节点的许可密钥。

一旦软件安装在服务器上，下一步则是指定服务器是主还是从。

- 如果此服务器将成为主，那么插入CC2000的USB密钥到USB端口；登录服务器(见第25页的*登录*)；到*Licence*页，点击**Upgrade**(详情请见第172页的*更新许可证*)。允许的从和节点数量依据购买的许可证密钥而变化。详情请联系经销商。

注意：更新许可证后，拔出密钥，将其放在安全的地方，因为您将需要它进行

以后的更新。

- 如果此服务器将成为从，则无需插入许可证密钥 – 只需将其注册在主上即可。详情请见第167页的*注册*。

卸载 CC2000

从 Windows 系统卸载

从Windows系统卸载CC2000，请按如下操作：

1. 打开*Start*菜单。
2. 导航至CC2000条目(Programs → CC2000)，选择**Uninstall** CC2000。

注意： 卸载程序并不删除操作期间创建的多个CC2000文件和文件夹。要进行完整卸载(如果您打算重装，则有此必要)，必须将CC2000文件和文件夹其本身从CC2000被安装的位置(默认文件夹是C:\CC2000)删除。

从 Linux 系统卸载

从Linux系统卸载CC2000，以系统管理员的身份执行如下命令：

```
/install-path/Uninstall_CC2000/Uninstall_CC2000
```

/install-path/代表安装程序时为CC2000指定的路径和目录。

注意： 卸载程序并不删除安装期间创建的多个CC2000文件和文件夹。要进行完整卸载(如果您打算重装，则有此必要)，必须手动删除CC2000文件和文件夹其本身。默认文件夹为/home/CC2000。

更新 CC2000

如果已安装CC2000程序，则不必执行完整安装。运行CC2000-Upgrade程序，即可更新至最新CC2000版本：

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

注意：更新时，必须要更新主和各从服务器。

更新程序新版本可选用时，就发布到我们的网站上以便下载。请查看我们的网站以获得最新的版本。

准备步骤

这些步骤确保所有CC2000设备上的安装数据库都是最新的。如果更新后出现了问题，可用这些步骤创建的备份，将数据库恢复到最新工作水平。

我们建议您开始更新前，在各CC2000设备上采用如下备份步骤：

1. 复制各从的数据库；用*Run Now*作为scheldule设置(见第205页的*复制数据库*)。
2. 复制完成后，返回去将scheldule设置为更新期间此计划不会发生的时间(下星期，下个月等)。
3. 在主设备上，做一个数据库备份(见第192页)。

一旦完成了这些准备步骤，您即可更新主和各从。运行更新程序时，遵循安装精灵来完成操作即可。

CC2000 从服务器

完整的CC2000设备包括位于世界各地的1个主和多达31个从服务器。当您更新CC2000软件附带的演示版许可证时，主服务器自动被指定。详情请见第171页的*许可证*。

一旦设置了主服务器，即可用*注册*功能，将其它各CC2000服务器注册为从。详情请见第167页的*注册*。

CC2000 冗余从服务器

提供CC2000服务器冗余功能－备份(备用)CC2000自动接替故障主(首选)CC2000继续运行－请按如下操作：

1. 在同一网段安装两台CC2000服务器。
2. 在*Device Management*项，在设备的ANMS设置页上，为网段上的各设备指定首选和备用CC2000的IP地址(见第136页的*设备设定(针对KVM设备)*)。

现在，如果设备不能连接首选CC2000服务器(由于网络故障、CC2000故障等)，设备则连接备用CC2000。一旦其连接了备用CC2000，此后设备将备用CC2000作为其连接首选。备用设备保持首选直到设备不能与之连接为止，然后其寻求与原先的首选服务器的连接。

注意：冗余从服务器不是特殊类别的CC2000服务器。它们与CC2000管理系统中的其它任何从服务器没有区别。它们在设备首选CC2000发生故障时提供备用

支持，在这种情况下它们才是冗余服务器。这与为TCP/IP网络指定首选和备用DNS服务器相似。

此页刻意留白

第三章
浏览器操作

为确保多平台互通性，通过大多数标准网络浏览器可实现对 CC2000 的访问。一旦用户登录并通过验证，CC2000 的浏览器 GUI 界面出现。本章说明登录步骤，并描述 CC2000 的浏览器 GUI 组成部分。

登录

登录 CC2000，请按如下操作：

1. 打开浏览器，在浏览器地址栏，指定 CC2000 的 IP 地址。

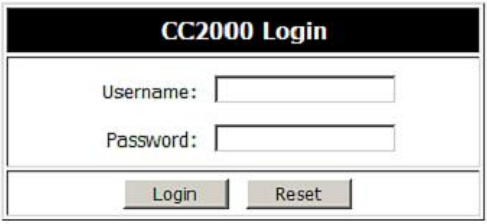
注意：如果系统管理员已设定HTTP或HTTPS端口设置为非CC2000默认值，您必须要在IP地址前包括htttp://或https://，并在IP地址后给出端口号。例如：

`http://192.168.1.20:8082`

其中*8082*是http端口号，其与IP地址之间要加入一个冒号。

---

2. 如果安全警告对话框出现时，请接受此认证 - 此认证是可以信赖的。详情请见第 252 页的*受信认证*。片刻之后，登录页出现：



3. 请提供您的 CC2000 用户名和密码*，然后点击**登录**。

注意：有一个预安装的系统管理员帐户，可用来进行首次登录，以创建用户和群组、添加设备、设定系统等等。此帐户的用户名是administrator；密码是password。为安全起见，我们强烈建议您将其修改为您自己的用户名和密码。详情请见第60页的*管理用户帐户*。

4. 如果您在使用 SMTP 认证，提供的 PIN 和 OTP*，然后点击登录。

注意：当使用SMTP认证，您应该键入分配给您的PIN密钥或OTP。关于MOTO信息，请参考第73页。

CC 界面

成功登录后，CC 网络页出现：

CC 网络页组的成部分在下一页的表格中描述。

页面组成部分

CC 的页面组成部分如下表所述：

编号	条目	功能描述
1	选项卡栏	选项卡栏包含 CC2000 的主要操作类别。出现在选项卡栏的项目取决于用户类型，及创建用户帐户时被选定的授权选项。
2	菜单栏	菜单栏包含与在选项卡栏选择的项目相关的、可操作的子类别。出现在菜单栏的项目取决于用户类型，及创建用户帐户时被选定的授权选项。
3	侧栏	侧栏提供树形视图清单，其列出与各种选项卡栏菜单栏选项相关的项目。点击侧栏中的某项目，则调出一个页面，页面显示与之相关的详细信息。
4	关于	关于提供关于 CC2000 当前版本的信息。
5	退出	点击此按钮，则退出 CC2000 会话。
6	欢迎信息	如果启用此功能(见第 31 页的*用户偏好*)，一个欢迎信息显示与此。
7	导航按钮	这些按钮使您移动经过侧栏树形图。其用法在本章的下一部分讨论。
8	交互显示面板	此处是主要工作区。出现的窗口反映您的菜单选项和侧栏项目选择。此面板的使用在本章稍后部分讨论 – 见第 29 页的*交互显示面板*。

导航按钮

这些按钮让您浏览侧栏树形图中的各项目，如下所述：

按钮	操作
	从当前选择移动到树形图中上一级且上一阶的项目(其母项目)。在下面的图例中，如果当前选择是*OutletA*，则移动到*PN0108RPSwitch*。
	从当前选择移动到树形图中同一级深度且上一阶的项目(其同辈项目)。在下面的图例中： ◆ 如果当前选择是*OutletB*，则移动到*OutletA*。 ◆ 如果当前选择是*PN0108RPSwitch*，则移动到*KN4132-23*。
	从当前选择移动到树形图中同一级深度且下一阶的项目(其同辈项目)。在下面的图例中： ◆ 如果当前选择是*KN4132-23*，则移动到*PN0108RPSwitch*。 ◆ 如果当前选择是*OutletA*，则移动到*OutletB*。
	从当前选择移动到树形图中下一级且下一阶的项目(其子项目)。在下面的图例中，如果当前选择是 *PN0108RPSwitch*，则移动到 *OutletA*。

不点击侧栏中的条目而使用导航按钮的优势之一在于从项目到项目移动时，您一直处在同一子菜单页面中。

> **注意**：当您选择菜单时，一个带有深层选项的子菜单栏出现在交互显示面板。见第29页的交互显示面板，及第30页的表格。

例如，如果您修改了 OutletA，您也想对 OutletD 做同样的修改，使用导航按钮，可方便地到达 OutletD 中的预期位置，不必点击经过所有子菜单才到达此位置。

但是，如果您通过在侧栏树形图点击某项目进行访问，此项目的开启页出现。要像修改 OutletA 那样，修改 Outlet，您不得不从首页开始，点击经过所有子菜单才到达预期位置。

> **注意**：如果此条目包括一个问号图标，表明设备信息与储存在CC2000数据库中的信息不匹配，如何解决此问题，请见第131页的*更新*部分。

树形图考虑事项

- 只有用户被授权访问的项目才出现在侧栏树形图中。
- 项目前面的加号(+)说明另有项目嵌套其内。点击加号，扩展树形图并显示被嵌套的项目。
- 当项目扩展后，加号变为减号(–)。点击减号，收缩树形图并隐藏被嵌套的项目。
- 对于设备来说，如果设备在线，其图标为彩色；如果设备离线，其图标为灰色。

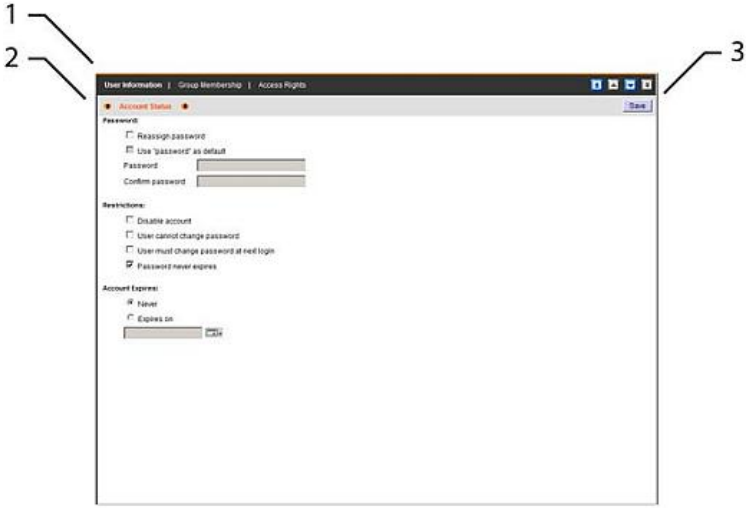
注意：用户可设定设备和端口在侧栏树形图中显示的方式。详情请见第31页的*用户偏好*。

交互显示面板

概述

交互显示面板(也称作主面板)是主要工作区。出现的窗口反映您的菜单选项和侧栏项目选择。称作交互显示面板的原因是，除了显示菜单选项的内容之外，它也是工作区，您可在此设定设置及在被选择的设备上执行操作。

典型的交互显示面板的说明如下所述：



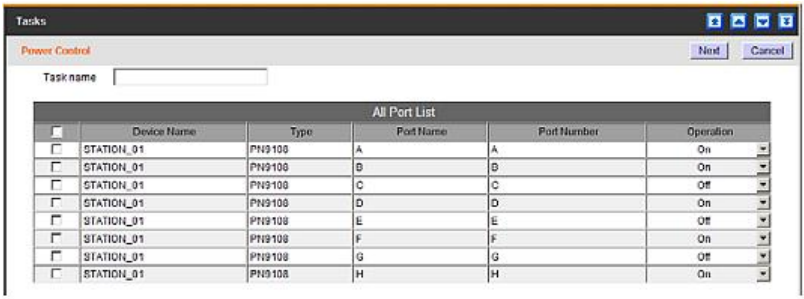
(接上页)

编号	条目	功能描述
1	子菜单栏	◆ 将菜单类别细化成较小的相关分组。 ◆ 如果有次级子菜单页，光标停在子菜单标题上，一个弹出菜单即会出现。点击菜单项目以进入想找的次级菜单页。

		◆ 出现在子菜单栏的项目取决于用户类型及创建用户帐户时所选的授权选项。
2	子菜单标题栏	◆ 描述子菜单类别。 ◆ 箭头图标说明含有次级子菜单页。点击下箭头图标按顺序进入下一页；点击上箭头图标按顺序进入上一页。
3	操作输入区	此处显示一个按钮或输入框，指导您执行关于当前页的操作(保存、删除、添加、下一页等等)。

选择列表项目

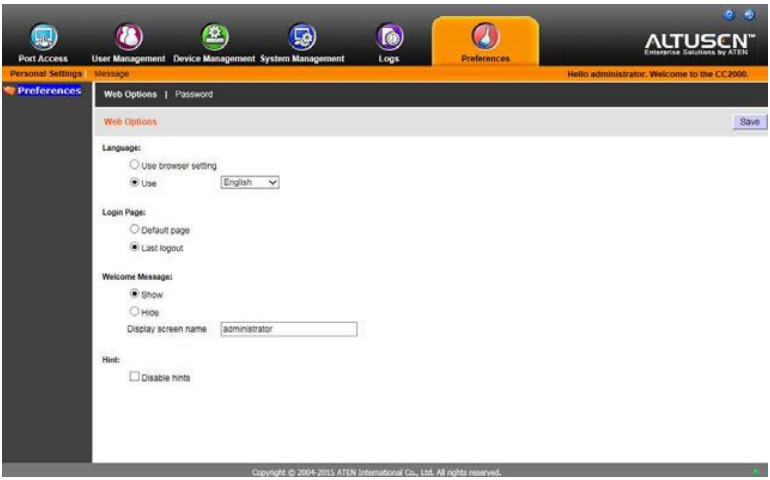
显示在交互显示面板中的许多页面都包含一个项目列表(设备、用户、群组、设定文件等)，可选择这些项目以执行某项操作。例如：



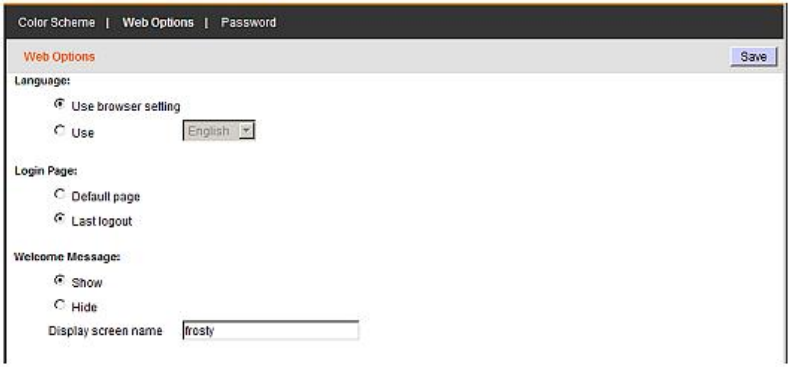
- 通过点击勾选项目名称前面的复选框，可以选择单个项目。
- 通过点击勾选项目栏顶部的复选框，可以选择所有项目。

用户偏好

通过点击选项卡栏上的 *Preferences* 选项卡，用户可为浏览器会话设置个人偏好。交互显示面板打开默认页面－网页选项卡。子菜单栏显示可选类别：*Web Options*(网页选项)和 *Password*(密码)。


Port Access
User Management
Device Management
System Management
Logs
Preferences
ALTUSCN
Enterprise Solutions by ATEN
Personal Settings | Message
Hello administrator, Welcome to the CC2000.
Preferences
Web Options | Password
Web Options
Save
Language:
Use browser setting
Use
English
Login Page:
Default page
Last logout
Welcome Message:
Show
Hide
Display screen name
administrator
Hint:
Disable hints
Copyright © 2004-2015 ATEN International Co., Ltd. All rights reserved.

网页选项


Color Scheme | Web Options | Password
Web Options
Save
Language:
Use browser setting
Use
English
Login Page:
Default page
Last logout
Welcome Message:
Show
Hide
Display screen name
frosty

- 对于 *Language*：
  - 点击 **Use Brower Settings** 单选按钮，以使 CC2000 的页面显示与浏览器设置的语言相同。

    注意：如果浏览器设为不支持的语言，CC2000则搜索服务器操作系统的语言设置。如果操作系统设为支持的语言，CC2000则使用此语言显示其页面。如果操作系统设为不支持的语言，CC2000则默认用英语。

  - 点击 **Use** 单选按钮，以下拉支持的语言列表，及使 CC2000 的页面显示您选择的语言。

    注意：此处选择的语言，如果与浏览器的设置不同，则只在登录后才生效。登录页将遵循*使用浏览器设置*的注意中所描述的顺序。

- 对于 *Login Page*：可以选择登录时使 CC 打开默认页 – 此页是选项卡栏上第一个可用选项卡的第一页 – 或者可以选择使 CC 打开您上次退出时所在的页面。

- 对于 *Welcome Page*：
  - 如果您想要欢迎信息出现于屏幕，则选择 **Show**；如果您不想要欢迎信息出现，则选择 **Hide**；
  - 如果您想要窗口名称和欢迎信息一起出现，则将窗口名称键入 *Display screen name* 文本框中。

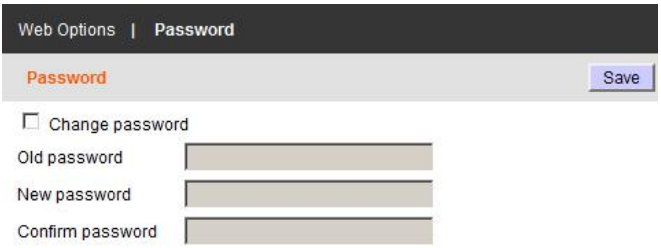
    注意：1. 这里提供一种修改在用户帐户中指定的窗口名称的方法。当在此修改名称时，用户帐户设置中的窗口名称条目自动改为在此指定的内容(见第56页的*添加用户帐户*)。

    2. 窗口名称将不会显示，除非您选择*显示*欢迎信息。

- 如果想禁用 mouse-over 提示，请点击 *Disable hints* 的复选框。

选择完成后，点击 **Save**。

密码

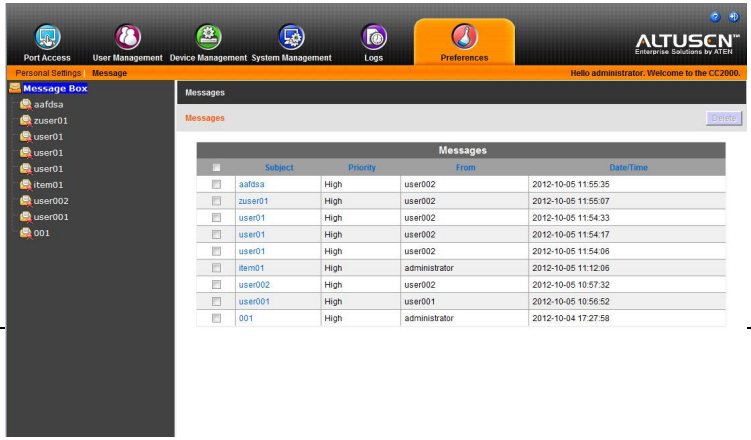


如果您要修改您的密码，请按如下操作：

1. 勾选 **Change Password**。这将启动密码输入区。
2. 在 *Old password* 区键入老密码。
3. 在 *New password* 区键入新密码。
4. 在 *Confirm password* 区再次键入新密码。
5. 点击 **Save**。

通知与信息框

在 *Preferences*(用户偏好)选项卡的 Message(信息)部分有通知系统选项，允许管理员发送通知至任意或所有 CC2000 用户。

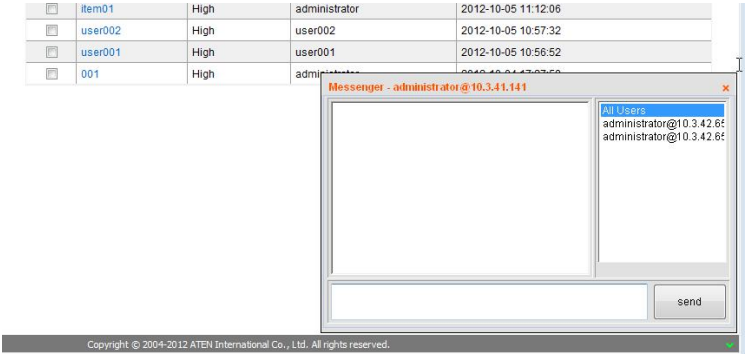


注意：仅管理员拥有此功能

此信息板为所有用户提供在线聊天式功能，当前登录到 CC2000 的用户可通过此功能相互沟通。

当用户收到邮件时，邮件图标  会出现在右下页面的角落。在读的时候，图标变为一个 V 型。

点击信息框右下角的绿色 V 型图标，可开启/禁用聊天窗口。

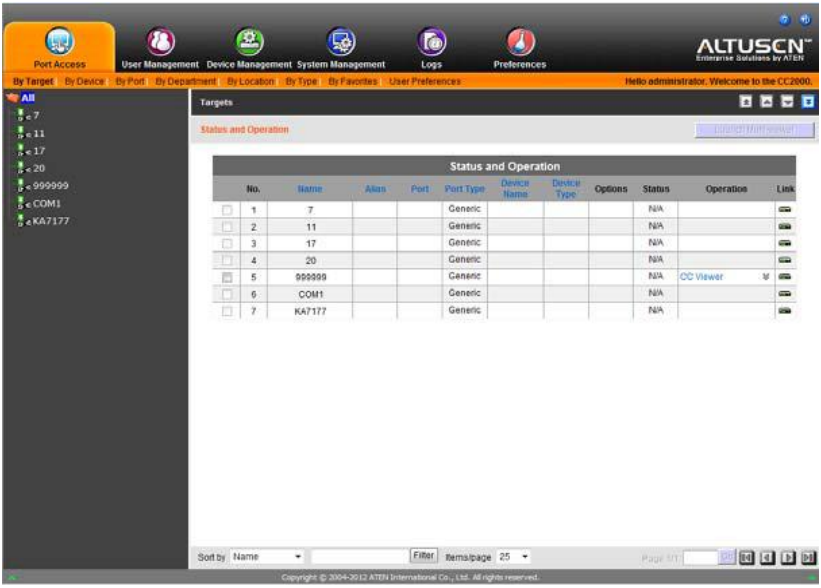


注意：此聊天功能在整个界面都可用

第四章
端口访问

概述

端口访问 页面用于访问并控制通过CC2000网络管理的设备、端口和插座。页面的选单栏提供这些项目的不同的组织视图，入下面截屏所示：



点击选单栏中想要查看的项目。此时可以按照下文描述对项目进行操作。

注意：若用户没有访问权限，端口访问选项卡和访问页面不会显示出来 – 系统管理员异同。

标题栏

下表提供了各栏标题的解释。

注意：1. 表格上面的标题不会出现在每个视图中。哪些标题会显示取决于所选的视图。

2. 可以通过在栏中点击改变项目分类顺序。

标题	解释
Name（名称）	添加到CC2000架构中时为端口赋予的名称。
Alias（别名）	若为端口赋予了别名，其别名将在此处显示。
Port（端口）	设备端口的端口编号。
Port Type（端口类型）	表示端口所属设备的设备种类。
Device Name（设备名称）	端口所属设备的设备名称。
Device Type（设备类型）	端口所属设备的设备类型（SNxxx、PNxxx、KNxxx、刀片等等）
Options（选项）	◆ KVM端口：指示端口的*访问模式* 。详见第138页。 ◆ 串口端口：指示端口的*操作模式* 。详见第151页，*端口设置* 。 ◆ 电源插座：指示端口的 *电源管理配置*。详见第145页，*端口设置* 。
Status（状态）	◆ KVM端口：指示端口联机或脱机。 ◆ 串口端口：指示端口联机或脱机。 ◆ 电源插座：指示插座端口的电源插座开启或关闭。 **注意**：此类别不适用于刀片机箱，因此Blade Chassis（刀片机箱）区会显示*N/A*（不适用），个别刀片处将显示为*Unknown*（未知）。
IP Address（IP地址）	实体设备 – 设备的IP地址在此处显示。
MAC Address（MAC地址）	实体设备 – 设备的MAC地址在此处显示。
Operation（操作）	访问设备/端口的默认操作在此单元格中显示。 ◆ 点击单元格右侧的箭头查看其他可用操作（如有）。 ◆ 点击选择的项目，打开设备/端口对话框。各种设备/端口操作选项将在接下来的*端口操作* 章节进行描述。
Link（链接）	点击可前往设备的设备管理 → 端口页面。

执行按钮

主界面上有两个按钮：页面下方的*Filter*（筛选），和页面右上角的*Launch Multiviewer*（启动多检视器）。

筛选

筛选功能允许您控制出现在主界面列表上的项目。输入字符串并点击**Filter**（筛选）（或按下**[Enter]**）。只有有输入的特定字符串的项目显示在列表上。

例如，若您输入*TD* ，只会显示名称中包含TD的项目，例如*TD-AGG-01* 。

Sort By（分类方式）：如要对现实在主界面上的设备进行分类，使用**Sort by**（分类方式）选单，选择分类方式：*Name*（名称）、*Alias*（别名）、*Type*（类型）、*IP Address*（IP地址）或*MAC Address*（MAC地址）。

Items/Page（项目/页面）：使用此下拉选单选择您希望现实在页面上的设备数量。选项为：*25*、*50*、*75*、*100* 和*400* 。为了避免加载速度过慢，每页可显示设备的最大数量为400。

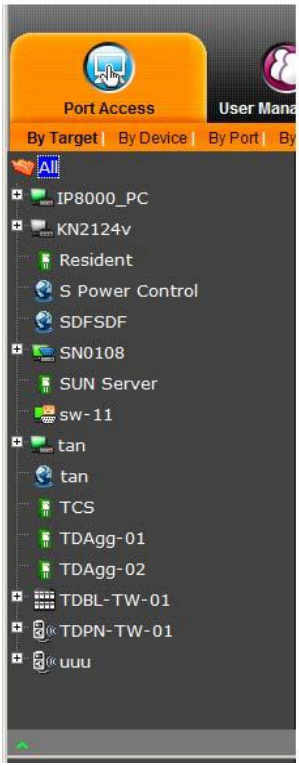
如要清除筛选重新显示完整列表，删除输入框中的内容并再次点击**Filter**（筛选）。

启动多画面

如要一次启动多个端口的查看器，勾选您想要访问的端口名称前面的勾选框，然后点击**Launch Multiviewer**（启动多画面）。

侧边栏

在CC2000上进行过设定的设备、端口和插座在屏幕左侧侧边栏的树状图中列出。



侧边栏特点

侧边栏树状图特点如下：

- 用户只允许查看有权限的设备、端口和插座。
- 端口/插座和子设备可以嵌套在其母设备下。
  - 点击设备前的+可以展开树状图，查看嵌套在其下的端口/插座。点击-收起树状图并隐藏嵌套在其下的端口/插座。
  - 为了更快地进行访问，树状图收起并且必须为节点访问展开。每2000节点树状图即分割成一个单独的文件夹，这样页面可以更快地显示。
- 联机的切换器和端口其显示屏幕图标为绿色；脱机的切换器和端口其显示其屏幕图标为灰色。

- 点击树状图中的某一项目将出现*Status and Operation*（状态和操作）页面。
- 双击某一活跃设备或端口打开启其检视器。
- 右击某一活跃设备或端口可打开一个弹窗，允许您选择某一检视器进行访问（详见第40页，*端口操作* ）。

侧边栏筛选

Filter（筛选）功能允许您控制显示在侧边栏的设备、端口和插座的数量和类型。点击侧边栏界面左下方的漏斗图标，将弹出筛选对话框，与下图类似：

下表为选项含义的检视：

选项	说明
All（全部）	默认查看。没有选择其他筛选选项，用户可访问的所有设备、端口和插座都在侧边栏列出。 下拉列表框可查看所有可用选项，选择其中一项。只有符合选项的项目显示在树状图中。
Online（联机）	若您选择*Online*（联机）（勾选勾选框），只有联机的项目显示在树状图中。
Search（搜索）	若您输入搜索字符串并点击**Search**（搜索），只有名称符合搜索字符的设备、端口和插座显示在树状图中。支持万用符号（?和*），所以列表中可显示多个项目。例如，如果输入**Web***，Web Server 1和Web Server 2都会出现在列表中。

如要关闭筛选对话框，请点击侧边栏界面左下角的倒三角符号。

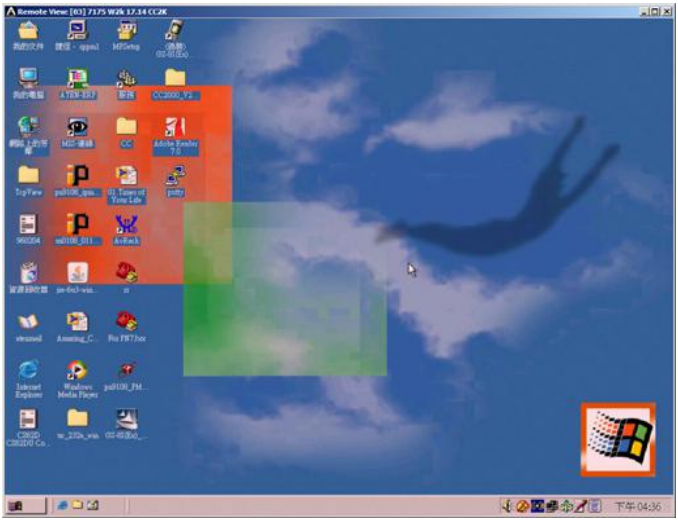
端口操作

根据所选项目不同，有多重可用的访问和控制端口操作的方式。点击操作单元格右侧的箭头可选择操作方式，如下文所述。

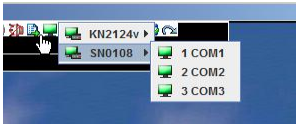
CC检视器

点击CC检视器直接打开在选中端口上运行的KVM或串口检视器。其效果与直接登入设备后在设备GUI上选择端口相同。

例如，43页屏幕截图的TD-AGG-01是一台包含一台KN2124v KVM多电脑切换器、一台PN0108PDU和一台SN0108串口设备的整合设备。点击*CC Viewer*（CC检视器）时，将出现一个窗口，其中有选中的整合设备中KN2142v的第一个端口：



如果要在检视器中切换端口，打开隐藏的控制面板（鼠标滑到检视器串口上方中央），选择*Port List*（端口列表）图标。端口列表选项中包涵设备的所有端口。

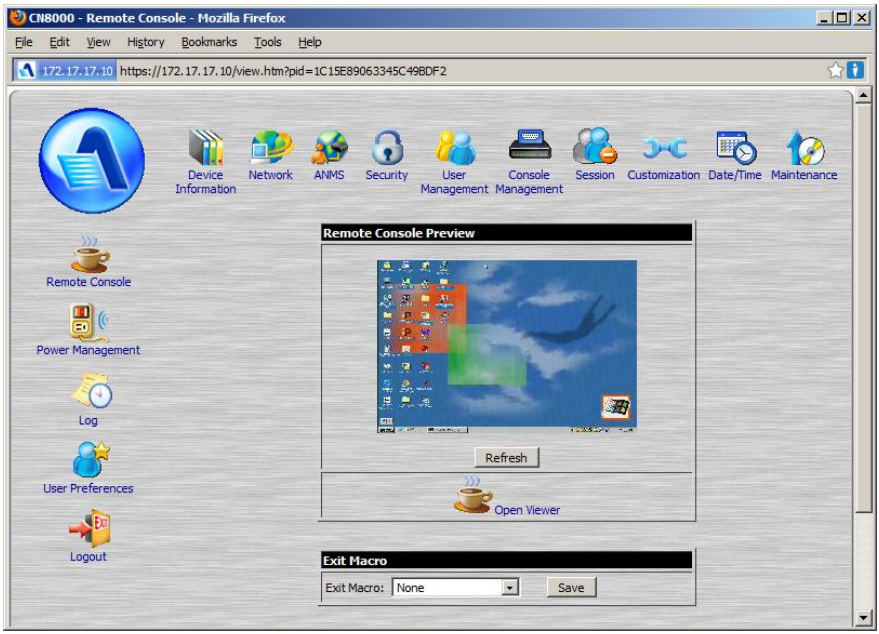


- 在列表中，选择所属设备（截图中为SN0108）,点击想要访问的端口。
- 设备或端口名称（端口ID）显示在CC检视器的标题栏。
- 每个端口的检视器窗口都有一个隐藏的控制面板。如要切换到设备的不同端口，请打开端口列表并点击想要访问的端口。
- 若目标设备与PDU相关联，额外的电源控制将出现在CC检视器的控制面板中。
- 完成会话后，打开控制面板并选择*Exit*（退出）图标。

注意：CC检视器不支持OpenJDK。

网页访问

点击Web Access（网页访问）打开桌面设备的浏览器会话，其效果与打开浏览器在地址栏登入相同：



电源开启/关闭

- 对于整合和电源设备，可以选择全部开启或全部关闭，也可开启或关闭所有属于该设备的插座。
- 对于电源插座，可以选择开启或关闭。如果端口的状态为开启，选项为关闭 – 点击OFF关闭插座电源。

注意：离开页面并返回后，变化才会再表格中体现出来。

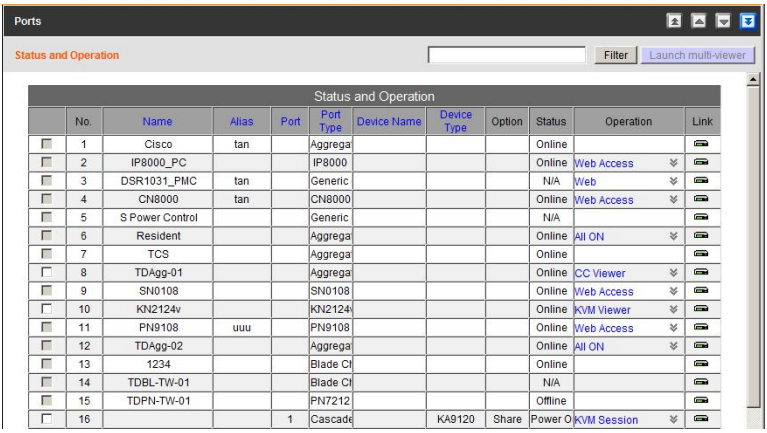
SSH/远程登入会话

选择打开选中端口的SSH或远程登入会话。您将获得SSH或远程登录检视器，其效果与使用浏览器登入串口设备（如SN0108）并在网络主页选择*Telnet*（远程登入）效果相同。

端口访问视图

端口视图

在选项卡栏中选择端口访问后，默认页面为端口视图。此页面列出所有在CC2000管理系统下分配的端口，独立于其设备：

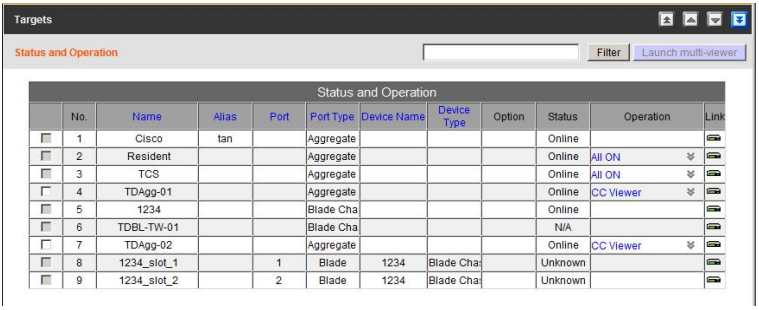


	No.	Name	Alias	Port	Port Type	Device Name	Device Type	Option	Status	Operation	Link
	1	Cisco	tan		Aggrega				Online		
	2	IP8000_PC			IP8000				Online	Web Access	
	3	DSR1031_PMC	tan		Generic				N/A	Web	
	4	CN8000	tan		CN8000				Online	Web Access	
	5	S Power Control			Generic				N/A		
	6	Resident			Aggrega				Online	All ON	
	7	TCS			Aggrega				Online		
	8	TDAgg-01			Aggrega				Online	CC Viewer	
	9	SN0108			SN0108				Online	Web Access	
	10	KN2124v			KN2124v				Online	KVM Viewer	
	11	PN9108	uuu		PN9108				Online	Web Access	
	12	TDAgg-02			Aggrega				Online	All ON	
	13	1234			Blade Ch				Online		
	14	TDBL-TW-01			Blade Ch				N/A		
	15	TDPN-TW-01			PN7212				Offline		
	16			1	Cascade		KA9120	Share	Power O	KVM Session	

如要单独查看某一端口，在侧边栏点击该端口。

目标视图

目标视图包括整合设备、刀片机箱（独立刀片）和虚拟机。目标页面默认视图选择了侧边栏顶部的*All*（全部），*Status and Operation*（状态和操作）页面显示在交互显示面板中。

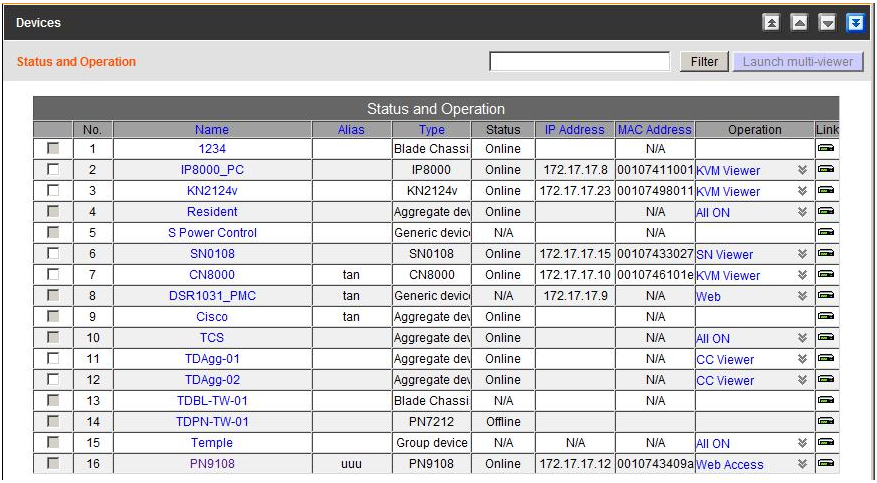


	No.	Name	Alias	Port	Port Type	Device Name	Device Type	Option	Status	Operation	Link
	1	Cisco	tan		Aggregate				Online		
	2	Resident			Aggregate				Online	All ON	
	3	TCS			Aggregate				Online	All ON	
	4	TDAgg-01			Aggregate				Online	CC Viewer	
	5	1234			Blade Cha				Online		
	6	TDBL-TW-01			Blade Cha				N/A		
	7	TDAgg-02			Aggregate				Online	CC Viewer	
	8	1234_slot_1		1	Blade	1234	Blade Cha		Unknown		
	9	1234_slot_2		2	Blade	1234	Blade Cha		Unknown		

如要单独查看某一设备，在侧边栏点击该设备。

设备视图

设备视图显示所有在CC2000管理系统下分配的设备：

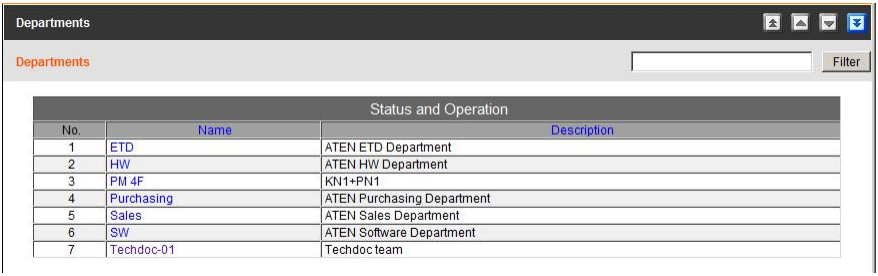


No.	Name	Alias	Type	Status	IP Address	MAC Address	Operation	Link
1	1234		Blade Chassi	Online		N/A		
2	IP8000_PC		IP8000	Online	172.17.17.8	00107411001	KVM Viewer	
3	KN2124v		KN2124v	Online	172.17.17.23	00107498011	KVM Viewer	
4	Resident		Aggregate dev	Online		N/A	All ON	
5	S Power Control		Generic devic	N/A		N/A		
6	SN0108		SN0108	Online	172.17.17.15	00107433027	SN Viewer	
7	CN8000	tan	CN8000	Online	172.17.17.10	0010746101e	KVM Viewer	
8	DSR1031_PMC	tan	Generic devic	N/A	172.17.17.9	N/A	Web	
9	Cisco	tan	Aggregate dev	Online		N/A		
10	TCS		Aggregate dev	Online		N/A	All ON	
11	TDAgg-01		Aggregate dev	Online		N/A	CC Viewer	
12	TDAgg-02		Aggregate dev	Online		N/A	CC Viewer	
13	TDBL-TW-01		Blade Chassi	N/A		N/A		
14	TDPN-TW-01		PN7212	Offline				
15	Temple		Group device	N/A	N/A	N/A	All ON	
16	PN9108	uuu	PN9108	Online	172.17.17.12	0010743409a	Web Access	

如要单独查看某一设备，在侧边栏点击该设备。

门类视图

门类视图显示所有在CC2000管理系统下创建的门类以及各门类所指定的端口：



No.	Name	Description
1	ETD	ATEN ETD Department
2	HW	ATEN HW Department
3	PM 4F	KN1+PN1
4	Purchasing	ATEN Purchasing Department
5	Sales	ATEN Sales Department
6	SW	ATEN Software Department
7	Techdoc-01	Techdoc team

如要单独查看某一门类的端口，在侧边栏点击该门类。

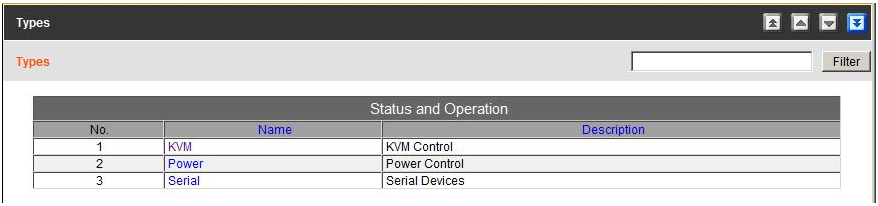
位置视图

位置视图显示所有在CC2000管理系统下创建的位置以及各位置所指定的端口：

如要单独查看某一位置的端口，在侧边栏点击该位置。

类型视图

类型视图显示所有在CC2000管理系统下创建的位置以及各类型所指定的端口：

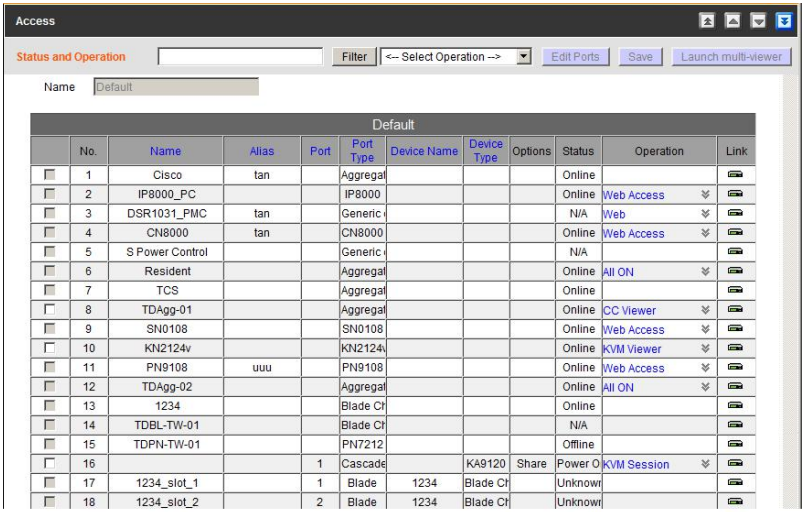


如要单独查看某一设备类型，在侧边栏点击该类型。

收藏夹视图

Favorites（收藏夹）页面与书签功能类似。经常访问的设备和端口可以在此处所选择的收藏名称下保存。只需打开此页面并选择名称 – 无需在侧边栏搜索设备和端口。该功能尤其适合在大型、拥挤的架构中使用。

在选单栏选择收藏夹后，默认页面将会出现，并列出所有在CC2000管理系统下分配的设备和端口：



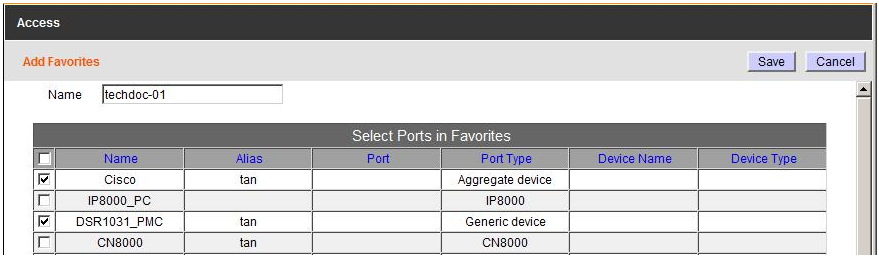
注意：*Filter*（筛选）和*Launch Multiviewr*（启动多画面）运作方式与其他视图页面相同。

添加收藏

如要添加收藏并将其填入端口，按下述操作：

1. 下拉*Select Operation*（选择操作）列表，选择**Add Favorites**（添加收藏）。

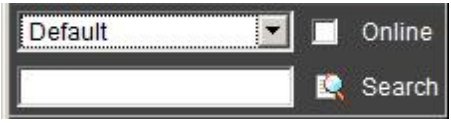
2. 在出现的页面中，为收藏命名，点击想要加入的端口勾选框，点击**Save**（保存）。



操作完成后，收藏将显示在主界面中，也会再侧边栏列出。

查看收藏

侧边栏的地步有一个筛选界面，可以控制显示在此页面的项目：



按下表说明使用筛选功能：

默认	说明
Default（默认）	默认视图。没有选择其他筛选选项，用户可访问的所有端口都在侧边栏列出，并在主界面显示。 如果创建了*收藏*，您可以下拉列表框，选择您想要查看的项目。选择某项收藏后，只有您选择的项目会显示在侧边栏和主界面上。
Online（联机）	若您选择*Online*（联机）（勾选勾选框），只有连接设备联机的端口出现在侧边栏和主界面上。
Search（搜索）	若您输入搜索字符串并点击**Search**（搜索），只有名称符合搜索字符的端口显示在侧边栏和主界面上。支持部分输入，所以如果输入**Web**，任何名称中含有*Web* 的端口都会出现在侧边栏和主界面上。

管理收藏夹

从收藏夹中添加或移除端口，请按下述操作：

1. 从筛选列表中选择收藏夹。
2. 点击Edit Ports（编辑端口）（界面右上角）。

   出现一个页面，显示用户可访问的所有端口，以及当前包含在收藏夹并被勾选的端口。

Access

Ports in Favorites　Save　Cancel

Select Ports in Favorites

	Name	Alias	Port	Port Type	Device Name	Device Type
☐	Cisco	tan		Aggregate device		
☐	IP8000_PC			IP8000		
☐	DSR1031_PMC	tan		Generic device		
☑	CN8000	tan		CN8000		
☐	S Power Control			Generic device		
☐	Resident			Aggregate device		
☐	TCS			Aggregate device		
☑	TDAgg-01			Aggregate device		
☑	SN0108			SN0108		
☐	KN2124v			KN2124v		
☐	PN9108	uuu		PN9108		
☑	TDAgg-02			Aggregate device		
☐	1234			Blade Chassis		
☐	TDBL-TW-01			Blade Chassis		
☐	TDPN-TW-01			PN7212		
☐			1	Cascade Port		KA9120
☐	1234_slot_1		1	Blade	1234	Blade Chassis

3. 勾选想要加入到收藏夹的端口；取消勾选想从收藏夹中移除的端口。
4. 点击**Save**（保存）。

仪表盘

仪表盘 页面提供所有设备的分类快速视图。仪表盘可让您通过颜色查看每一设备的状态，并提供*Port Status and Operations*（端口状态和操作）页面的链接。

使用页面右上角的下拉选单选择设备分类。选择某一类别后，该类别下的设备将通过此类型下拉选单的颜色标记显示，白色背景的设备不在所选类别中。

联机设备以白色文本和深色背景显示：

脱机设备以黑色文本和浅色背景显示：

未被监控的没有支持开关状态协议的设备，如URL，总是显示**联机**。

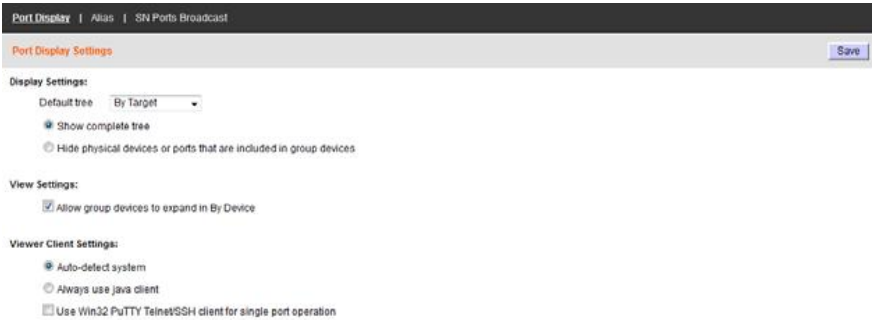
双击任一设备弹出*Port Status and Operations*（端口状态和操作）页面。

用户偏好

选单栏的最后一个项目，*User Preferences*（用户偏好），与选单栏的其他项目不同，因为其不提供设备和端口组织性的视图。它有两个界面选单项目：*Port Display*（端口显示）和*Alias*（别名）。端口显示允许您设定设备树状图如何在侧边栏显示；别名允许您为设备和端口设定昵称。

端口显示

端口显示页面是您选择*User Preferences*（用户偏好）后打开的默认页面。



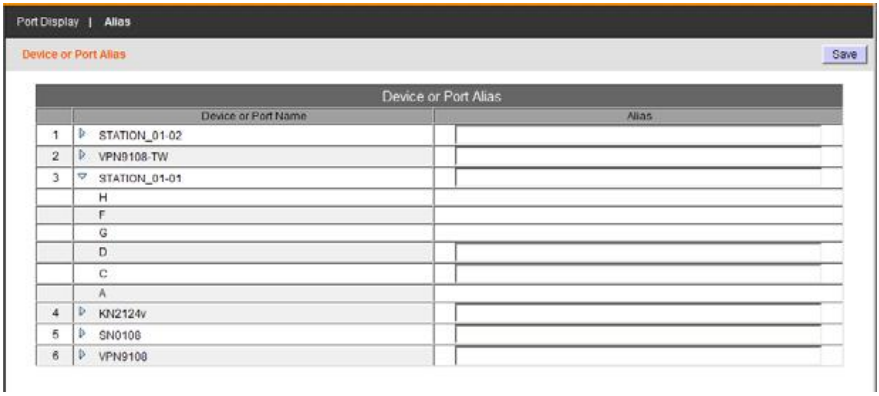
显示设置的说明在下表中列出：

项目	说明
Display Setting（显示设置）	◆ 下拉列表，选择您希望点击Port Access（端口访问）选项卡后想看到的页面。 ◆ 如果您选择**Show Complete tree**（显示完整树状图），点击展开树状图后，所有嵌套的设备和端口都会显示出来。 ◆ 如果您选择**Hide physical devices or ports that are included in group devices**（隐藏包含在设备组中的实体端口或设备），点击展开树状图后，设备组中的实体端口将不会在其初始设备下显示。
View Setting（视图设置）	若您选择**Allow group devices to expand in By Device**（允许设备组根据设备展开），嵌套在整合设备或设备组中的端口也会显示在树状图中。否则，设备组前不会有额外的标志，其端口也不会显示。

项目	说明
Viewer Client Setting（检视器客户端设置）	◆ 若您选择**Auto-detect system**（自动侦测系统），CC2000将检测您是否使用IE登入。如果您使用IE登入，访问设备或端口时将打开Windows Client Viewer。如果您使用IE之外的浏览器登入，将打开Java Client Viewer。 ◆ 若您选择**Always use java Client**（总是使用Java客户端），无论您使用何种浏览器登入，CC2000都将打开Java Client Viewer。 ◆ 勾选**Use Win32 PuTTY Telnet/SSH client for single port operation**（使用Win32 PuTTY Telnet/SSH客户端进行单一端口操作），通过CC2000连接串口设备时将打开PuTTY Telnet/SSH客户端软件。

别名

选择界面选单的*Alias*（别名），将弹出一个页面，允许您为您的设备、端口和插座设置别名，便于记忆和管理：

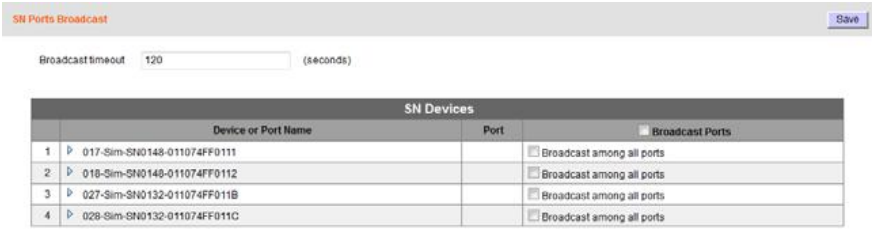


- 默认视图只显示设备。如要为某一端口或插座设置别名，点击设备名称前的箭头以显示。
- 在Alias（别名）区为对应设备、端口或插座输入别名。返回到组织视图页面后，别名将代替设备或端口名称出现在侧边栏。

注意：别名只对创建别名的用户显示。其他用户看到的事原始名称（或者其创建的别名）。

SN端口广播

在界面选单中选择*SN Ports Broadcast*，将弹出一个页面，允许您通过选择勾选框选择串口设备的端口，接收广播命令。选择多个广播端口允许您对单一串口端口进行访问并作出变更，同样的变更将应用于所有广播端口。



为了使用广播功能，您必须使用SNViewer访问一个广播端口，并开启控制面板上的广播功能。详见SN0148用户说明书的第38页，*控制面板功能* 。

广播超时：如果在设定的指定时间内没有用户输入，广播功能（对其他端口）将自动结束。输入0-240秒之间的数值。设置为0效果与关闭此功能相同。

选择**Broadcast Ports**（广播端口）将勾选所有串口端口并作出变更。

选择**Broadcast among all ports**（对所有端口广播）将勾选所有串口端口中的特定串口设备。您也可以展开串口设备，选择单独的端口进行广播。

注意：CC2000只列出连接在支持广播端口的切换器上的串口设备。

此页刻意留白

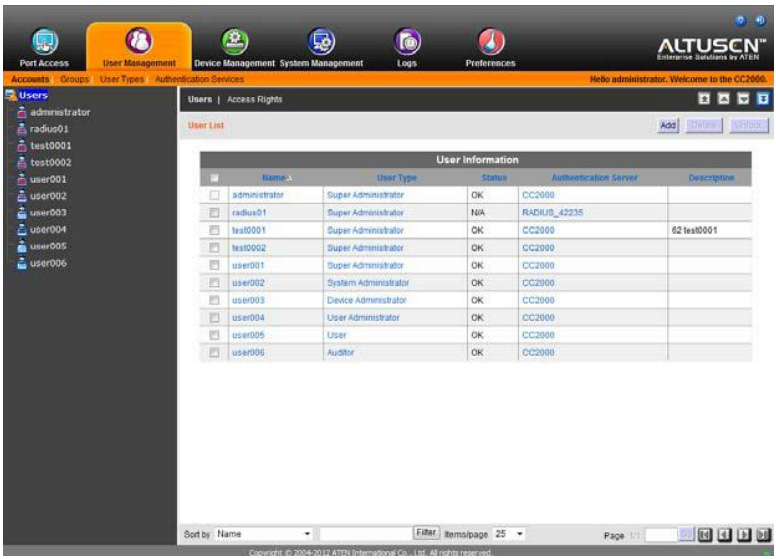
第五章
用户管理

概述

User Management(用户管理)页用来执行如下功能：

- 添加、修改和删除用户帐户
- 创建用户群组及向其分配用户
- 根据系统默认值或自定义的用户类型，为用户和群组指定设备访问权
- 指定用户的验证是通过 CC2000(内部)还是通过外部验证服务器执行

当点击 User Management 选项卡时，CC2000 打开默认的*帐户*页，其看起来类似如下窗口：



所有用户和群组都列于侧栏树形图和交互显示面板。要访问任何用户或群，点击其位置中的名称即可。

注意：用户管理页限于系统管理员和用户管理员使用。其他类型用户可跳过本章。

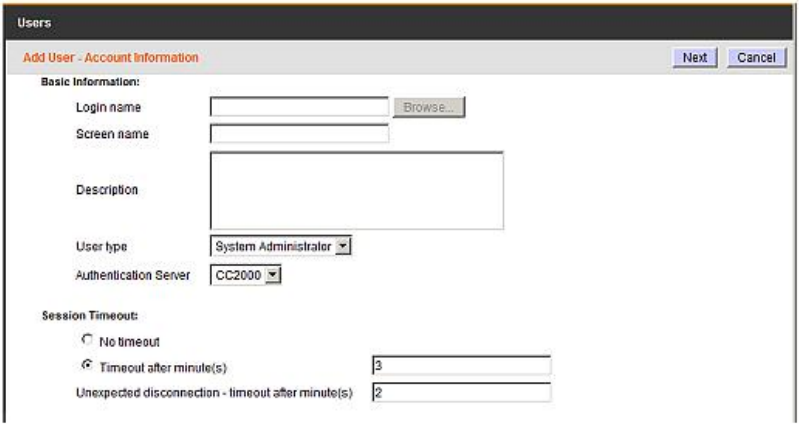
帐户

Accounts(帐户)页用来添加、修改和删除用户帐户。默认帐户页看起来类似如下：

添加用户帐户

添加用户帐户，请按如下操作：

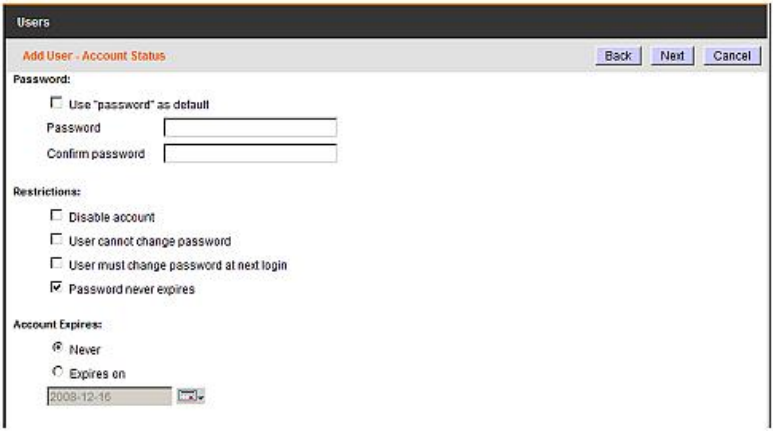
1. 在侧栏选择 **Users**。
2. 点击主面板右上方的 **Add**。*Add User - Account Information* 页出现：



3. 在正确的区域输入要求的信息。各区的描述在下面的表中给出：

区域	描述
Login name (登录名)	**内部(CC2000)帐户**：最多允许 16 个英文数字字母字符。最少字符数基于 CC2000 的帐户策略设置(见第 75 页的 *CC2000 验证*)。 **外部验证**：登录名应该是存在于外部验证服务器上的登录名。 **注意**：1. 这些外部服务器仅提供验证服务 – 不提供授权服务。授权由 CC2000 管理系统提供，因此访问权需要在 CC2000 内设置。 2. 如果 LDAP、LDAPS 或 Active Directory 被选作外部验证服务器，可通过点击 Browse 并从第三方验证服务器提供的列表中选择用户，来自动填写登录名。
Description (描述)	关于您希望包括的关于用户的额外信息。最多允许 256 字节。
User Type (用户类型)	下拉列表以选择您要向其分配新用户的用户类型。关于用户类型的信息，见第 69 页。
Authentication Server (验证服务器)	对于由 CC2000 进行的验证，不用管此选择。对于由外部验证服务进行的验证，下拉列表以选择您要使用的外部验证服务器。 **注意**：做出选择之前，必须先添加外部验证服务器。详情请见第 76 页的*外部验证服务器*。
用户 base RDN	如果认证服务器是一个 LDAP 服务器，用户群 RDN 设置必须在这个领域。
Session Timeout (会话超时注销)	如果您不想使用户在指定时间一直闲置之后被会话超时注销，选择 *No timeout* 单选按钮。 如果如果您想使用户在指定时间一直闲置之后被会话超时注销，选择 *timeout after* 单选按钮。有效设置为 1-99 分钟。默认为 3 分钟。 **注意**：此设置与网络登录会话相关。
Unexpected disconnection timeout (意外连接中断超时注销)	如果用户意外中断连接(即关闭浏览器)，在此指定的时间之后，CC2000 超时注销用户的会话。超时注销间隔为 3-10 分钟；默认为 3 分钟。

4. 点击主面板右上方的 **Next**。如果选择 CC2000 进行验证，*Add User - Account Status* 页出现：



注意：如果选择外部验证服务器进行验证，帐户状态信息保持在那台服务器，所以此页不出现。您反而直接进入*Add User - Personal Information*页(见步骤 5)。

各区的如下表所描述：

区域	描述
Password (密码)	◆ 启用 *Use "password" as default*，则设置 **password** 作为用户的密码。 ◆ 如果不启用 *Use "password" as default*，则在 *Password* 区输入用户的密码。最多允许 16 个英文数字字母字符。最少字符数基于 CC2000 的帐户策略设置(见第 75 页的 *CC2000 验证*)。 ◆ 为确保密码中无错误，在 *Confirm Password* 区再输入一遍。两次输入必须一致。

区域	描述
Restrictions (限制)	◆ *Disable account* 无需删除而暂时取消用户帐户－这样将来可轻松恢复帐户。 ◆ 如果启用 *User cannot change password*，用户不能修改密码。否则，用户可使用 *Preferences* 选项卡修改自己的密码。详情请见第 33 页的*密码*。 ◆ 如果启用 *User must change password at next login*，用户下次登录时必须修改其密码。 ◆ 启用 *Password never expires*，则预防用户的密码在一定时间后过期。此功能覆盖在 CC2000 帐户策略设置中所设的影响整个系统的设定(见第 75 页的 *CC2000 验证*)。 **注意**：启用某些限制功能将自动禁用其它限制功能。
Account Expires (帐户过期)	◆ 点击 *Never* 单选按钮，设置帐户永远不过期。 ◆ 要使帐户在特定日期过期，点击 *Expires on* 单选按钮；然后点击日历图标以选择过期日期。

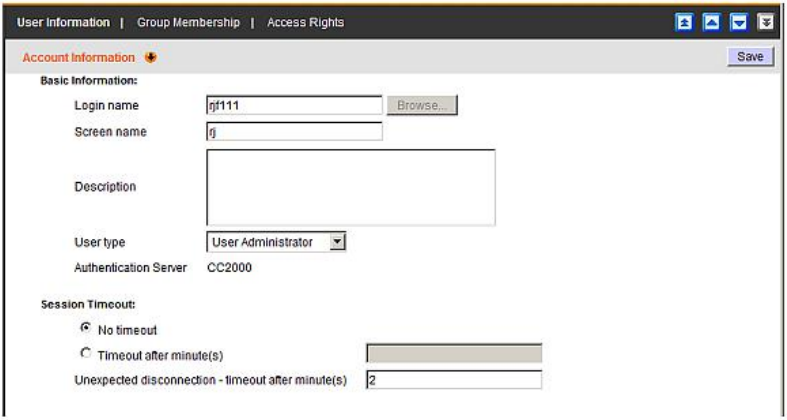
5. 点击主面板右上方的 **Next**。*Add User - Personal Information* 页出现。
   此页上的各区是可选项。您可以使它们留白，或喜欢填写多少就填写多少。
6. 当完成 *Add User - Personal Information* 页后，点击主面板右上方的 **Save** 以完成操作并添加用户到用户列表。
   此页面允许您设置存在安装下的设备和端口的用户访问权限。详见访问权限，第 61 页的信息设置。
7. 当您完成设置用户的访问权限，单击保存在主面板的右上方添加用户用户列表，并打开访问权限摘要页。详见第 61 页访问权限。

注意：如要添加新用户，您必须点击侧边栏的用户。

管理用户帐户

管理用户帐户，请按如下操作：

1. 在列表面板选择用户 **Users**。
2. 或是在列表面板点击用户名，或是在交互显示面板点击用户名，用户帐户信息页出现：



此页于 Adding a user account 页相似，除了顶部有三个子菜单项目：User Information (用户信息)、Group Membership (群组成员资格)和 Access Rights (访问权)。

用户信息

此子菜单项目包含添加用户帐户步骤中的所有三个页面(见第 56 页)。要修改这些页面上的信息，或是通过点击箭头图标按顺序经过这些页面，或是通过停留在菜单上并从出现的弹出菜单选择页面，而直接到某页面。

群组成员资格

点击此子菜单项目，打开一个页面，其列出某用户所属的所有群组。可点击列表中的群组名，以到群组的*群组信息*页。关于此页的详细说明，见第 66 页的*群组*。

访问权限

如要设定某一用户对设备、端口和插座的访问权限，按下述操作：

1. 在选单栏选择**Accounts**。
2. 在侧边栏选择用户。
3. 在交互显示面板选单栏选择**Access Rights**（访问权限），打开用户的*Access Rights*（访问权限）页面。

如果用户未被指派设备，出现的页面如下所示：

注意：访问权限不必总是单独指派。详见第63页，*复制/粘贴访问权限* 。

■ 添加设备访问

如要添加用户可以访问的设备，按下述操作：

1. 点击界面右上方的**Add**（添加）。

   将出现一个列出结构中所有设备的页面：

2. 勾选您希望用户能够访问的设备、端口和插座。

3. 对于每一项设备、端口和插座，点击*Configuration Rights*（配置权限）栏的箭头，为该项目设置用户的配置权限。**Allowed**（允许）代表用户可以对设备或端口进行设置；**Denied**（拒绝）表示用户无法对该设备或端口进行设置。
4. 对于每一项设备、端口和插座，点击*Access Rights*（访问权限）栏的箭头，为该项目设置用户的访问权限。访问权限说明见下表：

权限	端口类型	说明
Full access and VM (Read/Write) 完全访问和VM（读/写）	KVM	用户可以访问设备（或设备上的指定端口）、查看屏幕并用键盘和鼠标执行输入/输出操作。用户也有使用虚拟媒体功能的读/写权限。
Full access and VM (Read Only) 完全访问和VM（只读）		用户可以访问设备（或设备上的指定端口）、查看屏幕并用键盘和鼠标执行输入/输出操作。用户对虚拟媒体也有只读权限。
Full Acess 完全访问		用户可以访问设备（或设备上的指定端口）、查看屏幕并用键盘和鼠标执行输入/输出操作。
View Only 仅查看		用户可以访问设备（或设备上的指定端口）、查看屏幕，但无法执行任何操作。
No access 无访问		用户没有对设备(或设备上的指定端口)的访问权限。设备（或指定端口）不会出现在*Port Access*（端口访问）侧边栏或列表中。
Allowed 允许		允许用户设定设备（或设备上的指定端口）的电源状态。
Denied 拒绝		不允许用户设定设备（或设备上的指定端口）的电源状态。设备（或指定端口）不会出现在*Port Access*（端口访问）侧边栏或列表中。
Telnet 远程登入	串口	设备（或设备上的指定端口）必须通过远程登入连接访问。
SSH		设备(或设备上的指定端口)必须通过SSH连接访问。
Administrator 管理员	ATEN Generic; Web SSO	管理员可执行所有配置和操作。

权限	端口类型	说明
User 用户	ATEN Generic; Web SSO	用户可以执行所有操作。
View only仅查看		用户可以查看屏幕，但不能执行任何操作
No access 无访问		用户无访问权限，网页访问选项不会出现在端口访问页面。

5. 作出选择后，点击**Save**（保存）。
6. 如要为额外的设备添加访问，打开用户的访问权限页面并重复上述步骤。

■ **修改设备访问**

如要变更对某一设备、端口或插座的访问权限，打开用户的访问权限页面；配置权限和访问权限，修改为期望的项目；点击**Save**（保存）。

■ **移除设备访问**

如要移除对某一设备、端口或插座的访问权限，打开用户的访问权限页面；勾选想要移除的设备前面的方框；点击**Delete**（删除）。

■ **管理设备**

您可以通过在*设备名称* 或*端口名称* 列表中点击，打开设备、端口或插座的管理页面。

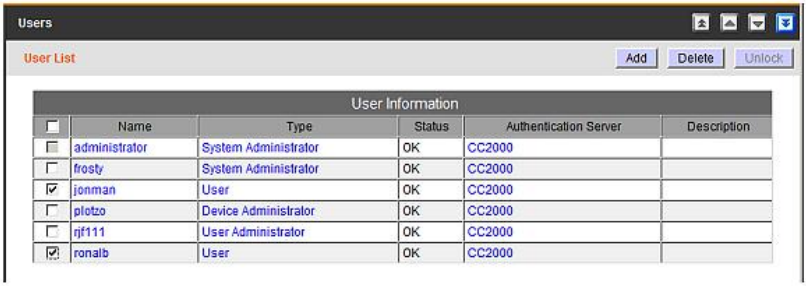
复制/粘贴访问权限

访问权限复制-粘贴功能可在兼容的节点间（如用户到用户）开启。如要使用此功能，在侧边栏树状图中，右击用户名称并选择*copy access right*（复制访问权限） 。右击另一用户并选择*paste access right*（粘贴访问权限）。

删除用户帐户

删除用户帐户，请按如下操作：

1. 在列表面板选择 **Users**。
2. 在交互显示面板，点击勾选您要删除的用户。



注意：通过按您所需勾选多位用户，您可以删除多位用户。通过勾选栏目顶部的框，您可以删除所有可删除的帐户。

3. 做完选择后，点击面板右方的 **Delete**。
4. 出现的确认弹出框，点击 **OK**。

解锁用户帐户

如果由于超出了登录尝试允许的次数，用户被锁定，且已启用 *Force manual unlock* 选项(见第 161 页的*锁定策略*)，要解锁用户，请按如下操作：

1. 在列表面板选择 **Users**。

   被锁定的用户帐户在 Status 栏显示 **Locked**。

2. 在交互显示面板，点击勾选您要解锁的用户。

3. 做完选择后，点击面板右方的 **Unlock**。
4. 出现的确认弹出框，点击 **OK**。

注意：1. 通过按您所需勾选多位用户，您可以解锁多位用户。通过勾选栏目顶部的框，您可以解锁所有锁定的帐户。

2. 如果用户－包括系统管理员－被锁定，系统管理员可用CC2000工具恢复其帐户，然后解锁被锁定的用户。见第187页的*恢复*。

群组

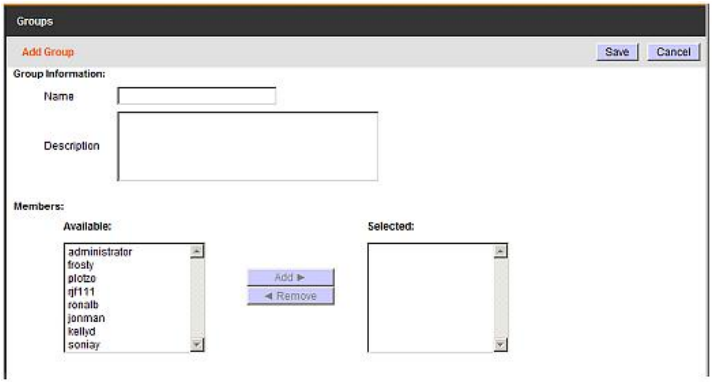
群组允许管理员轻松高效地管理用户和设备。因为设备访问权应用于群组的所有成员，所以管理员只需对群组进行一次设置即可为所有成员进行设置，而不用为各用户进行单独设置。可定义多个群组，以允许某些用户访问特定设备，而限制其它用户访问这些设备。

创建群组

要添加群组，请按如下操作：

1. 在用户管理菜单栏，选择 **Groups**。*Group List* 页出现：

2. 点击主面板右上方的 **Add**。*GroupInformation* 页出现：



3. 为群组键入一个名称和描述(可选项)。

注意：1. 群组名可以是2-32个英文数字字母字符，但不能包含如下符合：/ \ [ ] : ; | = , + * ? < > @ " '。
2. 描述可以多达256字节。

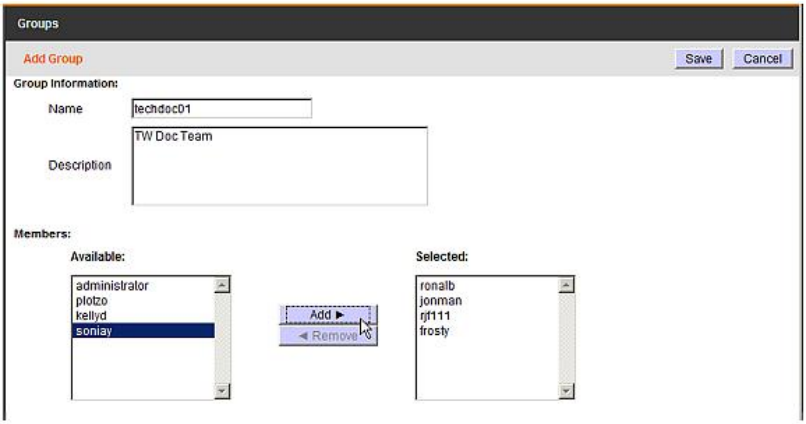
4. 点击 **Save** 以创建群组。群组现在出现在侧栏树形图和交互显示面板中的群组信息列表。

注意：您可以在执行此步之前添加用户到群组。关于添加用户到群组的详细说下，见下面的部分。

添加用户到群组

添加用户到群组，请按如下操作：

1. 在用户管理菜单栏，选择 **Groups**。
2. 或是在侧栏树形图或是在交互显示面板，点击群组名。*Group Information* 页出现：



3. 从 *Available* 列表选择您要添加到群组的用户，然后点击 **Add** 以移动用户从 *Available* 列表到 *Selected* 列表。
4. 为您要添加到群组的其他用户重复步骤 3.

注意：添加多位用户的快捷方法是，在Available栏，用Ctrl+Click或Shift+Click选择您需要的用户，然后点击Add，以一次移动所有被选择的用户。

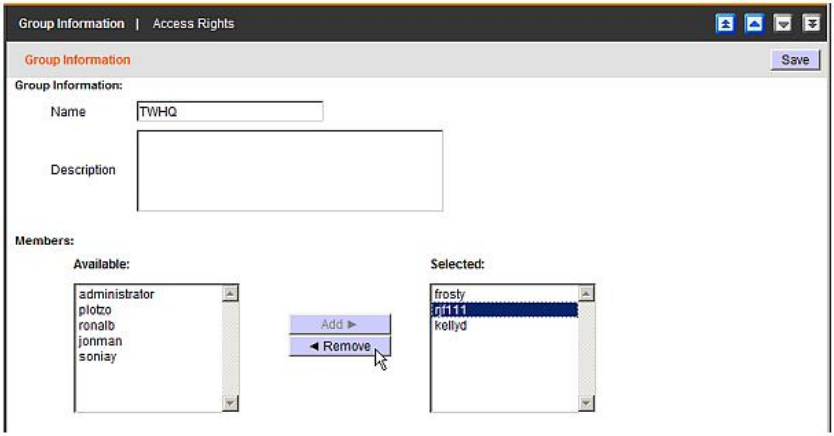
5. 当完成添加用户后，点击 **Save** 以完操作。

注意：如果用户除了有分配给群组的权限之外，还要其它权限，用户则保留分配给群组的权限以及这些权限。

从群组移除用户

从群组移除用户，请按如下操作：

1. 在用户管理菜单栏，选择 **Groups**。
2. 或是在侧栏树形图或是在交互显示面板，点击群组名。*Group Information* 页出现：



3. 从 *Selected* 列表选择您要从群组移除的用户，然后点击 **Remove**，以将用户从 *Selected* 列表移到 *Available* 列表。
4. 为您要从群组移除的其他用户重复步骤 3.

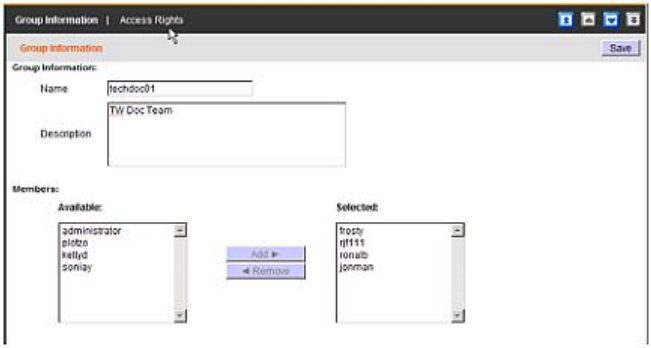
> **注意：**移除多位用户的快捷方法是，在Selected栏，用Ctrl+Click或Shift+Click选择您需要的用户，然后点击Remove，以一次移动所有被选择的用户。

5. 当完成移除用户后，点击 **Save** 以完操作。

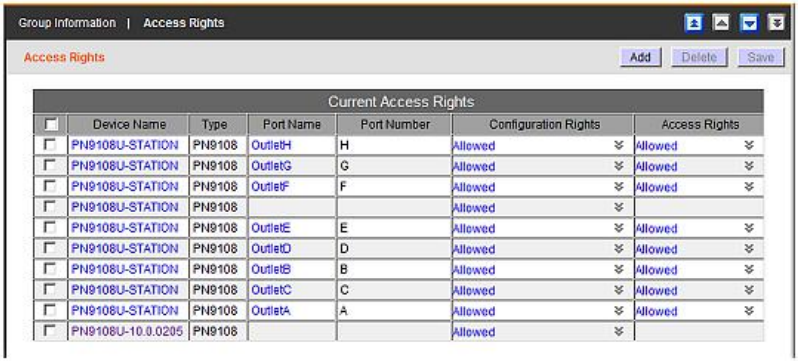
访问权

为群组设定访问权，请按如下操作：

1. 在用户管理菜单栏选择 **Groups**。*Group List* 页出现。
2. 选择您要为其设定访问权的群组。
3. 在出现的 *Group Information* 页，在子菜单栏选择 **Access Rights**：



出现的页面列出已分配到群组的所有设备和端口。



Device Name	Type	Port Name	Port Number	Configuration Rights	Access Rights
PN9108U-STATION	PN9108	OutletH	H	Allowed	Allowed
PN9108U-STATION	PN9108	OutletG	G	Allowed	Allowed
PN9108U-STATION	PN9108	OutletF	F	Allowed	Allowed
PN9108U-STATION	PN9108			Allowed	
PN9108U-STATION	PN9108	OutletE	E	Allowed	Allowed
PN9108U-STATION	PN9108	OutletD	D	Allowed	Allowed
PN9108U-STATION	PN9108	OutletB	B	Allowed	Allowed
PN9108U-STATION	PN9108	OutletC	C	Allowed	Allowed
PN9108U-STATION	PN9108	OutletA	A	Allowed	Allowed
PN9108U-10.0.0205	PN9108			Allowed	

在此页，您可以：

- 点击 *Device Name* 或 *Port Name* 列表中的设备或端口，以到其设备管理*属性*页。
- 对于任何设备或端口，点击 *Configuration Rights* 栏中的箭头，设置群组对设备或端口的设定权。**Allowed** 表示群组成员可以设定设备或端口的设置；**Denied** 表示群组成员不可以设定设备或端口的设置。

- 对于任何设备或端口，点击 *Access Rights* 栏中的箭头，设置群组对设备或端口的访问权。如在第 123 页表格中所描述的，访问权根据所选的设备类型而变化。
- 分配额外的设备到群组，点击主面板右上方的 **Add**。在出现的页面，点击勾选您要添加的设备前面的复选框，然后点击 **Save**。

注意：通过勾选几个复选框，可选择不只一台设备。勾选栏顶部的框，则选择所有设备。

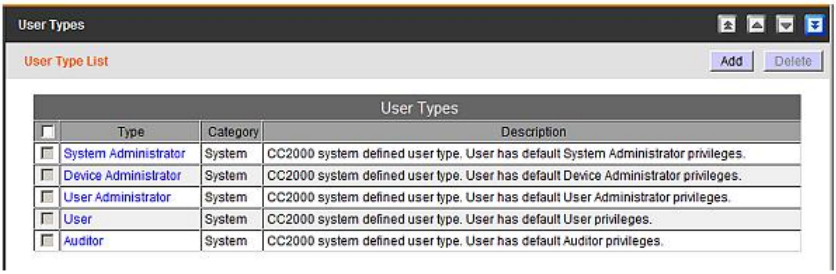
- 移除设备，点击勾选您要移除的设备，然后点击 **Delete**。
- 当作为修改后，点击 **Save**。

类型

有两个主要用户类型：System (系统)和 Custom (自定义)。默认 CC2000 支持五种用户类型。这些类型称作*系统*用户类型，因为它们内置于系统。分配给这些用户类型成员的角色是固定的，不能修改。

相反，*自定义*用户类型使您方便灵活地分配最适应您设备需求的各种角色组合。

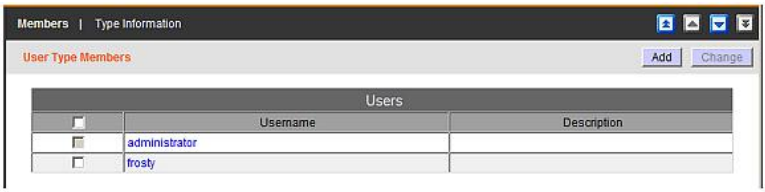
当点击菜单栏上的 **Types** 时，*User Type List* 出现在交互显示面板，显示已设定的所有用户类型：



用户类型

成员

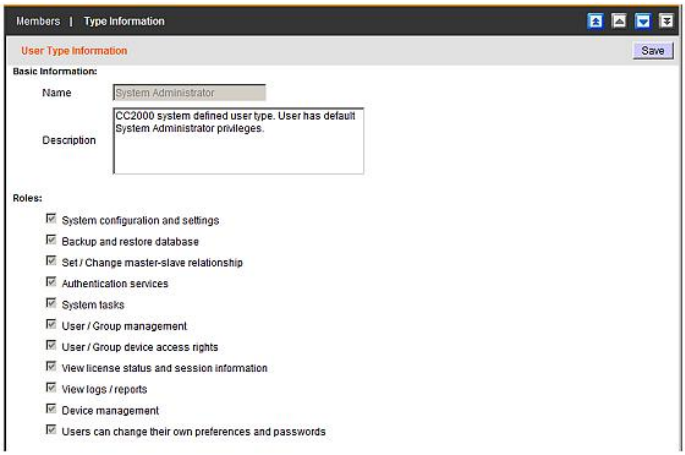
在侧栏或交互显示面板，点击某用户类型，打开 *Members* 子菜单页，其显示所有属于此类型的用户。



- 点击用户名，则带您到用户的 *Account Information* 页。
- 添加用户到某类型，点击主面板右上方的 **Add**。在出现的页面中，选择您要添加的用户，然后点击 **OK**。
- 修改用户的类型，勾选用户名前面的框，然后点击主面板右上方的 **Change**。在出现的页面中，为用户选择新类型，然后点击 **OK**。

类型信息

当在 *Members* 子菜单页时，您可以点击 **Type Information** 以查看此用户类型的描述，以及分配给它的角色：



注意：仅能在此页做修改的是*Description*区，此处提供关于用户类型的附加信息。

系统类型

系统类型成员执行的角色是固定的。与各类型相关的角色概括于下表：

分配的角色	系统管理员	用户管理员	设备管理员	用户	审查员
系统设定和设置	√				◇
备份和恢复数据库	√				◇
设置/修改主-从关系	√				◇
验证服务	√				◇
系统任务	√				◇
用户/群组管理	√	√			◇
用户/群组设备访问权	√	√			◇
浏览许可证状态和会话信息	√	√			◇
浏览日志/报告	√	√	√		◇
设备管理	√	√	√		◇
用户可修改自己的偏好和密码	√	√	√	√	√

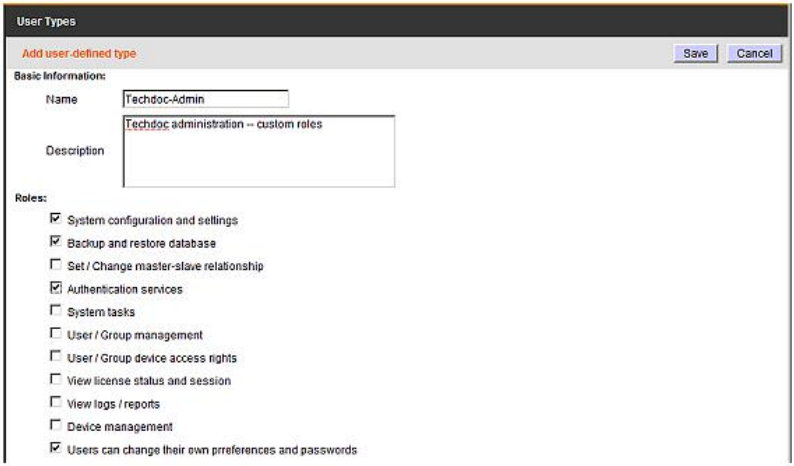
注意：关于*Auditor*(审查员)类型：

1. 审查员类型可以访问所有选项卡和页面，但仅限于*View Only*权限。
2. 在**Log**选项卡下，审查员类型除了浏览外，还可以导出并打印日志，但不能修改任何设置。
3. 在**Preferences**选项卡下，审查员类型可以修改他/她的*颜色方案*、*网络选项*和*密码*设置。

自定义类型

CC2000 提供创建自定义用户类型的功能，任意组合分配给用户类型的角色，这比预定义的系统类型更适应您的要求。要创建一个自定义用户类型，请按如下操作：

1. 从用户管理菜单栏选择 **Types**。
2. 在侧栏树形图点击 **Custom Types**。*User Type List* 出现，显示已设定的所有自定义用户类型。
3. 点击面板右上方的 **Add**。在出现的页面中，为新类型键入一个名称和描述，然后勾选你要新用户类型执行的角色。



注意：1. 名称可以是2-32个英文数字字母字符，但不能包含如下字符：" '。
2. 描述可以多达256字节。

4. 当做完修改后，点击 **Save**。

验证服务

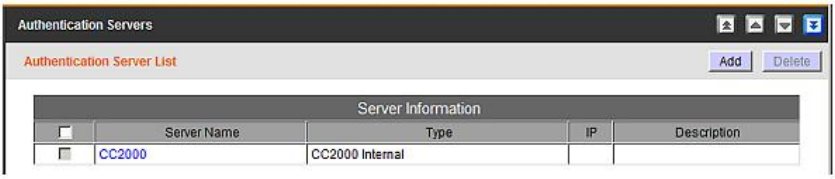
CC2000 提供一个内部*用户名/密码*验证服务。另外，CC2000 支持如下第三方外部验证服务：LDAP、LDAPS、Active Directory、RADIUS、TACACS+和 Windows NT Domain。

注意：1. 验证是指测定登录者的真实性；授权是指分配使用设备各种功能的权限.
2. 这些外部服务器仅提供验证服务－它们不提供授权服务。CC2000管理系统提供授权。

通过添加外部验证服务器到 CC2000 管理系统(详情请见第 76 页)，当添加一个用户帐户时，您可以从验证服务器列表选择外部验证服务器(见第 56 页的*添加用户帐户*)。

注意：对于LDAP、LDAPS和Active Directory，有一种额外的验证方式，在此方式下，尝试登录的用户在CC2000上没有帐户。在这种情况下，CC2000检查外部服务器，以查看是否其包含尝试登录用户的用户名和密码帐户。如果有，CC2000检查是否用户属于一个通过CC2000验证的群组。如果是，CC2000让用户登录，并分配其群组访问权。详情请见第82页的*群组授权*。

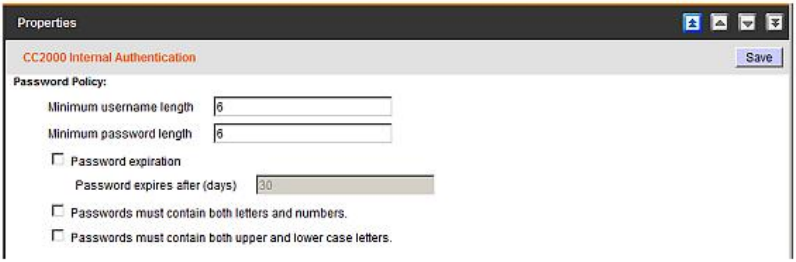
当点击菜单栏上的 **Authentication Services** 时，*Authentication Server List* 出现于交互显示面板，显示已设定的所有验证服务器：



CC2000 验证

关于 CC2000 的内部验证服务，您可以对密码策略功能做一些设定设置。所有用户帐户必须遵循您在此设置的要求。要设定 CC2000 的密码策略，请按如下操作：

1. 从用户管理菜单栏选择 **Authentication Services**。
2. 或是在侧栏列表，或是在交互显示面板中的验证服务器列表，点击 CC2000. *属性*页出现。



3. 选择您要的设定选项。(对于各区的说明，请参考下表。)

区域	说明
Minimum username length	用户名长度可以是 1-16 个英文数字字母字符。默认为 6 个字符。
Minimum password length	密码长度可以是 0-16 个英文数字字母字符。默认为 6 个字符。设置为 0 意味着不要求密码验证。由于这使您的设备处于高度不安全的状态，我们强烈建议不要设置为 0。
Password expiration	为了安全的目的，您可以强制用户以特定时间间隔更新其密码。要这样做，启用 *Password expiration*，然后指定天数，密码在此天数后过期。一旦密码过期，必须设置新密码。密码从帐户创建或新密码被设置的时间开始过期。
Passwords must contain both letters and numbers	为了安全的目的，启用此设置以强制用户在密码中包括字母和数字。
Passwords must contain both upper and lower case letters	为了安全的目的，启用此设置以强制用户在密码中包括大写和小写字母。

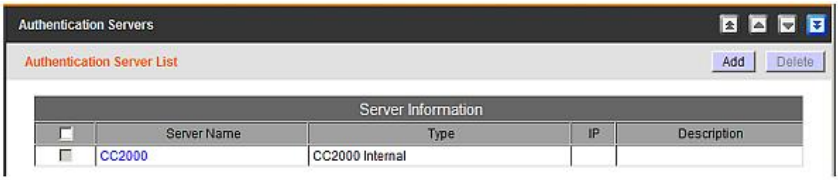
4. 完成设置后，点击 **Save**。

外部验证服务器

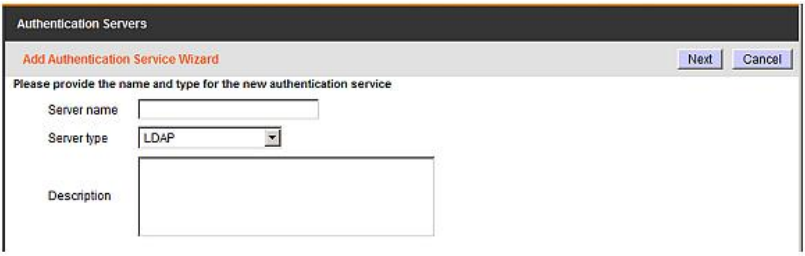
添加外部验证服务器

为了使用第三方外部验证服务器，必须先将其添加到验证服务器列表。要这样做：

1. 从用户管理菜单栏选择 **Authentication Services**，以打开验证服务器列表：



2. 点击主面板右上方的 **Add**。在出现的 *Add AuthenticationService* 页面，下拉 Server type 列表，以选择您要添加的服务器；为其指定一个名称和描述，然后点击面板右上方的 **Next**。



3. 接下来出现的页面取决于您选择的服务。跟随 Wizard 的页面，键入所选外部验证服务器要求的信息。完成设置后，点击 **Save**。

注意：1. 名称可以是2-32个英文数字字母字符，但不能包含如下字符：" '。
2. 描述可以多达256字节。

服务信息

各项服务要求的信息如下表所描述。

1. LDAP/LDAPS

标题	信息
Connection Settings (连接设置)	从LDAP管理员获得这些区的信息。端口默认为636，但请与 LDAP/LDAPS 管理员核对，查看其是否是别的值。 设置示例，见第 283 页的 *LDAP/LDAPS – OpenLDAP 设置示例*。
SSL Mode (SSL 模式)	◆ 点击 *Do not use SSL* 单选按钮，使用 LDAP。 ◆ 点击 *Use SSL in Trust All mode* 单选按钮，使用 LDAPS。
LDAP User Schema (LDAP 用户架构)	从 LDAP 管理员获得这些区的信息。 设置示例，见第 195 页的 *LDAP/LDAPS – OpenLDAP 设置示例*。
Browsing Method (浏览方式)	当添加或修改用户帐户时(见第 56 页的*添加用户帐户*)，您可以点击 **Browse** 按钮浏览 *User RDN* 中的所有用户，以选择登录名。 ◆ 选择 *Browse with user credentials*，允许用户用服务器上设定的证书浏览 LDAP/LDAPS。如果选择了此项，用户每次浏览时不必输入其证书。 ◆ 选择 *User must input credentials*，使用户每次浏览时输入其证书。

2. Active Directory

标题	信息
Connection Settings (连接设置)	从 Active Directory 管理员获得这些区的信息。 设置示例，见第 285 页的 *Active Directory 设置示例*。
SSL Mode (SSL 模式)	点击一个单选按钮，选择是否在 Trust All 模式中使用 SSL。
Browsing Method (浏览方式)	键入 User RDN 的信息。RDN 的 Active Directory 默认设置是 **cn=users**，但是请与 Active Directory 管理员核查，查看其是否是别的值。
	当添加或修改用户帐户时(见第 117 页的*添加用户帐户*)，您可以点击 **Browse** 按钮浏览 *User RDN* 中的所有用户，以选择登录名。 ◆ 选择 *Browse with user credentials*，允许用户用服务器上设定的证书浏览 Active Directory。如果选择了此项，用户每次浏览时不必输入其证书。 ◆ 选择 *User must input credentials*，使用户每次浏览 Active Directory 时输入其证书。

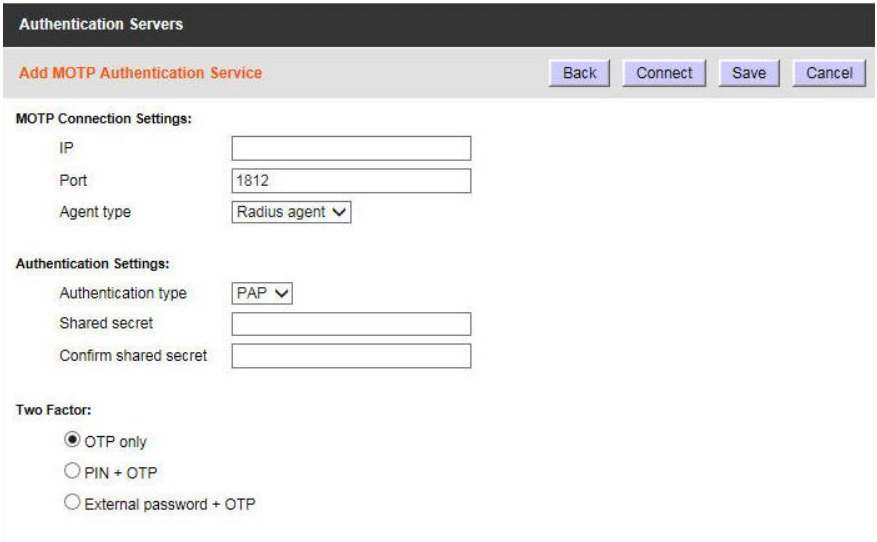
3. RADIUS 和 TACACS+

标题	信息
Connection Settings (连接设置)	从服务管理员获得这些区的信息。RADIUS 默认值为 1812；TACACS+默认值为 49，但请与服务管理员核对，查看其是否是别的值。设置示例，见第 286 页的 *RADIUS 设置示例*和第 288 页的 *TACACS+ 设置示例*。
Authentication Settings (验证设置)	从服务管理员获得这些区的信息。设置示例，见第 286 页的 *RADIUS 设置示例*和第 288 页的 *TACACS+ 设置示例*。 1. 下拉列表以选择您的 RADIUS 服务器所设置成的*验证类型*。 2. 在 Shared Secret 区，键入您用 RADIUS 服务器验证时使用的字符串。 3. 在 Confirm Shared Secret 区，再次键入在 Shared Secret 区输入的字符串。

4. Windows NT域名

从服务管理员处获得域名名称信息。例如设置，详见第290页，*NT域名设置实例* 。

5. MOTP（动态一次性密码）*



标题	信息
MOTP Connection Settings MOTP连接设置	从服务管理员处获取IP和端口相关信息。默认MOTP端口为1812，但是请向服务管理员确认是否有变更。选择*Radius agent*（Radius代理）作为代理类型。如需获得更多MOTP设置帮助，请参阅第298页，*MOTP设置* 。
Authentication Setting 认证设置	从服务管理员处获取这些方面的最新信息。如需获得更多MOTP设置帮助，请参阅第298页，*MOTP设置* 。

标题	信息
Two Factor 双元素	此部分允许您选择用于登入CC2000的认证方式。 1. 如果您选择OTP only（仅OTP），登入CC2000时，仅适用用户名和OTP对用户进行认证。可忽略密码/识别码。 2. 如果您选择PIN+OTP，登入CC2000时，MOTP服务器将认证用户、识别码和OTP。您不需要在CC2000登入页面密码/识别码区输入CC2000密码。 3. CC2000 login page.如果您选择*External password+OTP*（外部密码+OTP），登入CC2000时，MOTP服务器将认证用户名、密码和OTP。您不需要在CC2000登入页面密码/识别码区输入识别码。

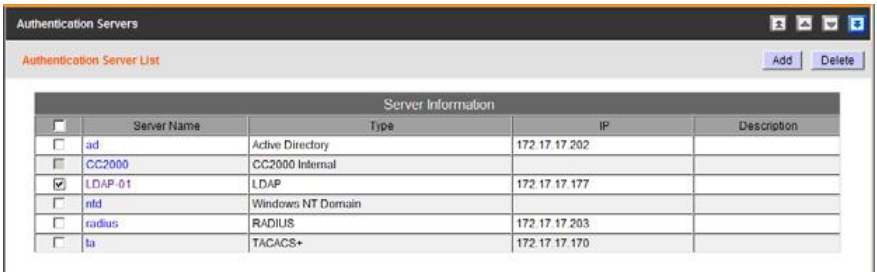
注意： 1. MOTP服务器为一次性密码（OTP）认证。若想使用OTP功能，首先需要安装MOTP服务器。

2. 如您向购买MOTP服务器，请咨询本地经销商。

删除外部认证服务器

如要删除外部认证服务器，按下述操作：

1. 从用户管理选单栏选择**Authentication Services**（认证服务），打开认证服务器列表：
2. 在交互式显示面板中，点击勾选您想要删除的外部认证服务器。



注意： 1. 您可以根据需要勾选多个名称，删除多台服务器。

2.您可以通过点击复选框删除所有可删除的服务器。

3.如果用户帐户已经在使用外部验证服务器的 CC2000 创建，服务器不能被删除。

4. 您作出选择后，点击在面板右侧的删除。

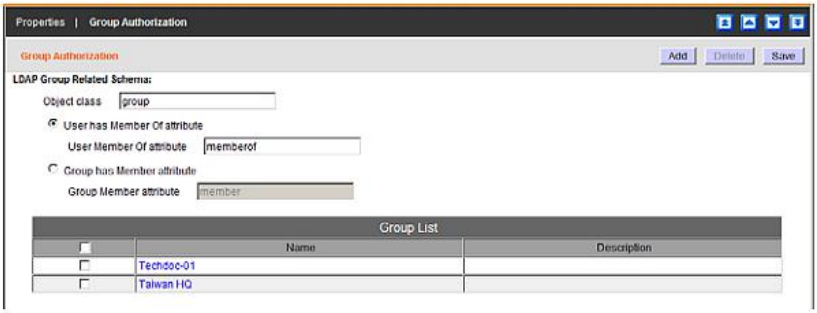
5. 出现弹窗后，点击确定。

群组授权

对于 LDAP、LDAPS 和 Active Directory，有一种额外的验证方式，在此方式下，设置特定群组的访问权。此功能用来使授权在外部验证服务器上有帐户的用户更简单。管理员分配用户到群组，用户继承群组所有的权限，从而不必一个权限一个权限地授予用户。

添加群组进行群组授权，请按如下操作：

1. 在 *User Management* → *Authentication Services* 下，从侧栏或主面板列表选择外部验证服务器。服务器的*属性*页出现。选择
2. 选择 **Group Authorization** (在子菜单栏)。*群组列表*页出现：



注意： 1. 屏幕截图显示的是选择了LDAP服务器的页面。如果选择了Active Directory，LDAP Group Related Schema设置区不出现。

2. 对于 LDAP Group Related Schema 设置，从 LDAP 管理员获得这些区的信息。设置示例，见第 291 页的 *LDAP 群组授权设置示例*。

3. OpenLDAP的默认设置是*Group has Member attribute* – 见第291页的*示例 1*。此种方式添加成员到LDAP服务器上的群组。

4. 另一设置是*User has Member Of attribute* – 见第293页的*示例 2*。用这种方式，群组被添加到在LDAP服务器上的用户帐户。

3. 添加一个授权群组，点击 **Add** (在面板右上方)。
4. 在出现的*属性*页，键入*基本信息*和*会话超时注销*信息。

注意：此页与添加用户帐户页相似，关于设置的详细说明，见第117页的*添加用户帐户*。

---

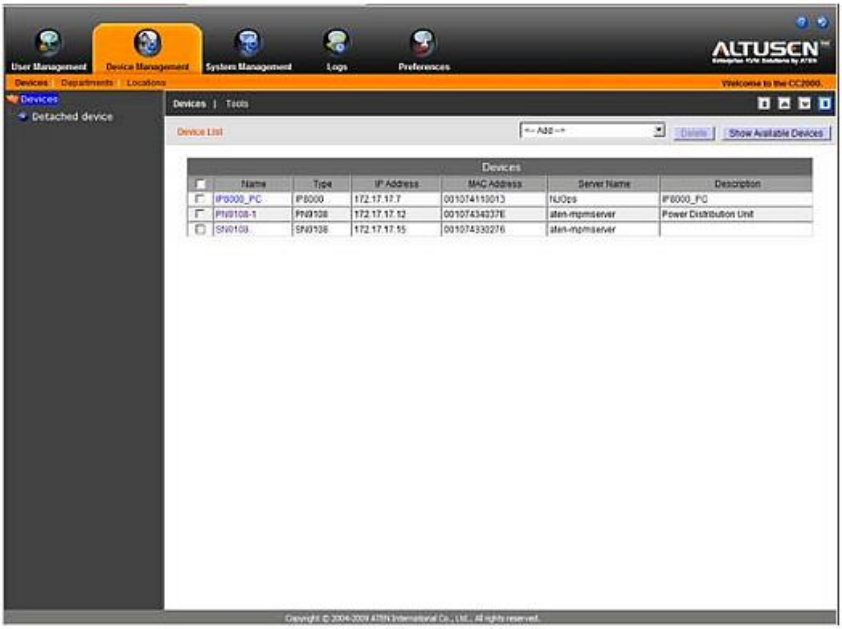
5. 在侧栏或主面板，选择您要添加的群组。
6. 在子菜单栏选择 **Access Rights**，然后点击 **Add**。一个可用设备列表出现。关于如何在此页分配访问权的信息，见第 122 页的*访问权*。
7. 做完访问权选择后，点击 **Save** (在面板右上方)。

此页刻意留白

第六章
设备管理

概述

Device Management (设备管理)页用来添加、设定和组织将通过CC2000网络管理的设备。当点击设备管理选项卡时，CC2000打开默认*设备*页，其看起来类似如下窗口：



所有设备和设备文件夹都列于侧栏树形图中和交互显示面板的表格中。要访问任何设备项目，在其中一个位置点击它即可。

注意：设备管理页限于系统管理员和设备管理员使用。其他类型用户可跳过本章。

准备步骤

设备被管理前，必须先添加到系统。这涉及四个基本步骤：

1. 连接设备到与CC2000相同的网段。必须为主和各从做此操作。
2. 一旦设备连接到与CC2000相同的网段，必须要使管理此网段的CC2000知道这些设备。这可通过在设备的ANMS页启用*CC Management*功能(见第245页)，或用*工具*菜单上的*Initialize devices IP/Port*功能(见第123页)来实现。然后各从通知与之所连设备的主。

注意：1. 通过点击 *Show Available Devices* 按钮(在面板右上方)，从可确保与之连接的设备被成功识别。如果设备已被成功识别，设备将显示在出现的列表中。

2. 点击主的 *Show Available Devices* 按钮，列出所有可选用设备，包括所有连接其从的设备。(下拉其 **Add** 设备列表产生相同结果。)

3. 已添加到 CC2000 管理系统的设备不显示在可选用列表中。

---

1. 下一步，必须从主 CC2000设备，把已在步骤2中识别的设备添加到CC2000的管理系统(详情请见第78页)。
2. 最后，创建设备，或是作为实际的物理端口设备(通过解锁各端口)，或是组合各种端口为逻辑设备架构(ATEN/Altusen通用设备、虚拟设备、群组设备等等)。详情请见第81页的*创建设备*。

使用 VPN

在某些设备中，您可能喜欢为 CC2000 管理功能使用 VPN(虚拟专用网)环境。在这种设定中，设备被管理其网段的 CC2000 识别是不必要的。设备可直接被主设备识别。这是通过启用 CC 管理功能(在设备的 ANMS 页 – 见第 245 页)并键入您要设备被其识别的 CC2000 主之 IP 地址来实现的。更多详情请见第 246 页的 *VPNs*。

菜单架构

设备管理菜单架构如下表所述：

选项卡	主菜单	子菜单	页码
	设备	设备	88
		工具	123
设备管理		默认访问权限	125
		设备同步	126
	侧栏设备树形图	属性 (KVM)	129
		访问权 (KVM)	132
		设备设定 (KVM)	136
		端口设定 (KVM)	137
		属性 (电源)*	139
		访问权 (电源) *	140
		层级设定 (电源) *	143
		端口设定 (电源) *	145
		属性 (串口)	148
		访问权 (串口)	148
		设备设定 (串口)	150
		端口设定 (串口)	151
	部门、位置、类型		153
	支持的设备		156

* 只有当属于“Power Over the NET™”(PNXXXX)设备的插座端口被选择时，此项目才出现。

设备

Devices(设备)菜单有两个子菜单：Devices、Tools(工具)和设备同步。其默认页面是设备子菜单的主页。设备子菜单在下面的部分讨论。工具子菜单在第 123 页讨论，设备同步将在第 125 页讨论。

设备

设备子菜单用来添加、修改、删除和组织设备和设备文件夹。所有已被设定在 CC2000 服务器上使用的设备和已被添加到 CC2000 数据库的设备项目都列于侧栏。

在主设备上，可被添加和设定的设备类型在主面板顶部的 *Add* 下拉列表中找到。

注意：下拉列表仅在主设备上可用，因为设备只能从主设备添加到 CC2000 管理系统。对于从设备，点击 Show Available Devices 按钮则列出可被识别的、与之连接的设备。

设备类型及其用途的说明在下表给出：

设备类型	用途
Device (设备)	选择此类型，添加ATEN/Altusen NET™设备到CC2000管理系统。详情请见第243页的*支持CC2000的Altusen/ATEN IP产品*。 **注意**：当设备被添加时，默认其所有端口被锁定，并且一定要被解锁。详情请见第121页的*解锁端口*。这允许添加其包含的端口超过许可数量的设备，然后选择某些端口进行解锁 – 从而不超越许可证限制。
APC PDU	选择此类型可添加APC PDU到CC2000管理系统。CC2000支持简单的设备设定、WebSSO及电源管理，如以下型号：AP79xx, AP89xx, AP86xx.。详细介绍见第97页 APC PDU。

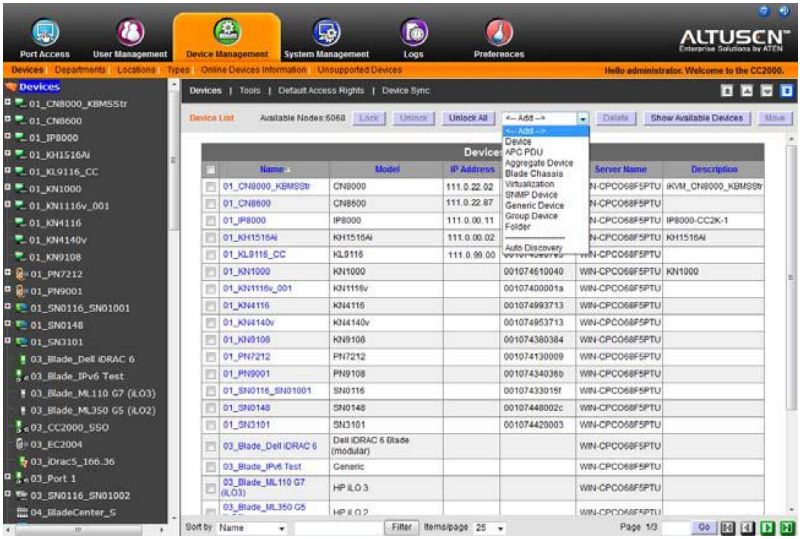
类型	目的
Aggregate Device 整合设备	选择此项创建合理的设备，包含从添加到CC2000管理系统中的ATEN/Altusen NET™设备和一些SPMs（IPMI, HPiLO2, HP iLO3, IBM RSA II, Dell DRAC 5, Dell iDRAC 6）设备中选择的端口。 此类设备用于管理多种连接方式的设备（KVM、电源、串口端口等），无需各自使用单独连接。每组整合设备都可算作一个节点，无论其包含端口数量多少，因此创建整合设备以及添加端口都可以让您管理超越实体证书限制数量的多个端口。详见第100页，*整合设备* 。 **注意：** 1. 已成为整合设备部分的端口只能用于该设备。如果不从该设备移除则无法被指派到其他设备。 2. 若某一端口已成为某一整合设备的一部分，则其不再作为独立端口，而且无法被手动锁定或解锁。如果您想把此端口作为实体端口，或者将其添加到设备组，您必须将其从整合设备中删除。
Blade Chassis 刀片机箱	选择此项添加刀片机箱。
Virtulazation 虚拟化	选择此项添加虚拟媒体/Citrix虚拟机。
NRGence PDUs	选择此类型添加PE系列能源只能PDU至CC2000管理系统。此处的“PD系列”不包括ARMbased PE系列产品。详见第243页，*能源智能机架PDU* 。 如果您要添加ARM基础的PE系列产品，见第92页，*添加设备* 。
Generic Device 通用设备	第三方通用设备（路由器、切换器等）包括任何有以太网接口的设备，并可通过HTTP/HTTPS或Telnet/SSH使用其URL或IP地址进行访问。 由于这些设备不含CC管理条款，因此不能通过CC2000认证，也不能成为CC2000单一登入配置的一部分。通用设备部占用设备节点许可。没有这些设备的代理支持（见第248页）。 选择这种类型的设备时，CC2000重新指向设备本身。您必须使用其认证步骤登录设备。 **注意：** 通用设备不占用许可的节点数。

设备类型	用途
Group Device (群组设备)	群组设备也可被创建成一个实际ATEN/Altusen NET™设备上的各端口的合成体。群组和虚拟设备的区别如下： 一旦物理端口被添加到虚拟设备，它不能被任何其它虚拟设备使用－而物理端口可被添加到数个群组设备。 **注意**：1. 群组设备不影响许可的节点数。 2. 不管它被添加到多少个群组设备，一个被添加到多个群组设备的物理端口只算作一个许可证。
Folder (文件夹)	设备文件夹提供另一种将相关设备组织成有用类别的方式(除部门和位置之外的)。(例如，将所有PN0108放入一个文件夹。)这样做，可轻松设定和维护相似类型对象。 **注意**：1. 文件夹是设备的容器，从而不影响许可的节点数。 2. 由于文件夹是进行设备管理的组织工具，所以它们不显示于端口访问侧栏或主面板列表。

添加文件夹或设备

如添加文件夹或设备，请按如下操作：

1. 点击面板右上方的 *Add*，下拉可被添加的项目的列表：



2. 点击列表中您想添加的项目。根据您的选择，一个页面出现以提供设置项目的界面。

下面的部分描述涉及设置各设备的操作。

■ **添加文件夹**

创建文件夹是一个组织方式(除了*部门*和*位置*之外的)，其允许您将企业范围内的设备组织成有用的类别。当您选择 *Folder* 作为被添加的项目时，*Add Folder* 页出现：

为文件夹填写一个名称(例如 PN9108-ALL)，及描述信息(可选项)，然后点击 **Save**。新文件夹添加到侧栏和设备列表表格中。

要将设备放入文件夹内，先在侧栏选择文件夹，然后进行下面描述的其中一个 *Add* 步骤。

注意：1. 设备可被放入文件夹唯一的方法是选择您要将设备放入的文件夹之后添加设备。

2. 文件夹可被嵌套。在侧栏选择母文件夹之后，进行添加文件夹步骤即可。

■ **添加设备**

此项目实际上是指添加ATEN/Altusen NET™设备到CC2000管理系统(详情请见第171页)。

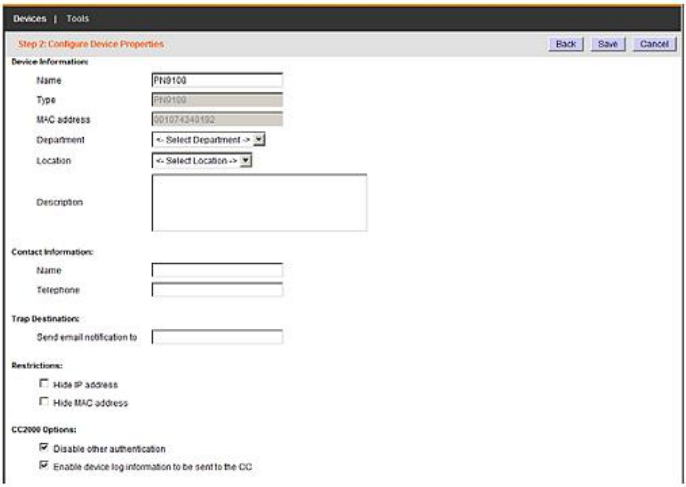
注意：1.添加ATEN/Altusen NET™设备到CC2000服务器之前，请确保设备已被识别。详情请见第86页的*准备步骤*。

2.如果您想看到添加可用设备的列表，请点击**显示可用设备**(面板右上角)。

当您选择 *设备*作为被添加的项目时，*Choose Device*页出现，列出可被添加的所有在线设备。

如要添加设备，请按如下操作：

1. 点击勾选您要添加的设备前面的复选框。
2. 点击**Next**。*Configure Device Properties*页出现：

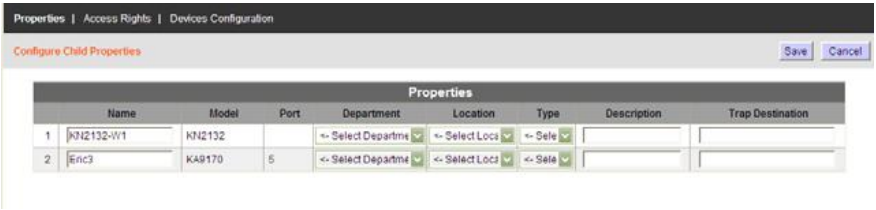


3. 根据下表中提供的信息填写各区：

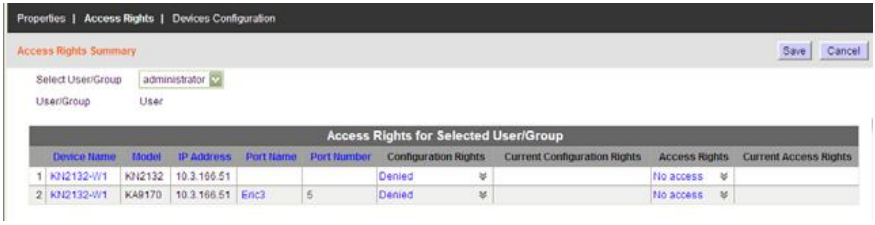
区域	信息
Basic Information (基本信息)	**Name:** 提供一个名称以识别设备。默认为在其单独设定中指定的名称。如果在此修改名称，修改只发生在 CC2000 数据库。原先设定中的名称保持不变。 **Type:** CC2000 自动识别设备类型并填写此区。 **MAC Address:** CC2000 自动填写此区。其不能编辑。 **Department:** 为了组织的目的，可以建立部门类别(例如，R&D)，并向其分配设备。如果希望分配本设备到某部门，下拉部门列表(以前创建的－见第 112 页的*部门和位置*)，并点击要设备属于的部门。 **Location:** 为了组织的目的，可以建立位置类别(例如，西海岸)，并向其分配设备。如果希望分配本设备到某位置，下拉位置列表(以前创建的－见第 153 页的*部门和位置*)，并点击要设备属于的位置。 **Description:** 如果希望提供描述设备的额外信息，在此输入。此为可选项。
Contacet Information (联络信息)	设备管理员的名称和电话号码。这些是可选项。
Trap Destination (陷阱目的地)	陷阱通知接收人的电子邮件地址。此为可选项。
Restrictions (限制)	**Hide IP Address:** 作为增加的安全措施，如果启用此功能，当用户通过浏览器登录时，它防止设备的 IP 地址出现在端口访问*状态和操作*列表。 **Hide MAC Address:** 作为增加的安全措施，如果启用此功能，当用户通过浏览器登录时，它防止设备的 MAC 地址出现在端口访问*状态和操作*列表。

字段	信息
CC2000 Options CC2000选项	**Disable other authentication**（关闭其他认证）：作为一个附加的安全措施，如果启用此功能，该设备将只接受通过CC2000登入。当设备连接到CC2000系统，用户无法登入到使用设备自己的认证系统的设备，只能通过CC2000界面管理设备。 **注意：**1. 如果该设备从CC2000系统断开连接，用户将能够使用设备自己的身份验证系统登入设备。 2. 如果复选框被选中，则意味着其他认证方式开启，用户将能够使用设备自己的身份验证系统登入设备。 **Enable device log information to be sent to the CC2000（允许将设备登入信息发送至CC2000）：**如果启用此功能， CC2000作为设备的日志服务器 – 接收并存储设备的接收事件信息，并可供检索的。 **Enable Trap notification to be sent to the CC2000（允许将陷阱通知发送至CC2000）：**如果启用此功能，CC2000将接收发生在设备上的陷阱事件的通知，并将其存储，用于检索和审计的目的。 **Enable monitor data to be sent to the CC2000（允许将监控数据发送至CC2000）**如果启用此功能，环境监测数据被发送到CC2000，记录到日志文件。在启用此功能后，下拉列表以设置传输之间的**时间间隔**。 **Device session timeout（设备会话超时）：**如果启用此功能，在此功能设置的时间内如果没有输入，会话被终止。设置范围为2-99分钟。设置为0表示禁用此功能。默认为3分钟。

4. 当您完成后，单击**Save**（保存）来完成程序。您将转到*Configure Child Properties*（配置子属性）页面，在这里您可以配置属性，如下所示：



5. 当您完成了填充字段后，单击**Save**（保存）。*Access Rights Summary*（访问权限汇总）页面出现：



6. 下拉选单来选择您想设置访问权限的用户或组。
7. 单击“访问权限”列中的箭头；勾选适当的复选框；然后单击**Save**（保存）。
8. 重复步骤6和7，用于任何额外的用户和/或组。
9. 点击**Save**（保存）完成程序。

注意：1. 添加一台设备后，它的端口被锁定。详见第121页，*锁定/解锁设备*

2. 对于CAT5 KVM切换器，只有那些有电脑端模块连接并且联机的端口可被识别并添加到设备列表。这是因为每一个模块都有自己的独立的身份，如果它是没有连接，是没有办法被识别的。一旦端口被添加，它便会出现在列表中，即使脱机。

■ 添加APC DPU

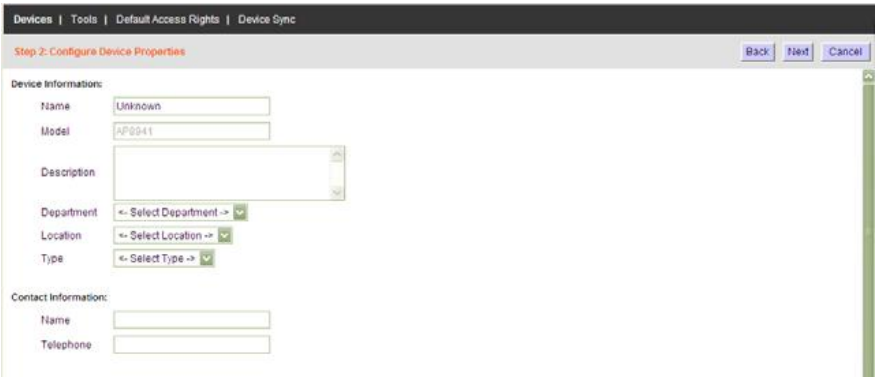
当您选择*APC PDU* 作为添加项目后，*Add APC PDU*（添加APC PDU）页面将出现：

如要添加APC PDU，按下述操作：

1. 根据下表提供的信息填充字段：

字段	信息
Auto Detect 自动侦测	如果您正在添加一个特别提到的类型，并启用自动检测，CC2000将检查设备是否联机。 只有具有管理员权限的用户才能启用此功能。
Detect Interval 侦测间隔	输入秒值，设置侦测间隔。此为系统自动检查APC PDU联机状态的间隔时间。
IP	输入APC PDU的IP地址，点击**Test Connection**（测试连接）以确认IP已被正确检测。
Connect Method 连接方式	从下拉选单选择SSH或Telnet。
Port 端口	输入曾经连接的访问端口（通过浏览器）。默认的SSH端口是22；Telnet是23。
Username/Password 用户名/密码	输入访问APC PDU需要的用户名和密码（仅限通过Telnet）。
Timeout 超时	取消连接前需要等待的完成时间。

2. 当您完成此页时，请单击**Next**（下一步）。Configure Device Properties（配置设备属性）页面出现：

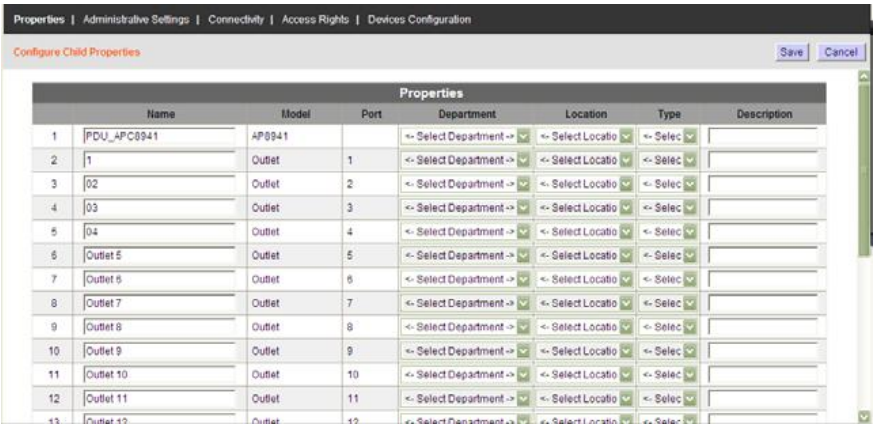


3. 根据表中提供的信息填写字段：

字段	信息
Device Information 设备信息	**Name**（名称）：提供鉴定设备的名称。 **Description**（描述）：如果您希望提供额外的信息来描述设备，在这里输入。此字段是可选的。 **Department**（门类）：出于组织性目的，您可以创建门类类别（例如R&D），并为其指派设备（详见第153页，*门类 位置和类别*）。如果您希望将此设备指派到某一门类，下拉门类列表（您之前创建的），并点击您希望设备所属的门类。 **Location**（位置）：出于组织性目的，您可以创建位置类别（例如西海岸），并为其指派设备（详见第153页，*门类 位置和类别*）。如果您希望将此设备指派到某一位置，下拉位置列表（您之前创建的），并点击您希望设备所属的位置。 **Type**（类型）：下拉列表选择设备类型。
Contact Information 联系信息	设备管理员的姓名和电话号码。这些字段为选填。

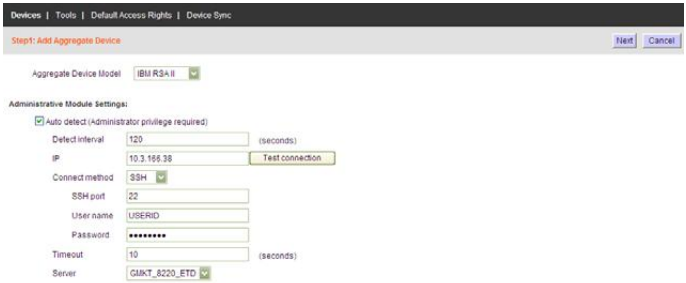
4. 单击**Next**（下一步）前往*Configure Network Connectivity*（配置网络连接）页面，在这里您可以启用Web/SSH/Telnet会话

5. 当您完成后，单击**Save**（保存）来完成程序。您将转到*Configure Child Properties*（配置子属性）页面，在这里您可以配置属性，如下图所示：



■ 添加整合设备

当您选择要添加的整合设备时，*Add Aggregate Device (*添加整合设备）页面会出现：



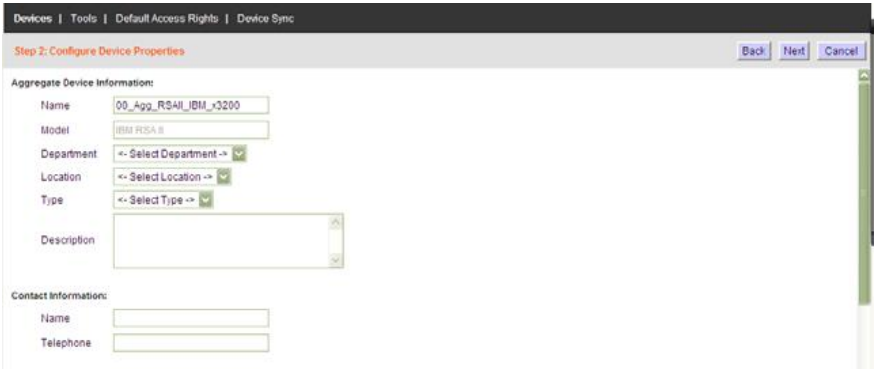
注意：详见第89页，*整合设备* 。

如要添加整合设备，按下述操作：

1. 从下拉选单中选择整合设备型号。然后，根据表中所提供的信息填写字段：

字段	信息
Auto Detect 自动侦测	如果您正在添加一个特别提到的类型，并启用自动检测，CC2000将检查设备是否联机。 只有具有管理员权限的用户才能启用此功能。
Detect Interval 侦测间隔	输入秒值，设置侦测间隔。此为系统自动检查APC PDU联机状态的间隔时间。
IP	输入APC PDU的IP地址，点击**Test Conncction**（测试连接）以确认IP已被正确检测。
Connect Method 连接方式	从下拉选单选择SSH或Telnet。
Port 端口	输入曾经连接的访问端口（通过浏览器）。默认的SSH端口是22；Telnet是23。
Username/Password 用户名/密码	输入访问APC PDU需要的用户名和密码（仅限通过Telnet）。
Loging name field/password field 登入名称字段/密码字段	输入信息，以便让CC2000了解在特定单一登入条件下将登入名和密码信息存放何处。
Timeout 超时	取消连接前需要等待的完成时间。
Server 服务器	选择整合设备服务器连接的CC2000设备。

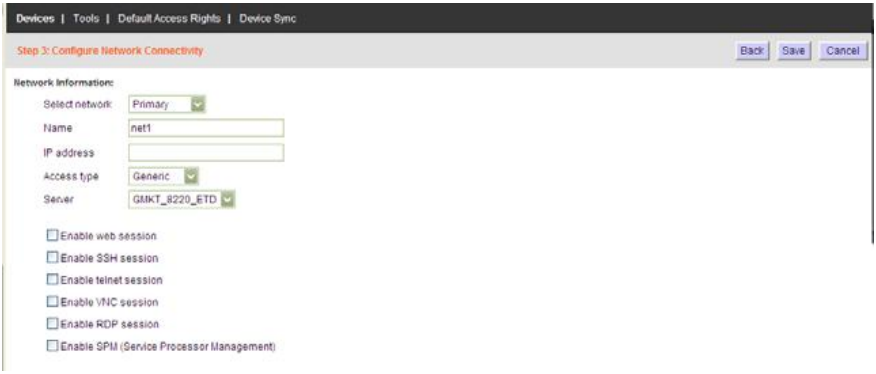
2. 在Configure *Device Properties* （配置设备属性）页中，提供一个名称，以鉴别名称字段中的整合设备。



3. （可选）在*Dscription*（描述）字段中提供对整合设备的进一步描述。
4. （可选）下拉门类、位置和/或类型列表并点击您希望整合设备所属的项目。
5. （可选）在*Contact Information*（联系信息）字段提供设备管理员的姓名和电话。
6. （可选）按照下述设置电源控制选项：
   - 勾选方框确认电源操作
   - 点击方框开启电源操作延时，在延时开机/延时关机字段输入秒数。

注意：若SPM不支持此功能，选项无效。

7. 完成此页面后，点击**Next**（下一步）。*Configure Network Connectivity*（配置网络连接）页面出现：



8. 根据下表提供的信息填充字段：

字段	信息
Network Information 网络信息	**Select network**（选择网络）：如果整合设备的服务器只有一个网络接口，选择**主设备**，然后移动到配置其余字段。如果它有一个以上的网络接口，完成配置的主要一个后，返回选择额外的，并分别配置。 **Name**（名称）：为了方便，每个网络接口都可命名。 **IP Address**（IP地址）：此处输入整合设备的IP地址。 **Access Type**（访问类型）：下拉列表选择访问类型。选项为Generic, Dell DRAC 5, Dell iDRAC 6, HP iLO2, HP iLO3, 以及IBM RSA II。只有*Generic* 选项支持VNC和RDP连接。 **Server**（服务器）：选择整合设备服务器连接的CC2000设备。
Web Session 网页会话	**URL**: 如要通过网页访问整合设备服务器，输入可以打开管理页面的URL。 **Enable SSO**（开启SSO）：勾选此框开启此功能，选择要使用的证书。 ◆ 选择*Use login user credentials* （使用登入用户证书）以使用和CC2000用户账户相同的用户名和密码。 ◆ 选择*Use following credentials*（使用之后的证书），在下面的字段中输入新的认证。 **Login name, Password**（登入名称、密码）：根据整合设备服务器的认证和认证步骤填充这些字段。 **注意：**由于浏览器、JRE和SPM固件经常更新，可能会出现兼容问题，影响CC2000的SPM和SSO的使用。
Loging name field/password field 登入名称字段/密码字段	输入信息，以便让CC2000了解在特定单一登入条件下将登入名和密码信息存放何处。
SSH/Telnet Session SSH/Telnet会话	**IP address, Login name, Password, SSH / Telnet port (IP 地址、登入名、密码、SSH/Telnet端口):**如要通过SSH/Telnet会话访问服务器，根据整合设备服务器的认证和认证步骤在这些字段中输入正确的信息。 **注意：**SSH会话也需要输入登入字符串信息
VNC Session VNC会话	**Port**（端口）：输入VNC会话的端口编号 **Enable SSO**（开启SSO）：勾选方框开启此功能并*仅限查看* 和*完全控制* 的密码。
RDP Session RDP会话	**RDP Port（RDP端口）：**输入VNC会话的端口编号 **Enable SSO(启动SSO)：**勾选方框开启此功能并选择使用的认证方式。 ◆ 选择*Use login user credentials* （使用登入用户证书）以使用和CC2000用户账户相同的用户名和密码。 ◆ 选择*Use following credentials*（使用之后的证书），在下面的字段中输入新的认证。

字段	说明
SPM（服务器处理器管理）	**SMP Method**（SPM方式）：从下拉选单选择。选项为IPMI, Dell DRAC 5, Dell iDRAC 6, HP iLO2, HP iLO3, and IBM RSA II. **Port**（端口）：输入SPM会话的端口编号。 **Login name, Password（登入名、密码）：根据SPM服务器的认证和认证步骤填写这些字段。** **Timeout**（超时）：设置取消请求前等待连接完成的时间。

■ 向整合设备添加端口

如要向整合设备添加端口，按下述操作：

1. 从设备列表或侧边栏选择您的整合设备。*Port List*（端口列表）页面出现。
2. 点击**Add**（添加）（界面右上角）。*Add Ports*（添加端口）页面出现，列出所有可以用于添加的端口：

Ports | Properties | Connectivity | Access Rights

Add Ports　　Save　Cancel

Available Port List

	Name	Port	Device Name	Device Type	IP Address	Server Name	Description
☐	DefaultPort	1	CN8000	CN8000			
☐		N/A	Detached device	Cascade Port			
☐		N/A	Detached device	Cascade Port			
☐		N/A	Detached device	Cascade Port			
☐	DefaultPort	1	IP8000_PC	IP8000			
☐	OutletA	A	PN0108RPSwitch	PN0108			
☐	OutletB	B	PN0108RPSwitch	PN0108			
☐	OutletC	C	PN0108RPSwitch	PN0108			
☐	OutletD	D	PN0108RPSwitch	PN0108			
☐	OutletE	E	PN0108RPSwitch	PN0108			
☐	OutletF	F	PN0108RPSwitch	PN0108			
☐	OutletG	G	PN0108RPSwitch	PN0108			
☐	OutletH	H	PN0108RPSwitch	PN0108			
☐	7175 Linux to .33	1	KN2124v	KA7175			
☐	9120 CN8 to .14	3	KN2124v	KA9120			
☐	7175 IP8 to .13.232	5	KN2124v	KA7175			
☐	DSView IP9 to .2	1	9120 CS9134	Cascade Port			
☐	9170 to .34	9	KN2124v	KA9170			
☐	OutletA	A	STATION_01	PN9108			
☐	OutletB	B	STATION_01	PN9108			

3. 您可以任意组合在整合设备页面列出的这些端口。勾选您想要添加的端口前面的选矿，然后点击**Save**（保存）。
4. 如果某一端口已经是另一整合设备或设备组的一部分，则会弹出一个对话框，提示您如要添加到此整合设备中，将从原始设备删除，并且要求您确定是否执行。点击**OK**接受变更或点击Cancel（取消）放弃。
5. 返回到*Port List*（端口列表）页面后，选中的端口将自动解锁，并且被列为与整合设备相关联。这些端口也会嵌套在侧边栏整合设备下。

■ 添加刀片机箱

若您选择*刀片机箱*作为添加项目时，*Add Blade Chasis* （添加刀片机箱）页面将会出现。

1. 根据表中所提供的信息填写字段：

字段	信息
Model 型号	下拉列表选出您想要添加的型号类型。如果不是提到的三种指定类型之一，若支持 iKVM 功能，选择 Generic with iKVM；如果不支持，选择 *Generic without iKVM* 。
Auto Detect 自动侦测	如果要添加特定的整合设备型号类型并开启自动侦测，CC2000 将会检查设备的联机状态。 只要拥有管理员权限的用户才能开启此功能。
Detect Interval 侦测间隔	输入秒数值，设定侦测间隔时间。此为系统自动侦测服务器在线状态的频率。
IP/Method/Port IP/方式/端口	若未使用自动侦测功能，输入刀片服务器的 IP 地址以及与其连接的访问端口（通过 Telnet 或 SSH）。选择连接方式。默认端口为 22（SSH）。点击 **Test Connection**（测试连接）确认 IP 和端口设置能够正确侦测到。
Username/Password 用户名/密码	输入访问刀片服务器需要的用户名和密码（通过 Telnet 或 SSH）。 **注意：**使用有管理员权限的账户以获取所需信息。
Login name field/password field 登入名称字段/密码字段	输入相关信息以让 CC2000 了解应在特定单人登入情况下，将登入名称和密码信息存放到何处。
Timeout 超时	取消请求前等待完成连接的时间。
Server 服务器	选择整合设备服务器所连接的 CC2000 设备。

2. 当您已完成此页时，请单击**Next** （下一步）。*Configure Device Properties* (配置设备属性）页面将会出现。

3. 根据表中所提供的信息填写字段：

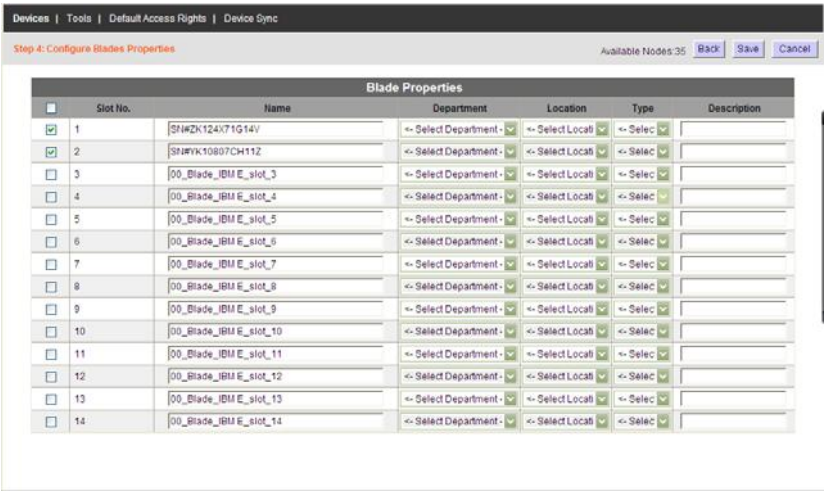
字段	信息
Device Information 设备信息	**Name**（名称）：提供可辨识设备的名称。 **Description**（描述）：如果您想提供更多信息对设备进行描述，请在此处输入。此字段为选填。 **Department**（门类）：出于组织性目的，您可以创建门类类别（例如 R&D），并为其指派设备（详见第 153 页，*门类 位置和类型* ）。如果您想要将某台设备指派到某一门类中，下拉门类列表（之前创建的），点击您希望设备所述的门类。 **Location**（位置）：出于组织性目的，您可以创建位置类别（例如西海岸），并为其指派设备（详见第 153 页，*门类 位置和类型* ）。如果您想要将某台设备指派到某一位置，下拉位置列表（之前创建的），点击您希望设备所述的门类。 **Type**（类型）：下拉列表选择设备类型。
Contact Information 联系信息	设备管理员的姓名和电话号码。这些字段选填。
Power Control Options 电源控制选项	设置如下电源控制选项： ◆ 勾选方框确认开启电源操作 ◆ 点击方框，开启延时开机操作，并在延时开机/演示关机字段处输入秒数

4. 当您已完成此页时，请单击**Next** （下一步）。*Configure Device Properties* (配置设备属性）页面将会出现。

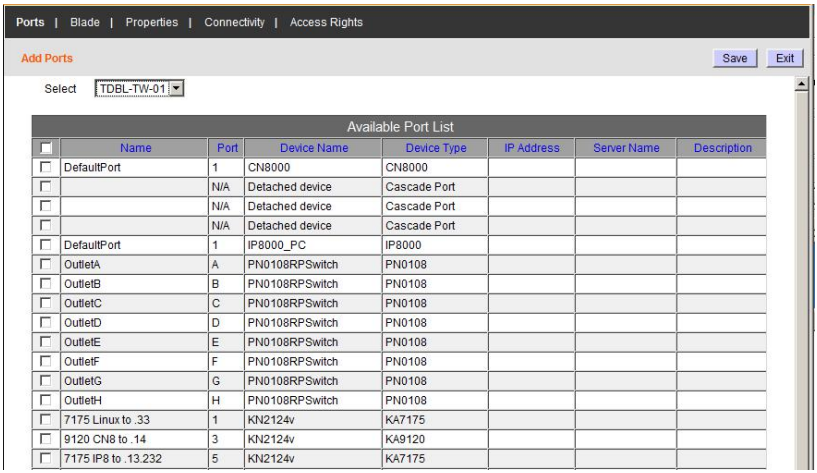
- *Maximum number of slots*（最大插槽数目）字段用于信息目的，不能配置在支持的底盘上。它只能设置在通用底盘上。
- 关于*刀片切换热键* ，信息是根据指定模型的细节自动填入的。
- 字段的其余部分与在*添加整合设备* 章节所讨论的字段相同。详情见第102页。

5. 当您已完成此页时，请单击**Next** （下一步）。*Configure Blade Properties* (配置刀片属性）页面将会出现。

6. 对于每一台刀片，可以指定它的门类、位置和类型，并提供一个简短的描述。



7. 当您已完成此页时，请单击**Save**（保存）。*Add Ports* (添加端口）页面将会出现。



8. 勾选刀片底盘连接的任何端口，然后单击**Save**（保存）。

■ **添加虚拟媒体**

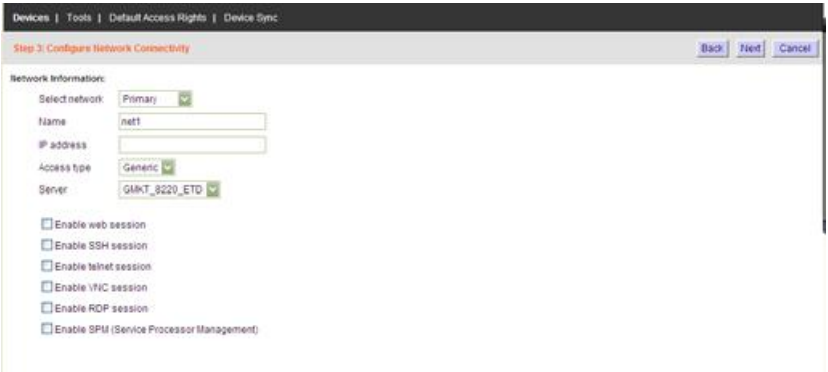
当您选择要添加的*虚拟化* (Virtualization) 项目时，*Add Virtual Server*（添加虚拟服务器）页面出现。

1. 根据表中所提供的信息填写字段：

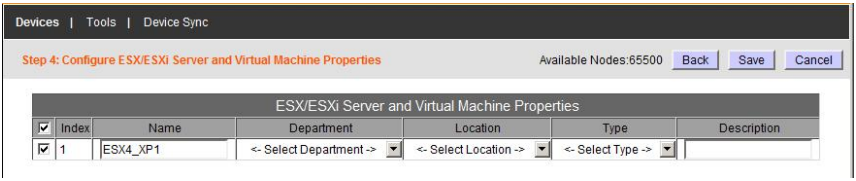
字段	信息
Virtulization Model 虚拟化型号	从下拉选单选择 VMware 或 Citrix。
Auto Detect 自动侦测	启用此功能，系统会自动检查虚拟机是否联机。只有拥有管理员权限的用户才能开启此功能。
Detect Interval 侦测间隔	输入秒数值，设定侦测间隔时间。此为系统自动侦测虚拟机在线状态的频率。
IP/Port IP/端口	输入虚拟机的 IP 地址和（通过浏览器的）连接的的访问端口。默认端口为 443。点击 **Test Connection**（测试连接）确认 IP 和端口设置能够正确侦测到。
Mapped IP 映射 IP	此功能不在“添加虚拟机工具”中，仅在“管理设置”中可用。此功能在已经安装的虚拟机在侧边栏选择后启用。见 110 页，*映射 IP 功能* 。
Username/Password 用户名/密码	输入访问虚拟机需要的用户名和密码（通过浏览器）。
Login name field/password field 登入名称字段/密码字段	输入相关信息以让 CC2000 了解应在特定单人登入情况下，将登入名称和密码信息存放到何处。
Server 服务器	选择整合设备服务器所连接的 CC2000 设备。

2. 当您已完成此页时，请单击**Next**（下一个）。*Configure Device Properties*（配置设备属性）页面将会出现。

3. 此页类似于在*添加整合设备* 章节描述的页面。根据第100页提供的信息填写字段，然后单击**Next**（下一步）。*Configure Network Connectivity* （配置网络连接）页面出现。



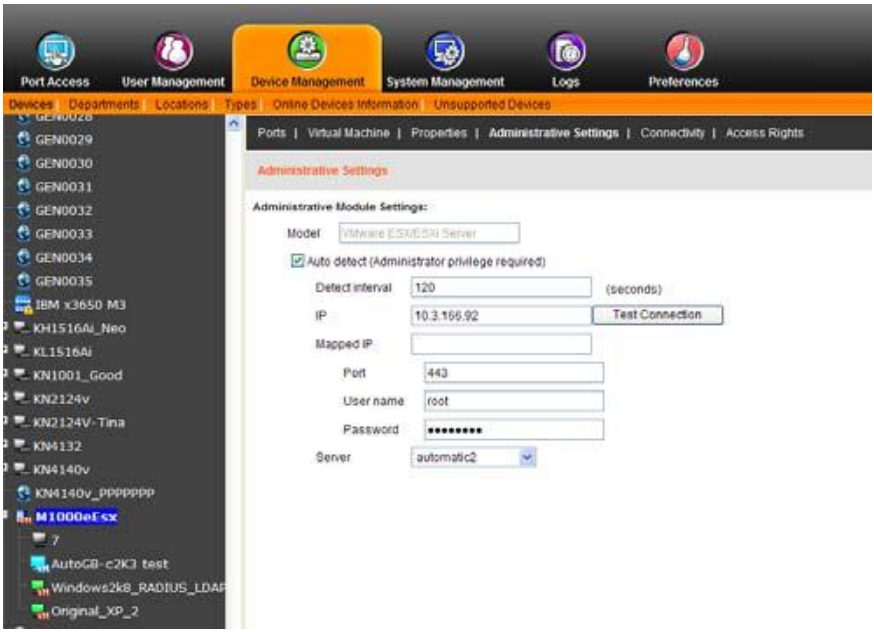
4. 此页类似于在*添加整合设备* 章节描述的页面。根据第102页提供的信息填写字段，然后单击**Next**（下一步）。*Server and Virtual Machine Properties* （服务器与虚拟机属性）页面出现。



5. 下拉门类、位置和类型并点击**Save**（保存）。

■ **映射IP功能**

一旦安装了虚拟机，映射IP功能就启用了。选择侧边栏中的VM并打开管理设置选项卡：

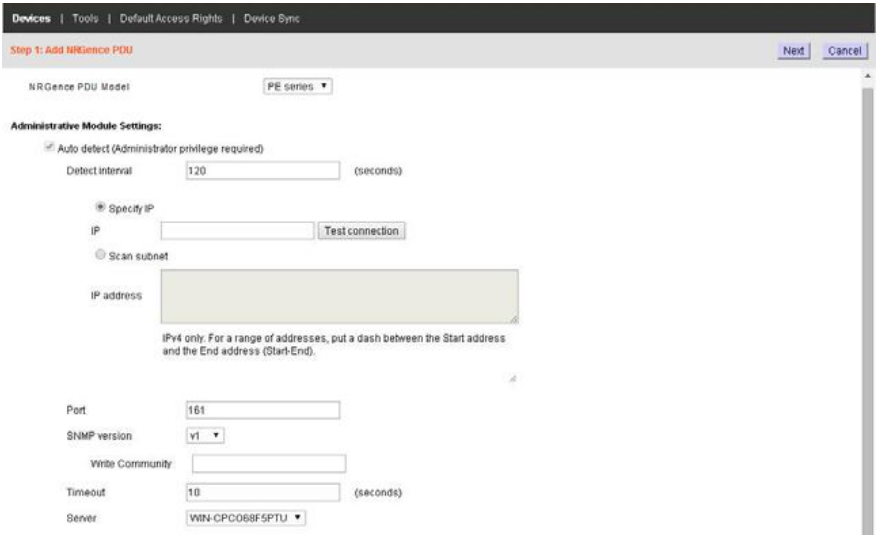


映射IP功能是VMware远程控制台支持的（通过路由器/防火墙VMRC）。

◆ 要启用该功能，在*Mapped IP*（映射IP）字段中输入路由器的外部IP地址。

■ 添加NRGence PDUs

当您选择*NRGence PDU* 为要添加的项目后，NRGence PDU的页面出现了：

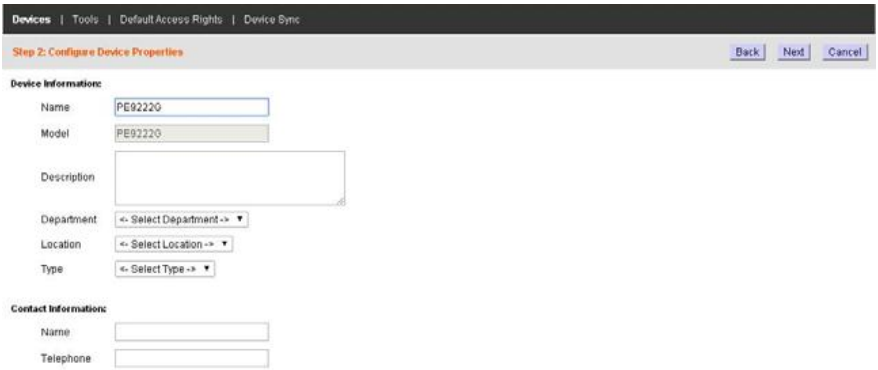


1. 根据表中所提供的信息填写字段：

字段	信息
NRGence PDU Model NRGence PDU 型号	“PE 系列”在这里指的是能源智能 PDU 不基于 ARM 的产品（详见 243 页，*能源智能机架 PDU* ）。 **注意**：如要添加 PE 系列基于 ARM 的产品，请参阅 92 页，*添加设备* 了解详情。
Auto Detect 自动侦测	启用此功能，系统会自动检查设备是否联机。只有拥有管理员权限的用户才能开启此功能。
Detect Interval 侦测间隔	输入 30-300 的秒数值，设定侦测间隔时间。此为系统自动侦测设备在线状态的频率。
Specify IP 指定 IP	输入设备 IP 地址。点击 **Test connection**（测试连接）确认 IP 地址能够检测到。
Scan subnet/IP address 扫描子网/IP 地址	输入某一范围的子网 IP 地址，帮助搜索设备。
Port 端口	输入用于访问设备的端口编号。默认端口为 161。
SNMP version SNMP 版本	选择使用的 SNMP 版本：v1、v2c 或 v3.
Write Community	如 SNMP 版本需要，请输入群体值(community value)。

字段	信息
User name 用户名	输入 SNMP 版本需要的用户名称。
Security Level 安全等级	选择使用的安全等级：“No Auth, No Priv 无验证 有权限”，“Auth, No Priv 有验证 无授权” 或“Auth, Priv 有验证 有权限”
Auth Protocol/Auth Password 验证协议/验证密码	如果选择 Auth ，然后可以选择 *Auth protocol* 认证协议。有两种选择 MD5 和 SHA。认证需要密码，不能少于 8 个字符。
Privacy protocol/Privacy password	如果 Priv 被选中，然后可以选择隐私协议。有四个选择：DES，AES-128，AES-192 和 AES-256。隐私密码是必需的，不能少于 8 个字符。
Context name 上下文名	输入设备的上下文名称。此字段可以是空白的。
Timeout 超时退出	输入服务器超时数值。范围在 10 和 120 之间。
Server 服务器	选择使用的服务器

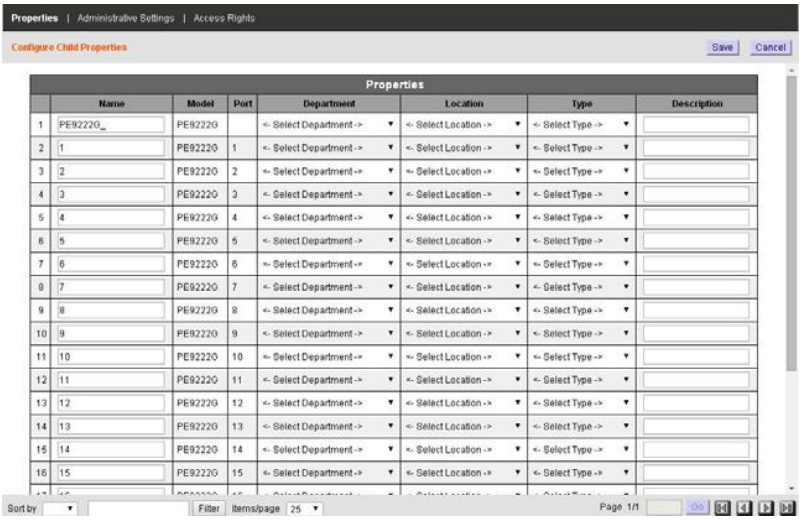
2. 当您已完成此页时，请单击**Next**（下一步）。将出现*Configure Device Properties*（配置设备属性）页面。



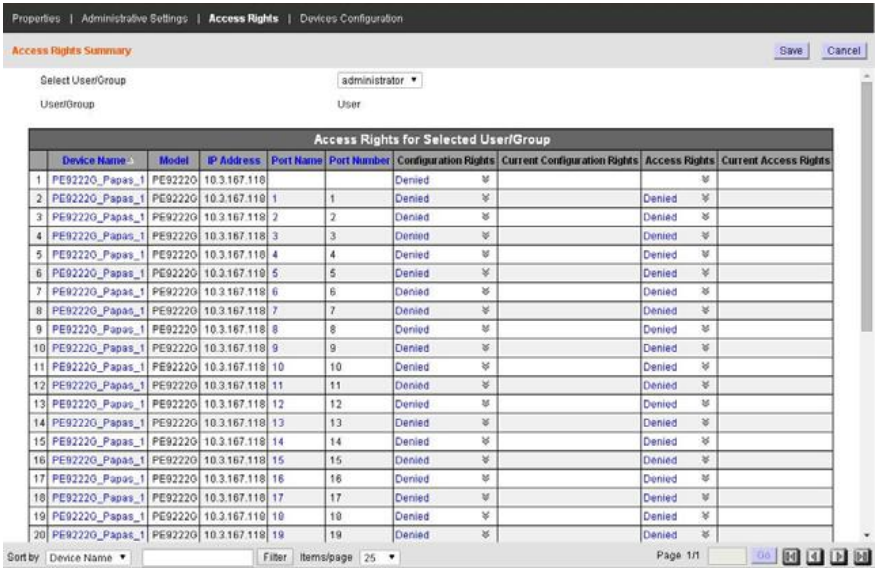
3. 根据表中所提供的信息填写字段：

字段	信息
Device Information 设备信息	**Name**（名称）：提供可辨识设备的名称。 **Description**（描述）：如果您想提供更多信息对设备进行描述，请在此处输入。此字段为选填。 **Department**（门类）：出于组织性目的，您可以创建门类类别（例如 R&D），并为其指派设备（详见第 153 页，*门类 位置和类型* ）。如果您想要将某台设备指派到某一门类中，下拉门类列表（之前创建的），点击您希望设备所述的门类。 **Location**（位置）：出于组织性目的，您可以创建位置类别（例如西海岸），并为其指派设备（详见第 153 页，*门类 位置和类型* ）。如果您想要将某台设备指派到某一位置，下拉位置列表（之前创建的），点击您希望设备所述的门类。 **Type**（类型）：下拉列表选择设备类型。
Contact Information 联系信息	设备管理员的姓名和电话号码。这些字段选填。

4. 当您已完成此页时，请单击**Next**（下一步）。*Configure Child Properties* （配置子属性）页出现，在这里您可以配置属性，如下图所示：



5. 当您完成此页时，单击**Save**（保存）。*Access Rights Summary*（访问权限汇总）页面出现：

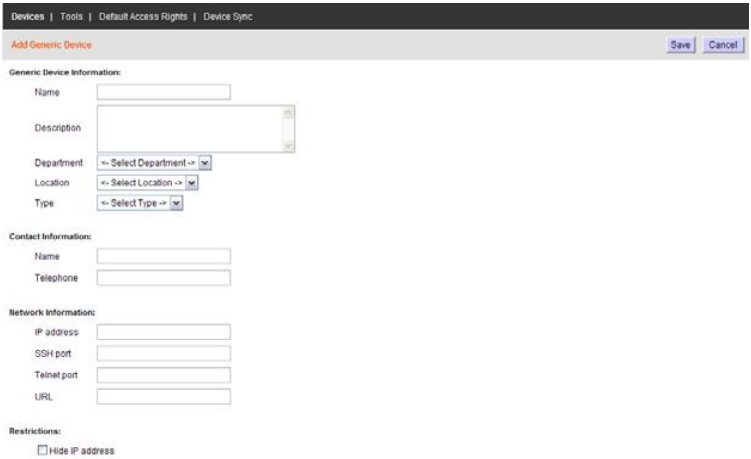


6. 使用*Select User/Group* “选择用户/组”下拉选单来选择要设置访问权限的用户或组。
7. 单击*Configuration Rights* 配置权限和*Access Rights* 访问权限列中的箭头；检查适当的复选框；然后单击**Save** “保存”。
8. 重复步骤6和7，用于任何额外的用户或组。
9. 单击**Save**“保存”完成程序。

注意：添加一个设备后，它的端口被锁定。详见121页 *锁定/解锁端口*。

■ 添加通用设备

当您选择要添加的通用设备时，*Add Generic Device*添加的通用设备页面会出现：



注意：请参阅89页，*通用设备* ，了解对通用设备的解释。

1. 根据表中所提供的信息填写字段：

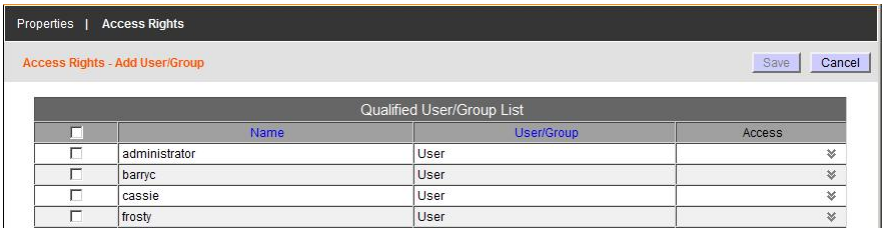
字段	信息
Device Information 设备信息	**Name**（名称）：提供可辨识设备的名称。 **Description**（描述）：如果您想提供更多信息对设备进行描述，请在此处输入。此字段为选填。 **Department**（门类）：出于组织性目的，您可以创建门类类别（例如 R&D），并为其指派设备（详见第 153 页，*门类 位置和类型* ）。如果您想要将某台设备指派到某一门类中，下拉门类列表（之前创建的），点击您希望设备所述的门类。 **Location**（位置）：出于组织性目的，您可以创建位置类别（例如西海岸），并为其指派设备（详见第 153 页，*门类 位置和类型* ）。如果您想要将某台设备指派到某一位置，下拉位置列表（之前创建的），点击您希望设备所述的门类。 **Type**（类型）：下拉列表选择设备类型。

字段	信息
Contact Information 联系信息	设备管理员的姓名和电话号码。这些字段选填。
Network Information 网络信息	根据下列信息填写字段： ◆ 如果通用设备是通过 Web 浏览器访问的，在网址字段输入它的 Web（或 IP）地址。 ◆ 如果通用设备是通过 Telnet 或 SSH 访问，在 IP 地址字段中输入 IP 地址，在对应的字段输入 Telnet 和/或 SSH 端口号。 ◆ 如果通用设备有所有可用的三种方法，您可以填写所有或任何您希望填入的。
Restrictions 限制	作为一项附加的安全措施，如果 *Hide IP Address* 隐藏 IP 地址被启用，设备的 IP 地址不会出现在端口访问 *Status and Operation* 状态和操作列表中。此设置是可选的。

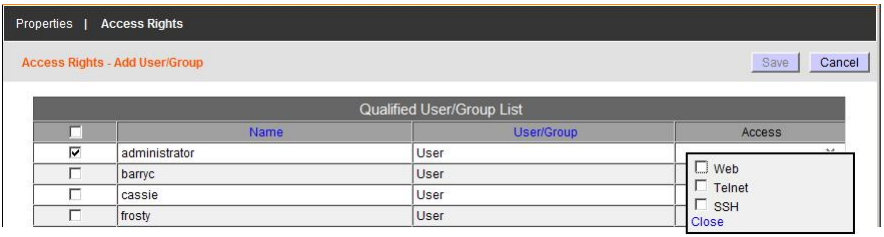
2. 如果您完成此页，请单击**Save** “保存”。您将返回到设备列表页。通用设备现在出现在侧边栏的列表中。

如要为用户和组授予访问权限，请按下述操作：

1. 在主面板或工具栏选择新添加的通用设备，然后在面板选单栏选择*Access Rights* 访问权限。用户/组列表页面出现。
2. 点击**Add** “添加”（在面板的右上方）。*Qualified User/Group List*有资格的用户/组列表页面出现，列出可以被授予该设备访问权限的用户：



3. 勾选在用户或组名前面的复选框，然后单击“访问”栏右侧的箭头以下拉访问权限选项的列表。



4. 勾选您希望用户或组有权限的项目，然后单击**Save**“保存”（在面板的右上方）。您将返回到设备列表页。通用设备现在出现在列表中及侧边栏。

   注意：访问权限面板中出现的项目取决于创建通用设备时所做的设置选项（见116页，*网络信息* ）。

■ 添加组设备

当您选择要添加的*组设备* 时，*Add Group Device*添加组设备页面会出现。添加组设备的过程基本上与添加整合设备相同。按照该节中描述的步骤（见第100页）添加组设备，并将其分配给它的端口。

注意：1. 参照第90页，*组设备*，了解整合和组设备之间差异的解释。

2. 端口可以属于任意数量的组设备。当一个端口是一个组设备的一部分时，它保留了原来的物理端口的锁定/解锁状态。如果您锁定或解锁这些端口的任何一个，所有的端口-包括原来的物理端口-将改变到新的锁定/解锁状态，

修改设备

如要修改设备设置，按下述操作：

1. 在侧边栏（如果可用）或在主选单栏（橘色条）选择**设备**。
2. 从侧边栏列表或主面板列表选择要修改设备。

3. 使用面板选单栏（黑栏）上可用的链接进行更改。参阅第129页*侧边栏设备配置*，了解关于这些面板选单的细节。

删除设备

如要删除设备，按下述操作：

所有未使用的节点也可以从侧边栏删除。要删除未使用的节点，要做以下几点：

1. 在**Device**设备选项卡中，选择侧边栏中的节点，然后单击**Delete** “删除”（在面板的右上角）。

注意：只有可拆卸的节点，如加密狗、PN站等等可以删除；插座不能删。

分离的设备

除了上面描述的设备类型之外，还有另一类设备，*分离的设备*，它表示已检测到的设备或端口与其他有效的设备或端口有某种冲突。

例如

1. 在CC2000托管的CAT5e KVM切换器上，如果有连接到端口4和6的适配器线缆，若您将适配器从端口4移除，CC2000将假设连接到端口4的设备为脱机。
2. 如果在CC2000托管的CAT5e KVM切换器上，您从端口6拔掉适配器线缆并插到端口4，电缆适配器ID将不会与端口4存储在CC2000的数据库设备信息匹配。CC2000会识别到端口4的新适配器ID，将原始的端口4适配器ID当作一台分离设备。
3. 如果您最初将适配器线缆连接到端口4*样本2*，并接入到KVM切换器的其他端口，CC2000会识别线缆适配器ID并相应地更新数据库，线缆将不被视为一个分离的设备。

分离的设备可以在树状图的底部找到。您可以查看设备试图解决冲突。问题未解决的分离设备在10天内将自动删除。

冗余电源

当一台设备有Power Over the NET™（PNxxxx）设备与它相关联时，这页的部分成为可用的*端口* 面板选单。这样二级PON插座可配置为冗余的电力设备供应－第二（荣誉）插座连接到设备的冗余电源端口。如果第一个插座的电源故障，冗余插座将继续为设备供电。

	Name	Port	Device Name	Device Type	IP Address	Server Name	Description
☐	7175 Linux to .33	1	KN2124v	KA7175			

如要配置冗余电源，按下述操作：

1. 单击**Add**（添加）（面板右上方）。
2. 在列出的可用的插座列表中，勾选您希望成为冗余电源的插座，然后单击**Save**“保存”。
3. 当您返回到该页面时，在*Enable redundant power*启用冗余电源复选框打勾，并根据表中所给的信息设置*Power on delay*延时开机和*Power off delay*延时关机参数，以下：

Power on delay 延时通电	设置电源按钮按下后连接在相应插座的电脑开机前需要等待得时间。
Power off delay 延时关机	设置电源按钮按下后连接在相应插座的电脑关机前需要等待得时间。 详见 PN 系列用户说明书的*电源管理配置* 章节。

4. 单击**Save**（保存）（界面右上方）。

锁定/解锁端口

当添加物理设备到CC2000管理系统，这些端口默认是锁定的–要想使端口可用，就必须解锁端口。当选择一个端口时，在端口属性页的右上角会出现两个按钮：*锁定*和*解锁*。要想解锁一个端口，在侧边栏或交互式显示面板，选中这个端口，点击**解锁**。

锁定和解锁端口的能力，允许您对超出了许可证的数量的安装对预先配置的设备节点进行设置。如果该安装上设备节点的总数超过了已被许可的数目，您可以通过选择该设备节点并单击"**锁定**"来排除它们。您可以在必要时通过锁定不同的端口创造空间来使用它们，然后解锁它们。

注意：当端口被添加到一个总的设备时，它们会被自动解锁，但如果您只想使用设备一个或两个物理端口，就没有必要去通过在创建一个聚合设备时所涉及到的过程去这样做。只需选择目标端口，然后单击"**解锁**"就可以了。

锁定/解锁设备

当物理设备被添加到CC2000管理系统，其端口默认是锁定的－使端口可用，就必须解锁。您可以使用下面所叙述的按钮锁定/解锁设备上的所有端口。

在设备页面的顶部您会发现**锁定**、**解锁**和**解锁全部**按钮，并在每个设备的属性页。这些按钮允许您锁定和解锁所选设备上的所有端口。当一个锁定设备从侧边栏扩展，所有的端口都会出现一个**X**。如要锁定和解锁个别端口，参阅上文的*锁定/解锁* 端口部分详情。

要锁定或解锁设备，从*设备*主页通过勾选空格；或从边栏单击设备，并点击**锁定**或**解锁**按钮。

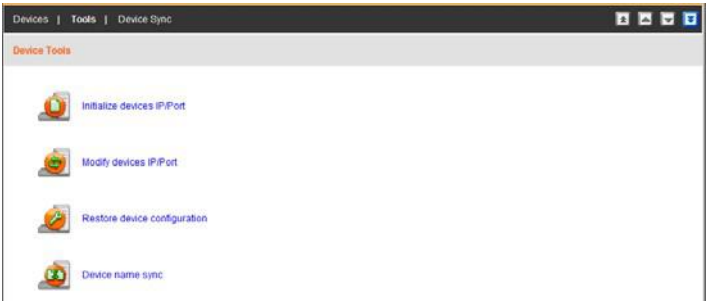
使用**解锁全部**按钮将CC2000 上从头到尾所有设备进行解锁，直到可用节点许可证都被用完。

传送设备的设置

在每个设备的属性页的顶部可以发现**传送**按钮。该按钮允许您将设备设置和访问权限从所选的设备转移到另一个设备上。单击“转换”按钮后，页面会显示所有将要转移设置的可用的设备（型号必须相同）。通过选择无线电按钮选定一个设备，然后单击“**OK**”。 会出现提醒询问您是否确认传输。CC2000将会转移所有设置（不包括设备编号、型号名称和端口号），记忆对设备的访问权限。转移不影响源设备的设置，它只适用于具有同型号名称和物理位置（端口）设备/适配器；不匹配的端口/适配器设置的访问权限将被忽略。

工具

当您单击“面板”选单栏上的“*工具*”时，会出现以下页面：



单击图标来执行一个特定的任务。每个图标执行的任务会在下一页表中描述。

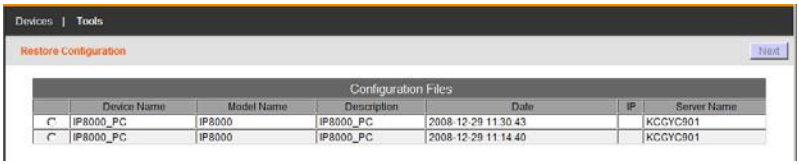
图标	任务
	**向设备广播 IP 地址和端口号**：在设备可与 CC2000 沟通前，它的 ANMS 设置必须指定 CC2000 的 IP 地址和设备管理端口号。点击这个图标，使 CC2000 向连接到网络上的设备广播其 IP 地址和设备管理端口号，自动设置他们的设备（而不是在设备本身手动设定）。这是您第一次连接设备到 CC2000 网络需要这样做，或者当一个设备被重置为默认设置。 **注意**：1.这个函数使用 UDP 来广播信息。因此，设备必须在同一网段（VPN 将不会工作）。UDP 协议使用端口 18768–确保安装 CC2000 的电脑的网络设置在这个端口开放。 2．加强安全，一旦广播播出了，信息被发送到了设备上，该设备将不接受任何其他 CC2000 UDP 广播。 3.如果您改变 CC2000s，您必须使用 ANMS 设置页用来指定 IP 地址和端口号（见 136 页，*设备配置（KVM 设备）*）。
	设备广播的 IP 地址和端口号变化：当修改 CC2000 的 IP 地址和/或设备管理端口数时使用此功能。点击这个图标，使 CC2000 向连接到网络上的设备广播其新 IP 地址和/或设备管理端口号–它们的 ANMS 设置会相应的进行自动更新。 注：1. 这个函数使用 UDP 广播信息。因此，设备必须在同一网段（VPN 将不工作）。 2.为提高安全性，接收设备将只接受从最初初始化它们的 CC2000 传来的 UDP 广播。

图标	任务
	恢复设备配置：此功能是用来恢复设备的配置和/或账户信息到一个保存在以前备份的配置文件（见第 200 页 *备份设备配置/帐户信息* ）。见下文，了解恢复程序。
	设备名称同步：如果设备名称发生了改变，这个功能是用于手动同步设备和 CC2000 之间的名字。详见第 125 页，*默认的访问权限*，了解自动同步的细节。

恢复设备配置

要恢复一个设备的配置和/或账户信息到一个保存在以前备份的配置文件，需要做以下工作：

1. 在设备管理→设备→工具面板选单，单击“**恢复设备配置**。会显示一个已保存的配置文件的列表：



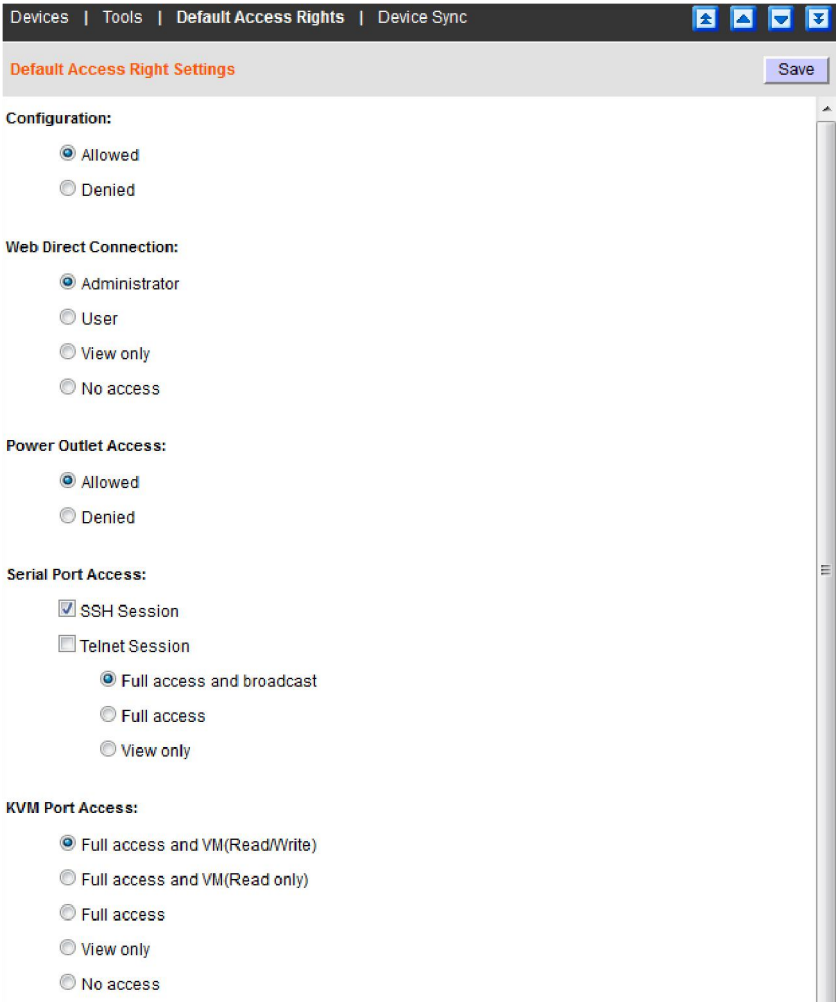
2. 选择要还原的文件，然后单击“下一步”。 出现恢复配置页面：

3. 当在密码字段中创建文件时，键入使用的密码。
4. 点击相应的复选框,仅恢复设备的账户信息；仅设备配置设置；或者两者。
5. 请在要恢复的设备名称前的复选框勾选，然后单击“**恢复**”。

   当恢复完成后，会有消息显示通知您结果。

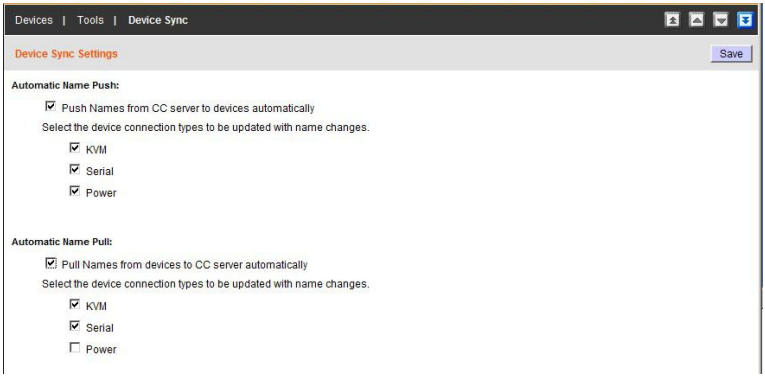
默认的访问权限

默认的访问权限 页允许设置所有添加到CC2000安装的新设备的默认访问权限。



设备同步

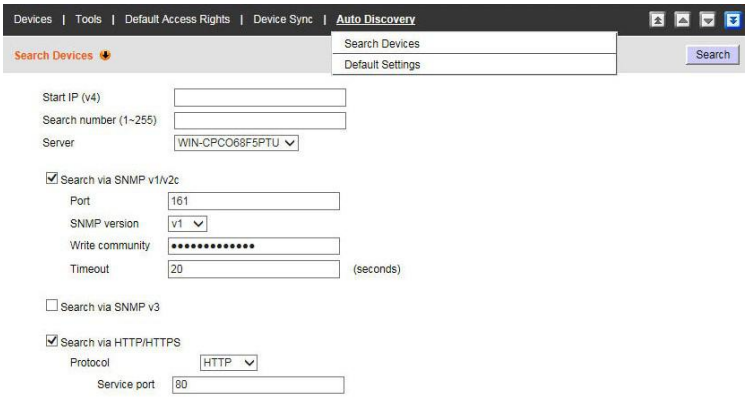
当您单击面板选单栏上的“设备设备”时，将出现如下页面：



这个网页可让您在配置的CC2000和安装设备之间自动同步名字。请勾选您要启用的功能的复选框，然后单击“**保存**”。

■ **自动发现**

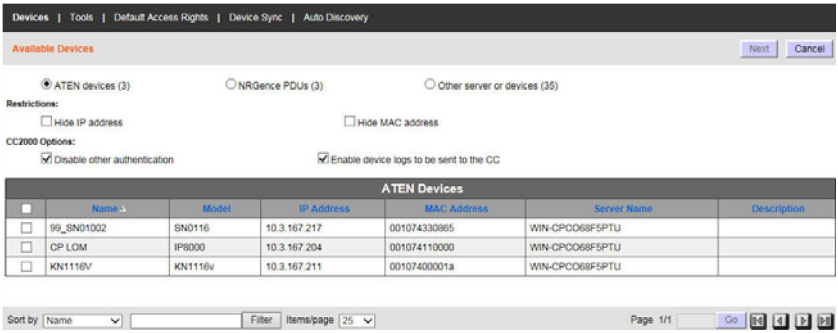
当您选择自动发现，会出现两个项目让您选择**默认设置**来扫描子网或**搜索设备**来搜索一个特定的IP地址，并将其添加到第三方服务器来支持服务处理器（如HP iLo3，APC的PDU，和虚拟化服务器），如下所示：



1. 根据以下表中所提供的信息填写字段：

字段	信息
初始 IP（v4）	在 IPv4 格式中输入 IP 地址设定搜索范围的开始。
搜寻数字 (1-255)	输入一个数字（1 到 255）来设置搜索范围的尾数。
服务器	使用下拉选单选择，设备连接到 CC2000 服务器。
通过 SNMP v1/v2c 进行搜索	如果您选中这个框，为端口填写相关的 SNMP 信息，SNMP 版本，写入社区和超时。这将使用 SNMP v1 / 2C 协议搜索设备。
通过 SNMP v3 搜索	如果您选中这个框，它将搜索使用 SNMP v3 协议的设备。
通过 HTTP/HTTPS 搜索	如果选中此框，使用下拉选单来选择协议，并输入服务端口号。这会寻找相匹配 HTTP 或 HTTPS 设置的设备。

2. 单击**搜索**将显示一个表格。使用单选按钮选择表中显示什么类型的设备（ATEN 设备、NRGence PDU 或其他服务器或设备）：



当选中**限制**和 **CC2000** 选项，*ATEN 设备* 表格会随着条件的变化而变化。

注意：当 CC2000 软件被安装在 Windows XP 平台时，搜索会延续一段时间。

描述 列揭示了三个结果中的一个：

结果	信息
空	未找到相关设备或者服务器

结果	信息
匹配 IP	CC2000 中发现具有相同的 IP 地址，但不同类型的设备或服务器。
匹配的	在 CC2000 中发现相匹配的 IP 地址和类型设备或服务器。

3. 单击要添加的设备或服务器的复选框。
4. 点击**下一步**。
5. 使用本章中指示来配置您在添加的设备类型。

侧边栏的设备配置

在创建设备时，建立了设备的配置的一些方面。当您在侧边栏或从主面板中的设备列表选择一个设备项目时，用来管理设备的额外设置变得可用。

从侧边栏或主面板中的设备列表点击调用几个面板选单，可以允许您改善设备项目的配置设置。提供的项目，以及面板选单下提供的设置项目，根据所选择的设备而变化。面板选单及其设置的说明将在下面的章节中提供。

注意：访问权限可以配置在在个人，端口到端口的基础上。给一个设备的用户访问和配置权限并不一定意味着把用户权限分配给设备上的每个端口的。

KVM设备和端口

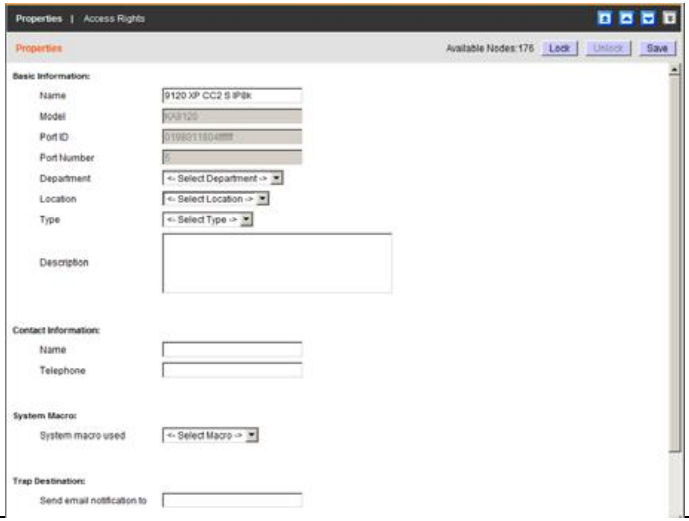
选择KVM设备，如IP8000或KN4132，或它的一个端口，在面板选单栏会在页面出现两个入口：属性和访问权限。这些项目中会在下面的章节中讨论。

属性

在“*属性*”页上发现的设置类似于“*添加设备*”部分中所描述的设置。详细信息见94页。

端口属性页与如下所示的屏幕类似：

在下表中给出了属性项的说明：



项目	解释
基本信息	**名称**：提供一个名称来标识端口。默认的是它的原始设备配置下的端口名称。如果您改变了端口名字，改变只会发生在 CC2000 数据库。原始配置的名称将保持不变。 **型号**: CC2000 识别了设备模型并且自动填写设备名称. 该名称不能被编辑. 如果设备是 Cat5e KVM 开关的，这里会显示 KVM 适配器电缆. **端口 ID**：端口身份是唯一的和永久的-他们不能被编辑。CC2000 自动填充这一领域。对于 Cat5e KVM 交换机端口，端口身份来自于 KVM 适配器电缆身份。 **端口编号**：CC2000 确定 KVM 切换器的端口是正在配置的端口并且自动填补这个区域。它不能被编辑。 **门类**：为了组织的目，您可以建立门类类别（例如，研发），并分配给他们的端口。如果您希望将此端口分配给一个门类，下拉列表的门类（您先前创建的-见 153 页 *门类、位置和类型*，），并点击一个您想要端口属于的门类。 **位置**：用于组织的目的，您可以建立位置类别（例如西海岸），并给他们分配端口。如果您希望将此端口分配到一个位置，下拉位置列表（先前已经创建-见 153 页 *门类、位置和类型*），并点击一个您想要端口属于的地点。 **类型**：用于组织目的，您可以指定设备的类型。如果您想这样做，下拉列表的类型（您以前创建的-见 153 页 *门类、位置和类型* ），并点击您想要的类型。 **描述**：如果您想提供额外的信息来描述端口，在这里输入。此字段是可选的。
联系信息	设备管理员的名称和电话号码。这些区域是可选的。
系统宏	如果已经取得系统宏，下拉列表并选择一个您想要的。当您关闭 KVM 查看器，宏将被发送到连接到该端口的服务器，该服务器将运行它。 **注意**：此项只出现在连接到它们的服务器的端口上。
陷阱目的地	您想要接收陷阱通知的人的电子邮件地址。此字段是可选的。

属性页操作按钮

当在侧边栏或交互式显示面板选择顶层（非嵌套）ATEN/ Altusen设备，在交互式显示面板的右上会出现一系列的动作按钮。下表中对这些按钮的目的有解释：

按钮	目的
Update All 更新全部	单击此按钮打开一个页面，列出所有嵌套在顶级设备之下的项目。此页面允许您配置每个（子）项目的（或重新配置）门类、位置、类型、描述和陷阱目的地。
Lock All 锁定全部	如果架构内设备节点的总数超出了许可数，您可以选择不包含哪些设备节点，并将其锁定。单击此按钮锁定所有的设备端口。详见第121页，锁定/解锁端口 了解更多信息。
Unlock All 解锁全部	如果有设备被锁定，单击此按钮解锁全部。
Save 保存	如果在属性页面做出更改，单击**Save**保存更改并继续。
Update 更新	如果设备安装信息不匹配CC2000数据库储存的信息 – 例如，如果适配器被移动到了另一端口，或者有新的适配器连接 – 其侧边栏图标上会添加一个问号，*Update*（更新）按钮会开启。在侧边栏选择设备，单击**Update**（更新）会使CC2000更新到设备在数据库的安装信息。
Move 移动	单击此按钮将设备移动到另一文件夹，在弹出的对话框中选择目标文件夹，单击**OK**。

若端口被选中，只有*锁定*、*解锁* 和*解锁全部* 按钮出现在页面右上方。这些按钮允许您单独锁定和解锁端口。详见第121页，*锁定/解锁端口* 。

访问权限 – KVM设备

当从侧边栏或交互式显示面板选中一台KVM设备时，您可以通过单击*Access Rights*界面选单项目设定配置和访问权限。单击此项目将弹出一个页面，显示所有获得权限的用户和群组。

■ 向设备用户、群组列表添加用户或群组

向用户或群组授予设备访问权限，执行如下：

1. 单击**Add**。符合条件的用户和群组出现。
2. 单击勾选您想要授予设备或端口访问的用户或群组名称前的复选框。
3. 为用户或群组设置配置权限：
   - **允许** – 用户或群组可以对设备进行设定。
   - **拒绝** - 用户或群组不可以对设备进行设定。
4. 为用户或群组设置访问权限：
   - **管理员** – 访问设备时，用户或群组有管理员权限（根据设备的认证政策）。
   - **用户** - 访问设备时，用户或群组有用户权限（根据设备的认证政策）。
   - **仅查看** – 访问设备时，用户或群组仅可以查看端口 – 无法执行任何活动。
   - **无访问** – 用户或群组无法访问设备端口。
5. 完成配置权限设定后，单击**Save**（保存）。新的用户和群组会被添加到设备的用户/群组列表。

■ 修改用户或群组权限

修改用户或群组对设备的权限，执行如下：

1. 在您想要修改的用户或群组相应的*配置权限* 栏，单击箭头；作出新的选择；然后点击**Close**（关闭）。
2. 在您想要修改的用户或群组相应的*访问权限* 栏，单击箭头；作出新的选择；然后点击**Close**（关闭）。
3. 单击**Save**（保存）（界面右上方）。

■ 删除用户或群组权限

删除用户或群组对设备的权限，执行如下：

1. 单击勾选您想要移除的用户或群组名称前的复选框。
2. 单击**Delete**（界面右上方）。

■ 操作按钮

除添加、删除和保存外，还有一个Update All（更新全部）按钮（界面右上方）。单击此按钮将打开一个页面，允许您为选中设备或端口的所有用户和劝阻设定配置和访问权限。

访问权限 – KVM端口

当从侧边栏或主界面选中一个端口时，您可以通过单击*Access Rights*界面选单项目设定配置和访问权限。单击此项目将弹出一个页面，显示所有获得权限的用户和群组。

■ **向端口用户、群组列表添加用户或群组**

向用户或群组授予端口访问权限，执行如下：

1. 单击**Add**。符合条件的用户和群组出现。
2. 单击勾选您想要授予端口的用户或群组名称前的复选框。
3. 为用户或群组设置配置权限：
   - **允许** – 用户或群组可以对端口进行设定。
   - **拒绝** - 用户或群组不可以对端口进行设定。

   注意：此设定仅限于Cat 5e KVM多电脑切换器。

4. 为用户或群组设置访问权限：
   - **完全权限和VM（读/写）/只读** – 用户可以查看远程屏幕并在自己的键盘和显示器上对远程系统进行操作。用户在使用虚拟媒体功能时有读/写或只读权限。

     注意：此功能仅限于KN2124v, KN2140v, KN4124v, and KN4140v切换器。

   - **完全访问** - 用户可以查看远程屏幕并在自己的键盘和显示器上对远程系统进行操作。
   - **仅查看** – 用户可查看远程屏幕，无法执行操作。
   - **无访问** – 端口不出现在用户的端口访问侧边栏或状态与操作列表（详见第35页，*端口访问*）。
5. 完成配置权限设定后，单击**Save**（保存）。新的用户和群组会被添加到端口的用户/群组列表。

■ 修改用户或群组权限

修改用户或群组对端口的权限，执行如下：

1. 在您想要修改的用户或群组相应的*配置权限* 栏，单击箭头；作出新的选择；然后点击**Close**（关闭）。
2. 在您想要修改的用户或群组相应的*访问权限* 栏，单击箭头；作出新的选择；然后点击**Close**（关闭）。
3. 单击**Save**（保存）（界面右上方）。

■ 删除用户或群组权限

删除用户或群组对端口的权限，执行如下：

1. 单击勾选您想要移除的用户或群组名称前的复选框。
2. 单击**Delete**（界面右上方）。

■ 操作按钮

除添加、删除和保存外，还有一个*Update All*（更新全部）按钮（界面右上方）。单击此按钮将打开一个页面，允许您为选中设备或端口的所有用户和劝阻设定配置和访问权限。

复制粘贴访问权限

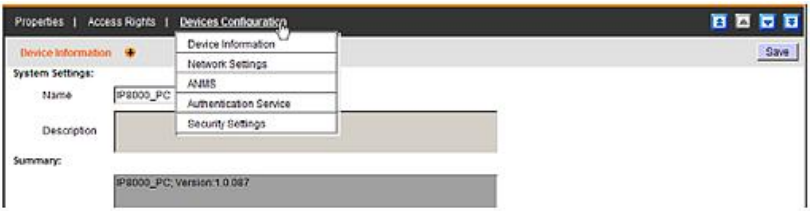
访问权限复制-粘贴功能在兼容的节点之间开启（如插座对插座）。如要使用此功能，在侧边栏的树状图中，右击插座，并选择复制访问呢权限。右击另一个插座，并选择粘贴访问权限。

设备设定(针对 KVM 设备)

设备设定的目的是为了允许您从 CC2000 内部设定设备，而无需直接访问设备。这些页面上的修改实际上在设备本身上做的。

注意：如果 CC2000 和设备之间的连接由于某些原因中断，在这些页面上做的修改将不会被传送到设备。要修改设备设定，您可以直接登录设备(详情请见第 80 页的 *CC2000 选项*)。

此子菜单项目包含几个次级子菜单页。要修改这些页面上的信息，或是点击主面板左边灰色栏中的箭头图标(和)，按顺序经过这些页面；或是停留于菜单之上并从出现的弹出菜单中选择页面，而直接到页面。



注意：如果设备离线，设备设定子菜单不出现。

Device Information 次级子菜单是此项目的默认页面。如果您喜欢的话，可以修改设备的*名称*。当修改名称时，修改只发生在设备上，在 CC2000 数据库中的名称不改变。

Description and *Summary* 部分仅供浏览，不能在此页修改。*Summary* 部分提供设备当前状态的清单。

次级子菜单页相当于设备的用户手册中描述的管理功能。对于设定设置，请参考手册的*管理*这一章，以获得必要信息。当完成设定设置后，点击 **Save**。

注意：1. 在 CC2000 的次级子菜单 ANMS settings 页，除了标为 *Preferred CC Server Settings* 的条目外，还要一个称作 *Alternate CC Server Settings* 的条目。Preferred 设置相当于设备上的 ANMS 设置(见 245 页的*设备 ANMS 设置*)。对此设置的修改发生在设备上。Alternate 设置条目允许您为 CC2000 冗余从服务器设置一个 IP 地址和端口(见 23 页的 *CC2000 冗余从服务器*)。虽然此设置不出现在设备的 ANMS 页，但是如果首选服务器不可用时，它将在设备上生效。

2. 在 CC2000 的次级子菜单 Customization settings 页，有一个称作 *Port timeout* 的条目。此区为端口上的用户设置一个时间限制，此端口的访问模式已被设置为*占用*(见第 138 页的*模式*)。

这相当于以前的设备上的*访问模式*设置。如果在此设置的时间内占用端口的用户没有操作，用户就被超时注销。端口被释放后发送键盘或鼠标输入的第一位用户占用端口。

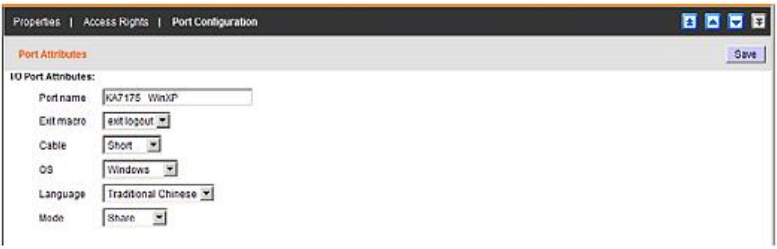
输入一个 0 到 255 秒的值。默认为 3 秒。设置为 0 导致没有输入端口立即被释放。

端口设定(针对 Cat 5e KVM 设备)

端口设定的目的是为了允许您从 CC2000 内部设定端口，而无需直接访问设备。这些页面上的修改实际上在设备本身上做的。

注意：如果 CC2000 和设备之间的连接由于某些原因中断，在这些页面上做的修改将不会被传送到设备。要修改设备设定，您可以直接登录设备(详情请见第 80 页的 *CC2000 选项*)。

此子菜单用来设置被选择端口的 I/O 属性：



属性标题的含义如下表所描述：

标题	含义
Port Name	这是为端口起的名称。
Exit Macro (退出宏)	如果已制作了系统宏，下拉列表以选择您要的宏。当您关闭 KVM 浏览器时，宏将被发送到连接此端口的服务器，且服务器将运行此宏。
Cable (线缆)	指定用来连接电脑和端口的 Cat 5e 线缆的长度。
OS (操作系统)	指定所连端口上电脑使用的操作系统。
Language (语言)	指定所连端口上的电脑使用的操作系统语言。
Mode (模式)	此功能相当于以前的设备是的访问模式：Share(分享)、Occupy(占用)、Exclusive(独占)。它限定多位用户登录时，端口如何被访问。 **Exclusive:** 第一位切换到端口的用户对端口有独占控制权。其它用户不能浏览端口。*Timeout* 功能不适用于有此设置的端口。 **Occupy:** 第一位切换到端口的用户对端口有控制权。但是，另外的用户可以浏览端口的视频。如果控制端口的用户没有活动的时间超过在 *Timeout* 框中设置的时间，端口控制权转移到下一位移动鼠标或敲击键盘的用户。 **Share:** 用户同时分享端口的控制权。用户的输入放在序列中，并按时间顺序执行。

设定设置，请参考设备的用户手册以获得必要的信息。当做完设定设置后，点击 **Save**。

电源设备、层级和端口

选择一台电源设备则打开一个页面，页面子菜单上有如下条目：Properties(属性)、Access Rights(访问权)和 Device Configuration.(设备设定)。

注意：1. 当在侧栏树形图中选择一台电源设备(PN9108)时，并扩展其下的条目，显示于 PN9108 条目之下的首层级实际上是 PN9108 其本身。第二层级是从首层级菊式串连出来的电源层级(PN9108 或 PN0108)。

2. 虽然从首层级 PN9108 可菊式串连出另外的 PN9108，但由于通过 CC2000 用单点登录可以访问它们全都，所以不必菊式串连它们来实现通过单一 IP 地址进行的管理。因此，它们可单个部署，而不用菊式串连。

3. CC2000 不直接支持 PN0108。因为 PN0108 没有因特网访问功能，只有当菊式串连到 PN9108 时，它们才被支持。

当您选择一个属于电源设备的层级时，Device Configuration 条目变为 *Station Configuration*。当您选择一个属于层级的插座端口时，Station Configuration 条目变为 *Port Configuration*，且另一条目 *Redundant Power* 出现。这些子菜单在下面的部分讨论。

属性

这些在*属性*页上找到的、针对设备、层级或插座端口的设置与在 *KVM 设备和端口*部分描述的设置相似。详情请见第 129 页的表格。

■ 锁定/解锁

当某插座端口被选择，两个按钮出现在端口属性页的右上方：*Lock* 和 *Unlock*。这些按钮执行的功能与它们在 KVM 端口上执行的功能相同。详情请见第 131 页的*锁定/解锁*。

访问权

可整个设备、逐层级或逐端口设定访问权。选择设备、层级或插座端口后，点击此子菜单条目则打开一个页面，页面列出已指定访问权的用户和群组。

■ 添加用户或群组到设备、层级或端口访问列表

可为用户或群组设置对设备、层级或端口的设定权以及端口访问权。要为用户或群组设置权限，请按如下操作：

1. 点击 **Add**。合格用户和群组的列表出现。
2. 点击勾选您让其要访问设备、层级或端口的用户或群组名称前面的复选框。
3. 为用户或群组设置设定权：
   - **Allowed** – 用户或群组可以设定设备的设置。
   - **Denied** – 用户或群组不可以设定设备的设置。
4. 如果选择了某插座端口，那么为用户或群组设置访问权：
   - **Allowed** – 用户或群组可以访问端口。
   - **Denied** – 用户或群组不可以访问端口。端口不出现在用户的端口访问侧栏或状态和操作列表(见第 143 页*端口访问*)。
1. 做完设定权设置后，点击 **Save**。新用户和群组被添加到设备、层级或端口用户/群组列表。

■ 修改用户或群组的权限

修改用户或群组的对设备、层级或端口的权限，请按如下操作：

1. 在对应于您要修改的用户或群组的 *Configuration Rights* 栏，点击箭头；选择 **Allowed** 或 **Denied**；然后点击 **Close**。
2. 如果选择了某端口，在对应于您要修改的用户或群组的 *Access Rights* 栏，点击箭头；选择 **Allowed** 或 **Denied**；然后点击 **Close**。
3. 点击**Save** (在面板的右上方)。

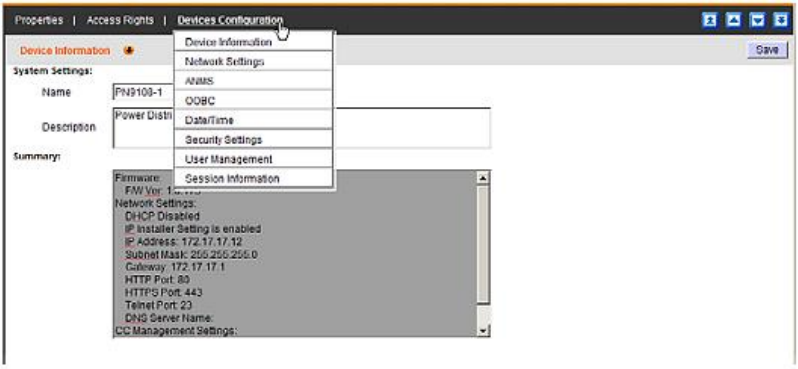
■ **删除用户或群组的权限**

删除用户或群组对设备、层级或端口的权限，请按如下操作：

1. 点击勾选要删除的用户或群组名称前面的复选框。
2. 点击 **Delete** (在面板的右上方)。

设备设定(针对电源设备)

此子菜单项目与 136 页上讨论的 KVM 设备设定子菜单项目相似，除了它有不同的次级子菜单页：



这些次级子菜单的目的是为了允许您从 CC2000 内部设定设备，而无需直接访问设备。

注意： 如果 CC2000 和设备之间的连接由于某些原因中断，在这些页面上做的设备设定修改将不会被传送到设备。要修改设备设定，您可以直接登录设备(详情请见第 95 页的 *CC2000 选项*)。

次级子菜单页相当于设备的用户手册中描述的管理功能。对于设定设置，请参考手册的*管理*这一章，以获得必要信息。当完成设定设置后，点击 **Save**。

注意：1. 在 CC2000 的次级子菜单 ANMS settings 页，除了标为 *Preferred CC Server Settings* 的条目外，还要一个称作 *Alternate CC Server Settings* 的条目。Preferred 设置相当于设备上的 ANMS 设置(见 245 页的*设备 ANMS 设置*)。对此设置的修改发生在设备上。Alternate 设置条目允许您为 CC2000 冗余从服务器设置一个 IP 地址和端口(见 23 页的 *CC2000 冗余从服务器*)。虽然此设置不出现在设备的 ANMS 页，但是如果首选服务器不可用时，它将在设备上生效。

2. 在 CC2000 的次级子菜单 ANMS settings 页，有一个标为 *Event Trap and Notification* 的条目。其列出四个事件，如下表所描述：

事件	描述
System Power On	当电源设备被供电时。
System Restart	当电源设备被重启时。
Outlet Fault	当插座端口出现问题 (过载情况或继电失败) 时。
UPS Fault	当 UPS 设备发生问题(连接电源与电源设备的 UPS 在简单信号设定中)时。关于更多信息，请参考设备用户手册的 UPS 第一部分。

勾选复选框，以启用您希望在指定的事件发生时被通知的项目事件。

层级设定(针对电源设备)

由于电源设备可菊式串连，被串连的层级显示在侧栏列表上电源设备条目之下。此子菜单的*属性*和*访问权*页已在从第 139 页开始的部分讨论。

此子菜单条目与第 141 页上讨论的电源设备的子菜单条目相似，除了它有不同的次级子菜单页：

次级子菜单页相当于设备的用户手册中描述的管理功能。对于设定设置，请参考手册的*管理*这一章，以获得必要信息。当完成设定设置后，点击 **Save**。

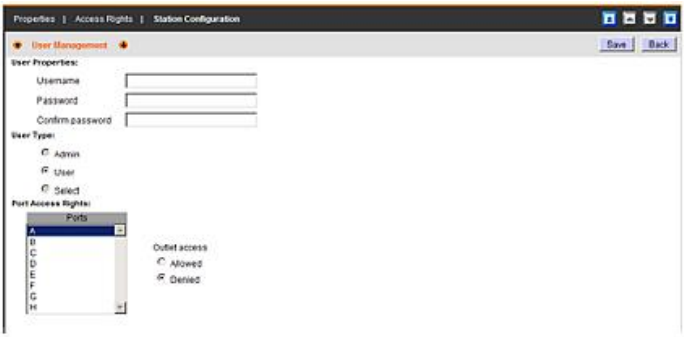
注意：1. 您对用户管理设置所做的修改影响电源设备的内部验证操作。其不影响 CC2000 的验证操作。

2. 如果 CC2000 和设备之间的连接由于某些原因中断，在这些页面上做的设备设定修改将不会被传送到设备。要修改设备设定，您可以直接登录设备(详情请见第 95 页的 *CC2000 选项*)。

用户管理次级子菜单页让您添加、编辑和删除用户对层级上的端口的访问权。

◆ 添加一位用户，请按如下操作：

1. 点击 **Add** 按钮(在面板的右上方)。用户管理页出现：



2. 在用户属性各区键入用户名和密码。
3. 跳过 *User Type* 条目－其是固定的，不能修改。
4. 所有插座的插座访问权默认为 *Denied*。对于您要使用户有访问权的各插座，先在列表中选择它，然后点击 *Allowed* 单选按钮。
5. 当完成此页后，点击 **Save**。

◆ 编辑用户的信息，请按如下操作：

1. 从用户管理次级子菜单页，点击 **Edit** (在面板右上方)。
2. 当用户管理页出现时，进行修改，然后点击 **Save**。

◆ 删除用户的端口访问权，请按如下操作：

1. 从用户管理次级子菜单页，点击选择用户名前面的单选按钮。
2. 点击 **Remove** (在面板右上方)。

关于设定其余次级子菜单页，请参考设备用户手册的*设定*部分。依设备而变，此部分将在*电源管理设定*或*设备控制*下找到。

当完成这些页面的设定设置后，点击 **Save** (在面板右上方)。

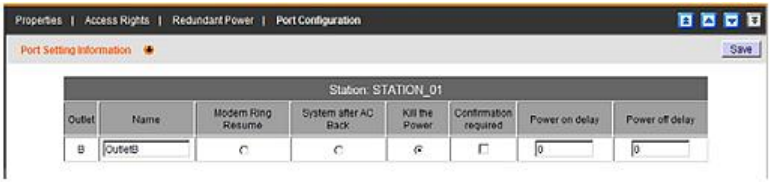
端口(插座)设定(针对电源设备)

电源插座端口嵌套在其各层级之下。各插座的设置逐端口可单独设定。端口设定有两个次级子菜单：*Port Settings*(端口设置)和 *Schedule Settings*(计划设置)。

注意：如果 CC2000 和设备之间的连接由于某些原因中断，在这些页面上做的设备设定修改将不会被传送到设备。要修改设备设定，您可以直接登录设备(详情请见第 95 页的 *CC2000 选项*)。

■ **端口设置**

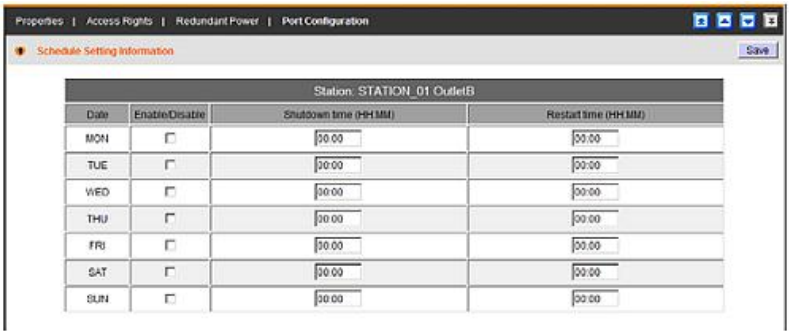
要打开针对特定插座的端口设置页，在侧栏选择它，然后点击子菜单栏上的 **Port Configuration**。一个类似如下的页面出现：



如果要修改这些设置，关于各区的说明，请参考设备用户手册的*设定*部分。依设备而变，此部分将在*电源管理设定*或*设备控制*下找到。当完成这些页面的修改后，点击 **Save**。

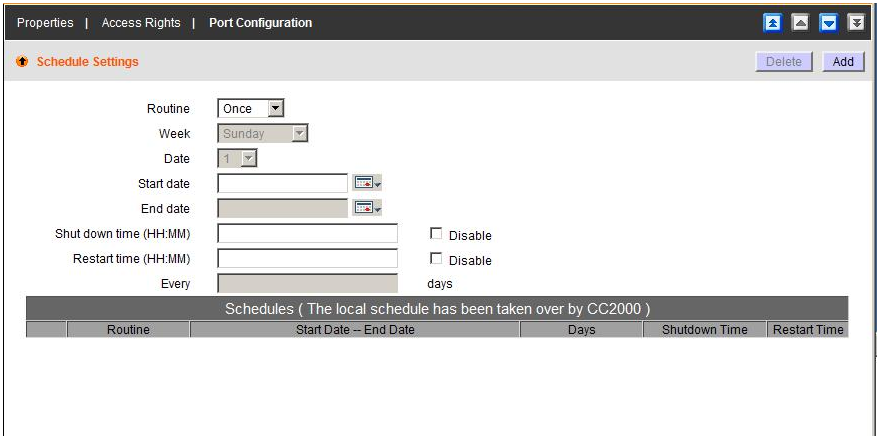
■ **计划设置**

计划设置页允许您为各插座设置一个电源开/关设定。要打开针对某特定插座的计划设置页，在侧栏选择它；停留在子菜单栏上的 **Port Configuration**；然后选择出现的菜单上的 **Schedule Settings**：



关于如何为插座设置电源开/关设定计划的说明，请参考设备用户手册的*计划*部分。当完成这些页面的修改后，点击 **Save**。

如果插座在PN7xxxx系列PDU上，如下的一个页面将会出现：



参阅每台设备用户说明书的*Schedule*（排程）章节，了解如何设置电源插座开机/关机排程。在端口配置页面完成变更后，点击**Save**（保存）。

注意：在CC2000上设置的电源设备插座排程，可替换在本地设备上设定的任何排程。

串口设备和端口

选择某串口设备，如 SN0108，则打开一个页面，其子菜单栏有如下条目：Properties(属性)、Access Rights(访问权)和 Device Configuration.(设备设定)。当选择串口设备时的某端口时，*Device Configuration* 标题变为 *Port Configuration*。

属性

除了一个额外的菜单条目*Enable SN device session history to be sent to the CC*之外，在设备或端口的*属性*页上找到的设置与在*添加设备*部分描述的设置相似。详情请见第94页的表格。

■ SN 设备会话历史

如果选择*Enable SN device session history to be sent to the CC*，串口设备的会话历史将被发送到并存储在CC2000服务器上，其将成为CC2000的可搜索的数据库的一部分。

■ 锁定/解锁

当某端口被选择时，两个按钮出现在端口属性页的右上方：*Lock* 和 *Unlock*。这些按钮执行的功能与它们在 KVM 端口上执行的功能相同。详情请见第 139 页的*锁定/解锁*。

访问权

可整个设备或逐端口设定访问权。选择设备或端口后，点击此子菜单条目则打开一个页面，页面显示一个已指定访问权的所有用户和群组的列表。

■ 添加用户或群组到设备或端口访问列表

要为用户或群组设置对设备或端口的访问权，请按如下操作：

1. 点击 **Add**。合格用户和群组的列表出现。
2. 点击勾选您要让其访问设备或端口的用户或群组名称前面的复选框。
3. 为用户或群组设置设定权：
   - **Allowed** – 用户或群组可以设定设备的设置。
   - **Denied** – 用户或群组不可以设定设备的设置。
4. 如果选择了某端口，那么为用户或群组设置访问权：
   - **Telnet** – 用户或群组必须通过 Telnet 会话访问端口。
   - **Denied** – 用户或群组必须通过 SSH 会话访问端口。。

5. 做完设定权设置后，点击 **Save**。新用户和群组被添加到设备、层级或端口用户/群组列表。

■ 修改用户或群组的权限

修改用户或群组的对设备、层级或端口的权限，请按如下操作：

1. 在对应于您要修改的用户或群组的 *Configuration Rights* 栏，点击箭头；选择 **Allowed** 或 **Denied**；然后点击 **Close**。
2. 如果选择了某端口，在对应于您要修改的用户或群组的 *Access Rights* 栏，点击箭头；选择 **Telnet**、**SSH(或两者)**；然后点击 **Close**。
3. 点击**Save** (在面板的右上方)。

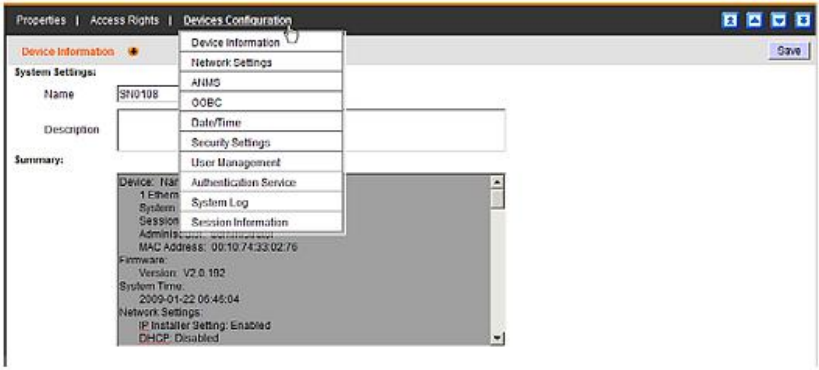
■ 删除用户或群组的权限

删除用户或群组对设备、层级或端口的权限，请按如下操作：

1. 点击勾选要删除的用户或群组名称前面的复选框。
2. 点击 **Delete** (在面板的右上方)。

设备设定(针对串口设备)

*设备设定*页与针对*电源设备*、*层级和端口*的页面相似(见第 141 页的*设备设定(针对电源设备)*)，但是在次级子菜单页有一些区别：



这些次级子菜单页是为了允许您从 CC2000 内部设定设备，而无需直接访问设备

次级子菜单页相当于设备的用户手册中描述的管理功能。对于设定设置，请参考手册的*管理*这一章，以获得必要信息。当完成设定设置后，点击 **Save**。

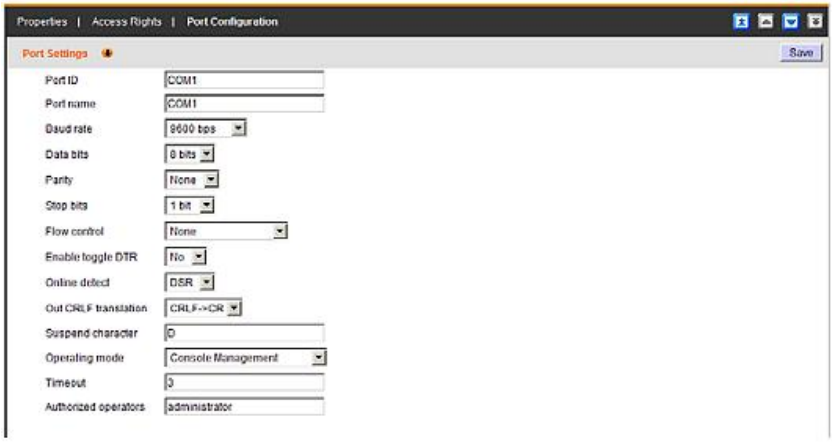
注意：如果 CC2000 和设备之间的连接由于某些原因中断，在这些页面上做的修改将不会被传送到设备。您可以直接访问设备(用其 URL)，但是如果已选择了 *Disable other authentication*，您必须取消对此功能的勾选(详情请见第 80 页的 *CC2000 选项*)。

端口设定(针对串口设备)

串口 COM 端口嵌套在其各设备之下。各端口的设置可逐端口单独设定。端口设定有两个次级子菜单：*Port Settings*(端口设置)和 *Advanced Port Settings*(高级端口设置)。

■ 端口设置

打开某特定端口的设置页，在侧栏选择它，然后点击子菜单栏上的 **Port Configuration**。一个类似如下的页面出现：

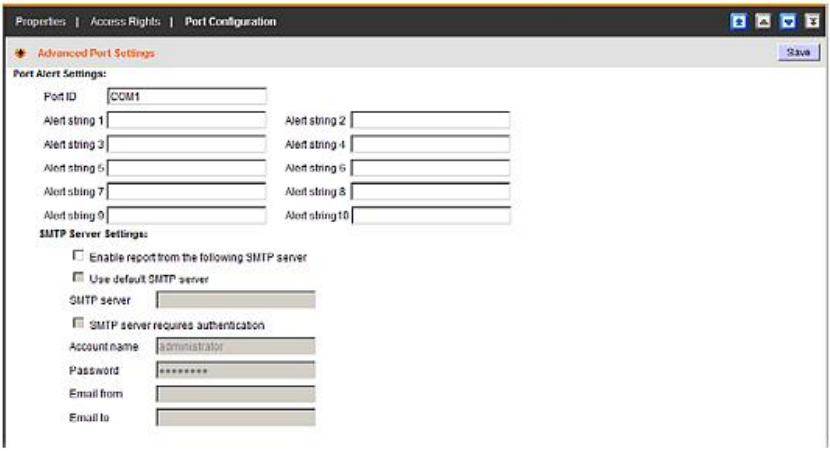


关于各区的说明，请参考设备用户手册的*端口属性设置*部分。当完成设定设置后，点击 **Save**。

■ 高级端口设置

此页提供一种方法，用这种方法逐端口通知您发生在设备 COM 端口上的问题。要设定通知，请按如下操作：

1. 在侧栏选择端口；停留在子菜单栏上的 *Port Configuration*；然后选择出现的菜单上的 **Advanced Port Settings**。一个类似如下的页面出现：



2. 关于各区的说明，请参考设备用户手册的*端口警告设置*部分。当完成设定设置后，点击 **Save**。

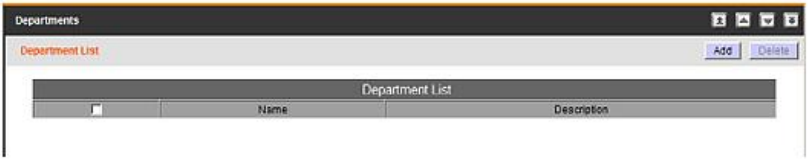
部门和位置

为了简便的管理，*Departments*(部门)和 *Locations*(位置)页提供另外两种组织设备的方法。要使用此组织方案，首先要创建适当的类别(如部门下的 *R&D* 和*生产部*，及位置下的*东海岸操作*)，然后向其分配设备(从设备的属性页)，如下面的部分所描述。

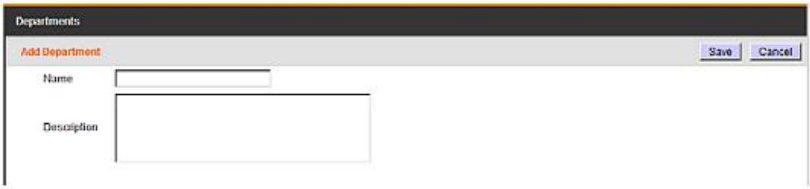
添加部门或位置

创建部门或位置，请按如下操作：

1. 在菜单栏选择 **Department** (或 **Location**)。部门列表(或位置列表)页出现：



2. 点击 **Add**(在面板右上方)。Add Department(or Location)页出现：



3. 填写名称和描述区，然后点击 **Save**。

分配设备到部门或位置

分配设备到部门或位置，请按如下操作：

1. 在菜单栏选择 **Devices**。
2. 在侧栏，选择您要分配到部门或位置的设备或端口。其*属性*页出现(见第 93 页)。
3. 下拉部门或位置列表，并点击您要设备或端口属于的部门或位置。

修改部门或位置

修改部门或位置的名称或描述，请按如下操作：

1. 在菜单栏选择 **Departments** 或 **Location**。
2. 在侧栏或主面板，选择您要修改的部门或位置。
3. 在子菜单栏，选择 **Properties**。
4. 进行修改，然后点击 **Save**。

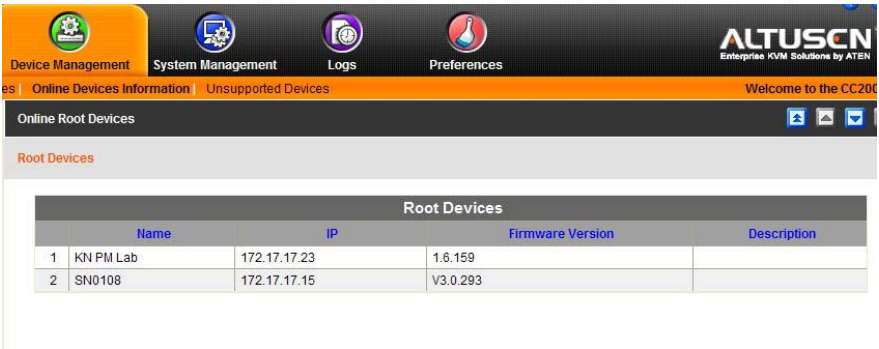
删除部门或位置

删除部门或位置，请按如下操作：

1. 在菜单栏选择 **Departments** 或 **Location**。部门或位置列表页出现。
2. 点击勾选您希望删除的部门或位置的名称，然后点击 **Delete**(在面板右上方)。

在线设备信息

Online Devices Information（在线设备信息）选项卡便于查看通过CC2000管理的设备信息。点击选项卡打开分布在架构中的设备/加密狗并显示其IP地址和固件版本，如下所示：



注意： 1. 此为进攻浏览选项卡 – 不能执行操作。

2. 列出的根设备根据名称、类型和IP分类。

不支持的设备

不支持的ATEN/Altusen设备，其固件版本不兼容CC2000当前的固件版本。点击选单栏的Unsupported Devices（不兼容设备），将弹出一个一面，列出CC2000机构中所有不兼容设备。

为确保这些设备可以在CC2000下进行管理，其固件必须更新到最新版本。按下述操作：

1. 添加设备的固件更新文件到CC2000。具体操作详见第206页，*设备文件* 。
2. 设备的固件更新文件保存到CC2000上之后，此页面上其勾选框会变为活跃。在勾选框上打勾。
3. 完成步骤2后Firmware Upgrade（固件更新）按钮，（面板左上方），变为活跃。
4. 点击**Firmware Upgrade**（固件更新）更新设备的固件。

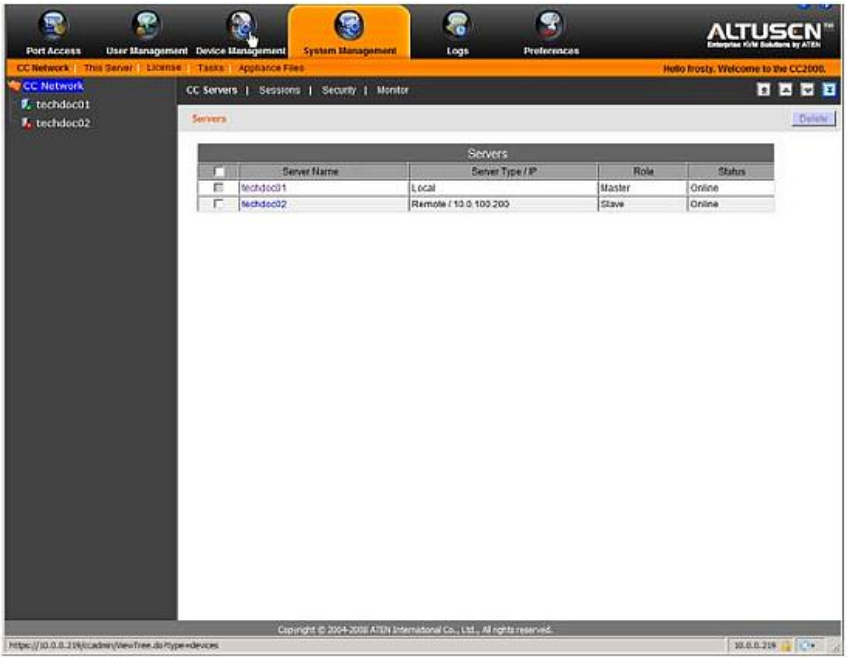
固件更新完成后，设备会从不支持的设备列表中移除，现在将显示在可用设备列表中（详见第91页，*添加文件夹或设备* ）。

第七章
系统管理

概述

CC2000 设备由兼容 CC2000 的设备组成，这些设备处在通过 IP 连接 CC2000 服务器的网段上，且 CC2000 也处于同一网段。CC2000 远程集中管理系统通过 IP 地址将单个 CC2000 服务器网段连接成一个整合的全球网络，它使您随时随地通过因特网连接从单一 IP 地址登录，安全、集中地访问所有数据中心设备。

为了管理和部署的目的，其中一台 CC2000 服务器作为*主*；其它服务器作为 *salve*。当点击系统管理选项卡是，CC2000 打开默认的 *CC 网络页*，此页类似如下窗口：



注意：系统管理页限于系统管理员使用。其它类型用户可跳过本章。

菜单架构

系统管理菜单架构如下表所述：

选项卡	主菜单	子菜单	被选择的 CC 服务器子菜单	页码
系统管理	CC 网络	CC 服务器	属性	159
			会话	210
		会话		160
		安全		161
		监控器		162
	本服务器	服务器信息		164
		服务器设置	SMTP	168
			NTP	170
			Syslog	171
			拨入	175
			拨出	176
		主设置 *		179
		SMTP 设置		180
		安全		181
		认证		184
	许可证			187
	任务			190
	设备文件			206

* 此项目仅出现于从 CC服务器上。

CC 网络

CC Network 菜单提供四个子菜单选项：CC Servers(CC 服务器)、Sessions(会话)、Security(安全)和 Monitor(监控器)。默认 CC 网络页是 CC 服务器，其类似如下：

CC 服务器

侧栏提供存在于设备中的所有CC服务器的树形图清单。图标上的绿色勾说明服务器当前可访问；红色X说明服务器当前不可访问。

交互显示面板提供CC2000服务器的表格形式清单，附带一些关于它们的基本信息。

如果从主服务器浏览本页，在任何从名称前的框内打勾，再点击主面板右上方的 **Delete**，即可将其删除。

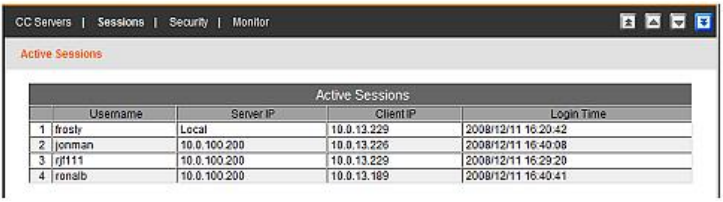
注意：仅可从主服务器删除服务器。

服务器表格标题的含义如下表：

标题	含义
Server Name (服务器名)	安装服务器时为其指定的名称(见第164页的*服务器信息*)。
Server Type/IP (服务器类型/IP)	*Local* 表示您已登录的 CC2000。对于设备中其它 CC2000，术语 *Remote* 和 CC2000 的 IP 地址出现。
Role (角色)	CC2000 管理系统中的两大角色是主和从。另外，还有第三个角色 *Substitute 主*，当主与系统连接中断时(例如由于网络问题)，在此角色中其中一个从暂时接替主的角色。当主与系统重又连接时，此 Substitute 主恢复其从状态。 **注意**：1. 充当 Substitute 主 的 CC2000 由 CC2000 管理系统自动选择。选择基于 CC2000 注册顺序(最早在主注册的成为 Substitute 主)。 2. Substitute 主执行关于提供集中管控的主角色，它不能用来添加或删除设备；它不能注册从服务器；从不能复制其数据库到 Substitute 主。
Status (状态)	说明 CC2000 在线或离线。

会话

此 *Sessions* 子菜单(当 CC 网络/CC 服务器在主菜单时被选择时或 CC 网络在侧栏被选择时出现的)列出当前发生在设备中所有 CC2000(主及从)上的所有会话，并提供各会话“谁、何地和何时”的信息。

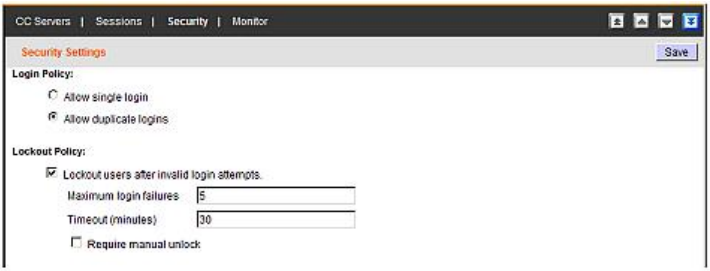


注意：1. 要只浏览特定 CC2000 服务器的会话，使用主面板右上方的导航按钮选择此服务器。

2. 要结束会话，必须从 CC Servers → Sessions 子菜单(见第 210 页)进行。

安全

Security 子菜单提供两个设置类别：Login Policy(登录策略)和 Lockout Policy(锁定策略)和用户角色限制政策：



登录策略

- 如果不希望用户能够同时多次登录，选择 **Allow single login**。
- 如果希望能够用同一帐户同时多次登录，选择 **Allow duplicate logins**。此为默认选项。

锁定策略

- 在超过指定的失败登录次数后锁定用户，点击勾选 *Lockout users after invalid login attempts* 复选框，启用锁定功能。此为默认选项。

> **注意**：如果您未勾选此框，用户可以尝试无限制的多次登录。为安全起见，我们建议您启用锁定策略。

- 在 *Maximum login failures* 区键入希望允许用户被锁定前的登录失败次数。在此指定的值必须至少为 1。默认为 5。
- 在 *Timeout* 区键入被锁定的用户被允许再次登录前必须等待的时间值(分钟数)。在此指定的值必须至少为 1。默认为 30。
- 启用 *Require manual unlock* 意味着其帐户被锁定后用户将不能登录，直至用户联系管理员，让管理员手动解锁帐户。详情请见第 65 页*解锁用户帐户*。默认为禁用(不勾选此复选框)。

用户角色限制政策

此设置分类允许管理员创建用户账号，可以没有角色限制，或者有三者之一的预设限制政策。选项如下：

- 没有角色限制
- 限制系统管理角色（1-5）
- 限制系统和用户管理角色（1-8）
- 限制所有角色（1-12）

注意：1-12的完整信息，请参阅第71页，*系统类型* 下的表格。

监视器

Monitor（监视器）面板选单项目提供另一种访问架构中CC2000服务器的方式：

此页面可以开启实时地图视图，允许您查看架构中所有CC2000服务器，其联机/脱机状态。主服务器在顶部；次级排场一排（或几排）在主服务器之下。联机状态通过图标是否显示绿色信号灯表示。

点击图标打开服务器的*Properties*（属性）页面。此页面与在侧边栏点击服务器的名称，或在*CC Server*（CC服务器）交互式显示面板列表点击相同（详见第159页截图）。

注意：当此页面打开后，用户的超时设置（详见第56页，*用户账户*），变为无效 – 用户不会超时退出。

您可以创建地图视图并保存至收藏夹：点击 **Add**（添加）；在*收藏名称* 字段输入名称；点击 **Save**（保存）。如要返回到某一视图，从下拉列表选择即可。如要删除某一视图，从下拉列表中选择后，点击 **Delete**（删除）。

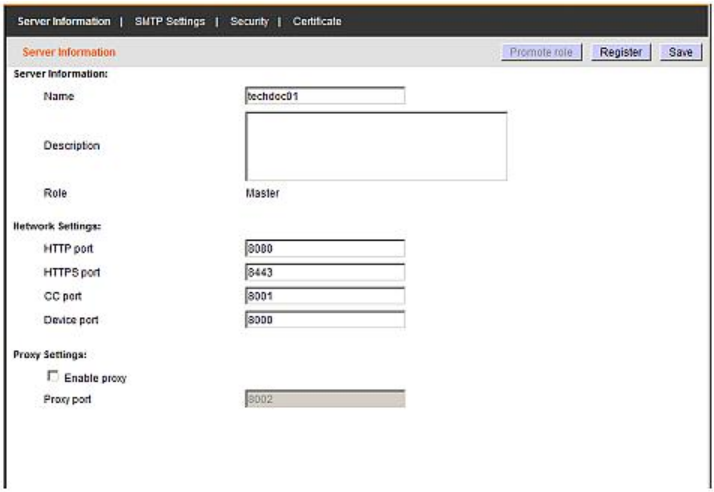
本服务器

This Server 菜单是指您当前登录的 CC2000 – 设备中其它 CC2000 服务器被忽略。菜单提供四个选项：Server Information(服务器信息)、SMTP Settings(SMTP 设置)、Security(安全)和 Certificate(认证)。

注意： 1. 换到其它服务器只能通过直接登录这些服务器来实现。
2. 从服务器有额外菜单项目 – 主 Settings(主设置) – 详情请见第 179 页。

服务器信息

默认页为 Server Information，此页类似如下：



此页允许您设定 CC2000 服务器的设置。各区标题的含义如下表所述：

区域	功能描述
Name *	编辑此区，可以修改 CC2000 服务器的名称。
Description	编辑此区，可以修改 CC2000 服务器的描述。描述可以是 2-32 字节的任何支持的语言。
Role	表示此服务器是主还是从。 **注意**：用面板右上方的 Promote Role 按钮(见第 166 页)可将从改为主。
HTTP *	CC2000 用来与因特网浏览器通讯的端口。
HTTPS *	CC2000 用来与浏览器因通过特网通讯的安全端口。
CC Port *	CC2000 用来与设备中其它 CC2000 通讯的端口。
Device Port *	CC2000 用来与设备中的设备通讯的端口。
Enable Proxy (启用代理)	如果您需要用代理功能，勾选此框，然后在指示区域指定代理端口。见第 248 页的 *CC2000 代理功能*。

* 详情请见第 15 页。

当完成所有设定设置后，点击 **Save**。

操作按钮

面板右上方有两个操作按钮：Promote Role(提升角色)和 Register(注册)。其功能在下面的部分描述：

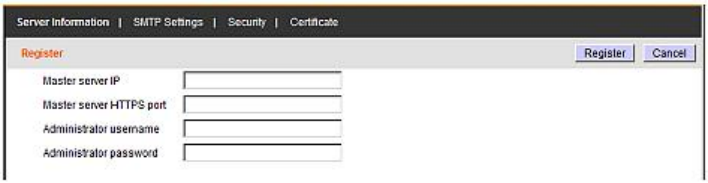
- 提升角色(从转主)

  Promote Role 按钮在面板右上方，用来转换从 CC2000 为主。当点击此按钮时，转换自动执行，先前的主现在变为从。所有其它在线从自动识别此新主。

注意：1. 此按钮仅在从设备上可用。
2. 必须换到不同页面，再换回以便看到这些修改。
3. 我们建议设备中所有 CC2000 服务器应该在转换角色时在线。如果转换角色时任何从离线，其必须再次执行*主 Settings* 操作。详情请见第 179 页的*主设置*。如果旧主在转换角色时离线，其重回在线时必须要在新主注册。详情请见下一页。

◆ 注册

Register 按钮在面板右上方，用来将 CC2000 服务器作为从整合到较大的 CC2000 网络中。点击此按钮时，如下窗口出现：



将服务器整合到较大的网络中，在正确的区域输入要求的信息，然后点击 **Register**。

注册完成后，您自动退出。重新登录时，您的服务器现在作为主设备中的一个从出现。

注意：1. 对于 *Administrator username* 区，我们建议使用默认的超级管理员用户名 (administrator)；对于 *Administrator password* 区，必须使用超级管理员的当前密码。默认为 *password*，但其也许已被改为其它值。

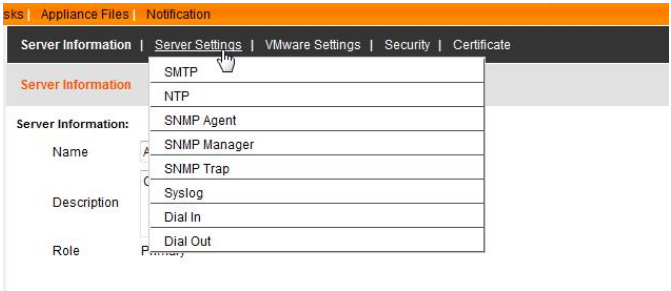
2. 注册后，以前独立 CC2000 (主或从)上的大多数原始数据丢失。作为从服务器，其现在将从注册的主服务器获得几乎所有数据。连接新注册的从的所有设备必须再次添加。关于添加设备的详细说明，见第 92 页的*添加设备*。

3. 登录设备中其它 CC2000 服务器的用户不能立即看到您的 CC2000。如果如果他们在系统管理选项卡，直到他们离开系统管理选项卡并再次回到此选项卡时，才能看到您的 CC2000。

4. 在某些情况下，您可能不得不清除您的浏览器缓存以便看到修改。

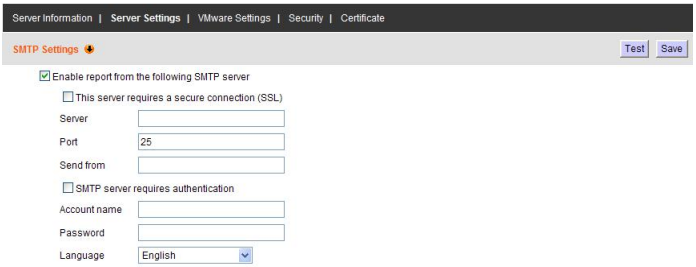
服务器设置

服务器设置的面板选单项目，只显示主服务器，包括若干次级页面。如要变更这些页面的信息，您可以点击灰色栏中主面板左侧的箭头图标，或者可以把鼠标停在选单上，在弹出的选单中选择页面直接跳到某一页面。



SMTP

CC2000可以把架构中发生的日志陷阱的邮件通知发送给指定用户。



注意：事件通知接受者需要在*Notification Settings*（通知设置）页面中指定。详见第216页。

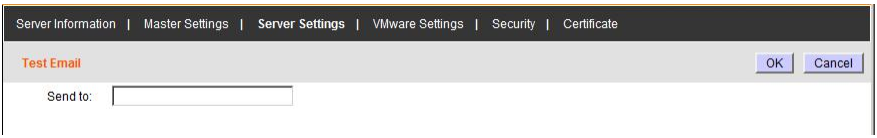
如要开启SMTP服务器设置，请按下述操作：

1. 勾选*Enable report from the following SMTP server*（允许如下SMTP服务器的报告）选框。
2. 在*Server*（服务器）字段指定运行SMTP服务器IP的电脑的地址或域名。
3. 指定SMTP服务器接收的端口编号。

4. 指定SMTP服务器接收的端口编号。

注意：此字段不能为空。

5. 如果SMTP服务器需要认证，请勾选*SMTP server requires authentication*（SMTP服务器需要认证）选框，然后在适当的字段指定认证账户名称和密码。
6. 在*Language*（语言）字段，从下拉选单中指定电子邮件通知语言。
7. 点击**Test**（测试），检查SMTP服务器的设置是否配置正确。如下图所示的页面将会出现：



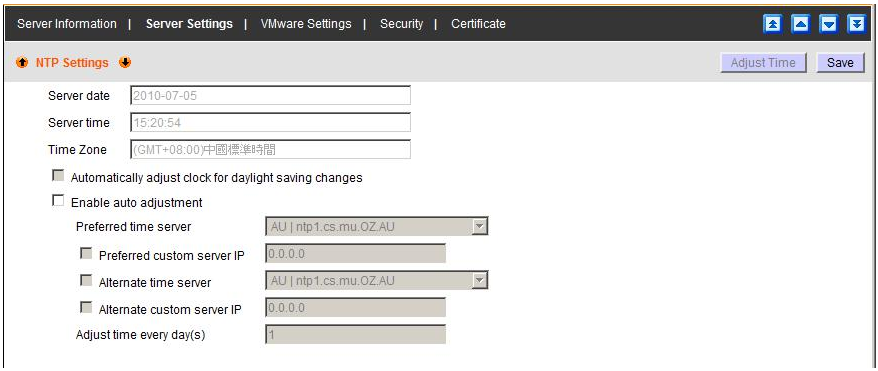
8. 输入测试邮件接收的邮件地址并点击**OK**。如果设置正确，接收人会受到测试邮件。

注意：接收人的邮件地址不能超过128个英语字母符号。

9. 点击**Save**（保存）完成步骤。

NTP

NTP页面可以使CC2000的时间自动与网络时间服务器同步：



注意：1. 如果最上面的三个字段由CC2000自动填充，则不可编辑。

2. 如果您所在的失去没有夏令时，则不要勾选*Automatically adjust clock for daylight savings time*（自动调整夏令时）选框。

如要使CC2000的时间自动与网络时间服务器同步，按下述操作：

1. 勾选开启自动调账选框。
2. 下拉时间服务器列表，选择您想用的时间服务器

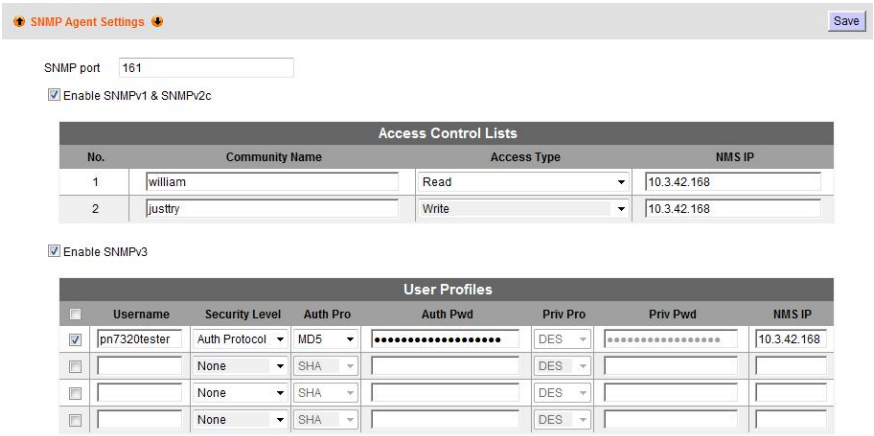
   - 或 -

   勾选想采用的定制服务器IP选框，输入您选择的时间服务器IP地址。
3. 如果您向设定一个备选时间服务器，勾选*Alternate time server* （备选时间服务器）选框，重复步骤2设定备选时间服务器。
4. 输入同步步骤之间的间隔天数。

若您向立即同步，点击**Adjust Time Now**（现在调整时间）。

SNMP代理

SNMP代理页可以设置CC2000的代理，以及访问控制SNMP陷阱事件，如下详述：



设置代理请按下述操作：

1. 在*SNMP Port*（SNMP端口）字段，输入能够收集陷阱事件信息的代理电脑的端口名称。有效的端口范围为1-65535。默认端口为161。

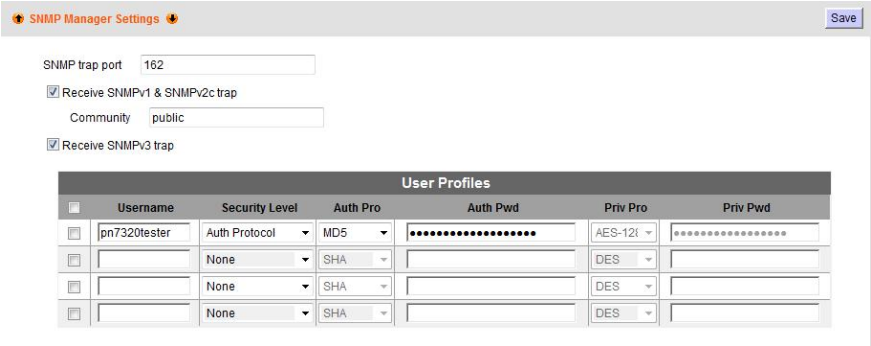
   注意：请确保在这里指定的端口号与SNMP管理器使用的端口号相配。

2. SNMP版本1和2，勾选*Enable SNMPv1 and SNMPv2c.Trap*（开启SNMPv1和SNMPv2陷阱）。
3. 在**Access Control Lists**（访问控制列表）表格中，输入社区名称和NMS IP地址，并从下拉选单中选择访问类型（读/写/禁用）。
4. SNMP版本3，单击启用*SNMPv3*。
5. 在**User Profiles**用户配置文件表格中，输入*用户名* 并选择一个*安全级别*（Auth Protocol / Authentication & Privacy / None）
6. 选择认证/隐私协议，输入与各配置文件相对应的认证/隐私密码和NMS IP地址。
7. 单击**Save**（保存）保存设置。

SNMP管理器

SNMP管理器页可以设置CC2000管理站，发送请求/接收SNMP陷阱事件通知，详情如下：

注意：最多可指定四个管理站。详见第173页，*SNMP陷阱* 。



如要设置管理器，按下述操作：

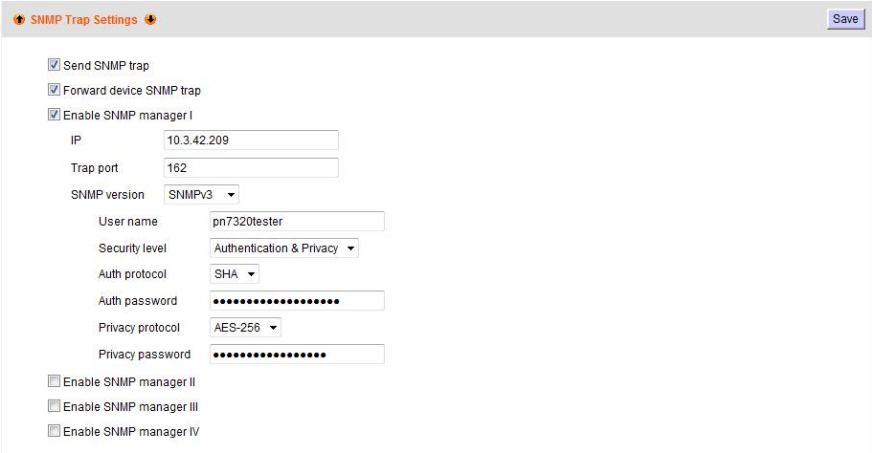
1. 在*SNMP Trap*（SNMP陷阱）字段，输入能够收集陷阱事件信息的代理电脑的端口名称。有效的端口范围为1-65535。默认端口为162。

   注意：请确保在这里指定的端口号与SNMP管理器使用的端口号相配。

2. SNMP版本1和2，勾选*Enable SNMPv1 and SNMPv2c.Trap* （开启SNMPv1和SNMPv2陷阱）。
3. 在**Access Control Lists**（访问控制列表）表格中，输入社区名称和NMS IP地址，并从下拉选单中选择访问类型（读/写/禁用）。
4. SNMP版本3，单击启用*SNMPv3* 。
5. 在**User Profiles**用户配置文件表格中，输入*用户名* 并选择一个*安全级别*（Auth Protocol / Authentication & Privacy / None）
6. 选择认证/隐私协议，输入与各配置文件相对应的认证/隐私密码和NMS IP地址。
7. 单击**Save**（保存）保存设置。

SNMP陷阱

SNMP陷阱页可以设置您的主SNMP陷阱设置，包括高达四个SNMP管理器的信息，如下：



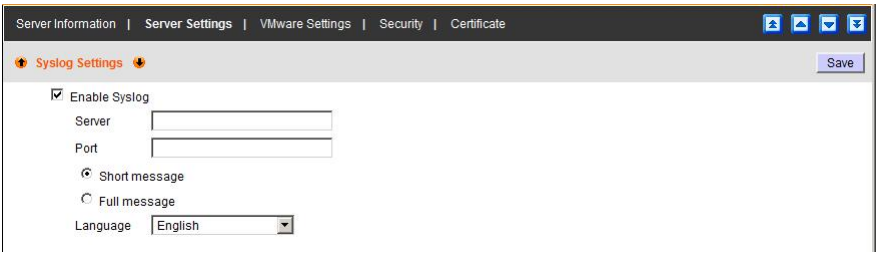
如要使用SNMP陷阱通知，按下述操作：

1. 勾选*Send SNMP Trap*（发送SNMP陷阱）。
2. 如果想把陷阱信息发送到某一设备，勾选*Forward Device SNMP trap*（抄送设备SNMP陷阱）。
3. 勾选*Enable SNMP manager I*（启用SNMP管理器1）进行第一次管理器配置。
4. 输入接收SNMP陷阱事件通知的管理器电脑的IP地址和服务端口编号。有效的端口范围为1-65535。默认端口为162。

   注意：请确保在这里指定的端口号与SNMP管理器使用的端口号相配。

5. 如果SNMP版本需要，输入社区值。
6. 选择协议并输入与每站对应的认证/隐私密码。
7. 重复步骤3-6，最多可再设置三个SNMP管理器。
8. 单击**Save**（保存）保存设置。

系统日志



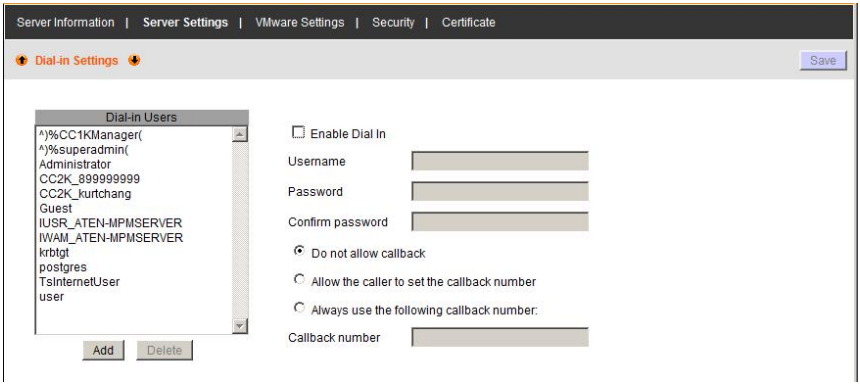
如要在系统日志服务器记录所有发生在CC2000的事件，按下述操作：

1. 勾选**Enable**。
2. 输入系统日志服务器的IP地址和端口编号，有效的端口范围是1-65535。
3. 选择短信息或完整信息。
4. 下拉选单选择信息语言。

完成所有设置后，单击**Save**（保存）。

拨入

除了互联网连接，CC2000也可以通过PPP（调制解调器）访问。拨入设置页用于指定哪些用户可以使用此功能，以及它们可以用来连接的方法。当您选择拨入时，类似于下面的一个页面将会出现：



如要允许PPP拨号连接，按下述操作：

1. 勾选*Enable Dial In* 复选框。
2. 提供用户拨号必须使用的用户名和密码，以便在拨号上进行身份验证。

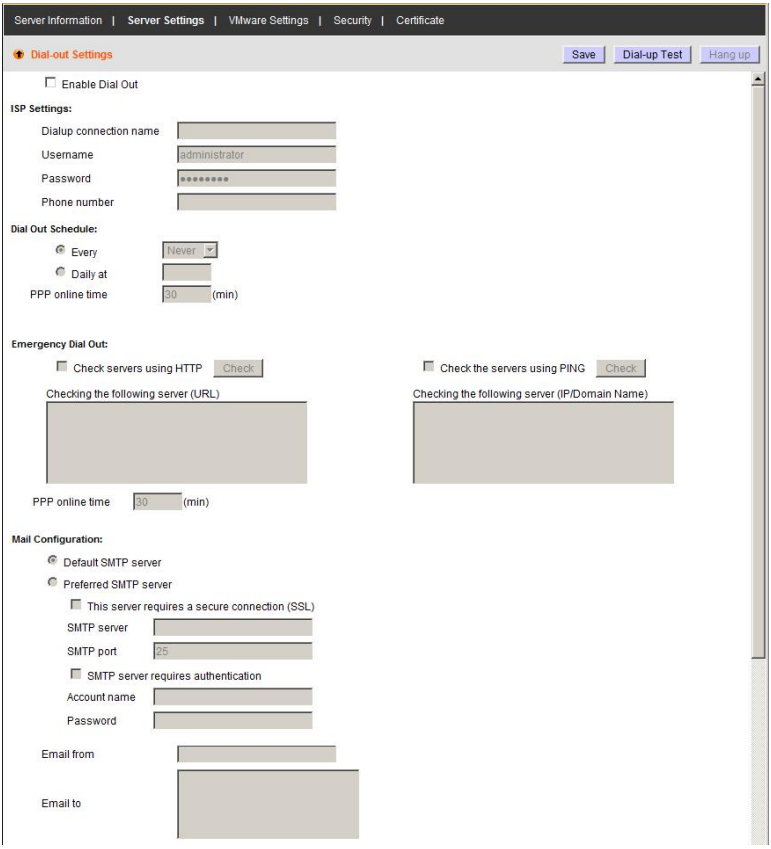
作为附加的安全措施，如果回拨功能启用，切换器会断开拨入连接，并且回拨到一个固定号码或弹性号码，如下表所述：

项目	操作
Enable Fixed Number DialBack 开启固定号码回拨	如果选择此单选按钮，则切换器将回拨 *Dial back number*（回拨号码）字段中指定的电话号码的调制解调器。在此字段输入希望 CC2000 回拨的号码。 **注意：**即使您想使用弹性回拨，也需要在此处指定一个号码。
Enable Flexible Dial Back 开启弹性回拨（使用电话号码作为用户名）	为了弹性和方便，如果选中此单选按钮，CC2000 回拨的调制解调器不一定是固定的。它可以回拨到任何方便用户的调制解调器。在拨入 CC2000 时： ◆ 登入时，使用您希望切换器回拨的调制解调器的电话号码作为用户名。 ◆ 使用回拨号码栏中指定的电话号码（见上文）作为您的密码。

拨出

对于拨出功能，您必须建立ISP（互联网服务提供者）的账户，然后使用调制解调器拨号到您的ISP帐户。如果您希望能够拨出，勾选*Enable Dial Out* 激活拨出功能。

注意：如果没有启用此功能，您只能拨入。拨出功能（下文所述）不可使用。



回拨页面上的项目的解释见下表：

项目	操作
ISP Setting ISP 设置	1. 为拨出连接提供一个名称（可选）。 2. 指定连接到您的ISP需要用到的电话号码、账户名（用户名）和密码。
Dial Out Schedule 拨出排程	设置您希望 CC2000 通过 ISP 连接拨出的次数。 ◆ *Every* 提供固定的次数李彪：永不、每小时和每两小时。 ◆ 例如，如果您选择 Every two hours 每两小时，CC2000 将在每两小时开始下一个整点开始拨出（如果现在是 13:10，它将在 14:00 启动拨号）。 ◆ 如果您不希望 CC2000 按照固定时间表拨出，从列表中选择 **Never** 永不。 ◆ Daily at 表示在一个指定的时间内每天拨一次。使用 hh:mm 格式（冒号前或后没有空格）。例如: 09:18 CC2000 会在您指定的时间每天拨出。 ◆ *PPP online time* 指定在终止会话和挂断调制解调器前要 ISP 连接要持续多久。设置为 0 表示一直联机。 ◆
Emergency Dial Out 紧急拨出	如果 CC2000 与网络断开连接，或网络出现故障，此功能可将切换器通过 ISP 拨号连接联机。 ◆ 如果您设定了 *PPP online time* ，与 ISP 的连接会再指定时间后自动终止。设置为 0 表示不会自动终止，一直保持联机，直到您手动终止连接（使用 *Hang Up* 按钮（在面板的顶部右侧））。 ◆ 您可以通过选择“*Check Server* 检查服务器”单选按钮来检查连接是否有效；输入适当的信息；然后单击“**Check** 检查”按钮。CC2000 会通知您结果。

项目	操作
Mail Configuration 邮件配置	这部分提供了对连接到CC2000端口的设备出现的问题的电子邮件通知。 ◆ 使用您设置为CC2000的SMTP服务器选择为*默认SMTP服务器*（见第168页，*SMTP*）。 ◆ 如果您想使用不同的SMTP服务器进行拨出，选择*Preferred SMTP server* 单选按钮。 ◆ 如果服务器需要安全连接，勾选*This server requires a secure connection (SSL)* 复选框。 ◆ 在*SMTP Server* 字段输入SMTP服务器的IP地址或域名。 ◆ 在*SMTP Port字段* 服务器监听的SMTP端口的编号。 ◆ 如果服务器要求身份验证，勾选*My server requires authentication* 复选框，然后在字段中输入正确的用户名和密码。 ◆ 在*Email From* 字段输入SMTP服务器负责人的电子邮件地址（或其他同样管理员），从现场的电子邮件。 ◆ 在*Email To* 字段输入您希望接收报告的电子邮件地址。如果您要将报告发送到多个电子邮件地址，用逗号或分号分隔地址。

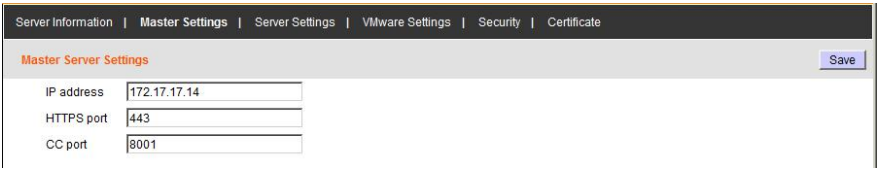
操作按钮的解释说明（面板右上角），在下面的表格中给出：

Save 保存	完成此页设置后，单击**Save**（保存）。
Dial Out Test 拨出测试	单击此按钮使 CC2000 拨出，以便查看是否成功连接 ISP。
Hang Up 挂断	单击此按钮强制 CC2000 调制解调器挂断。

主设置

此选单项仅出现在次级CC2000服务器中。它在以下条件下使用：

- 主IP地址变更。
- 主CC端口或HTTPS端口变化时次级设备脱机。
- 不同的CC2000从次级升为主级时次级设备脱机。



当这些情况发生时，没有必要再经历*注册* 过程（见167页 *注册*）以保持主/次连接。

管理员可以使用此页来相应地更新信息。

要保持连接，只需要输入新的IP地址和/或端口设置，然后单击“**Save**保存”。

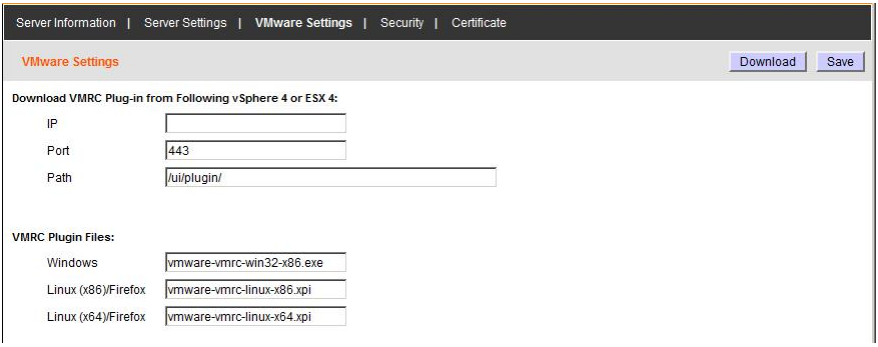
注意：1. 因为IP地址的变化是在操作系统级别下完成的（非2000服务级别），CC2000系统并不知道该变化。因此，主级无法自动变更次级信息。必须手动完成所有次级。

2. 任何脱机的CC2000次级设备都不能在发生变化时自动接收通知，因此这一过程必须在次级设备重新联机后完成。

3. 此过程允许在次级设备与主级设备无通讯时数据库的变更，合并到一个公共数据库。这适合最初为系统一部分但暂时无法通讯的CC2000，如果次级设备要重新在主级注册，它将失去分离时添加的任何数据库信息，并采取主级数据库的信息。

VMware设置

虚拟机远程控制台（VMRC）插件可以让您在浏览器中访问VMware虚拟机*。如果您在您的CC2000管理系统添加了VMware虚拟机，则需要安装这个插件。当您选择VMware的设置面板的选单条目时，类似于下面的一个页面将会出现：



如要安装插件，请执行如下：

1. 输入IP地址和vSphere 4或ESX 4插件文件库的端口号。（默认端口号为443。）
2. 输入要保存的插件文件的CC2000服务器的目录。
3. 单击**Download**。

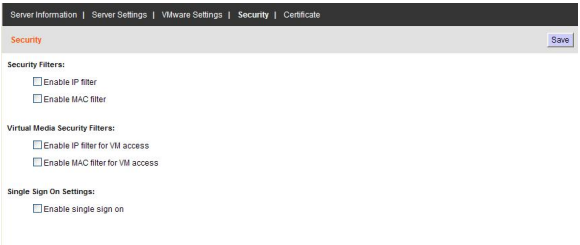
   在插件完成下载后，它将出现在相应的VMRC插件文件字段。

完成此页后，单击**Save**。

注意：虽然CC2000支持VMware 5.x（vCenter 5.x, ESX Server 5.x），但由于VMware 5.x软件的有所变更，CC2000不支持从上图中*VMware Settings*（VMware设置）页面下载的VMware 5.x的插件为。如要使用在VMware 5.x上使用VMRC插件为，从VMware的网站下载并复制文件(VMware-VMRC.i386.bundle, VMware-VMRC.x86_64.bundle, vmware-vmrcwin32-x86.exe)到CC2000服务器目录: “*CC2000\Web\webapps\ui\plugin\VMware5.x*”。

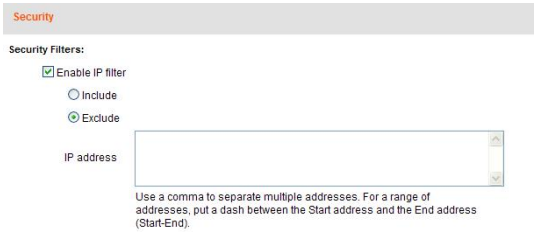
安全性

此页面通过控制对CC2000的访问提供安全级别。



IP筛选

IP筛选根据试图连接的计算机的IP地址控制对CC2000的访问。



- 如要开启IP筛选，勾选Enable IP Filter 复选框。
  - 如果选择了*Include* 按钮，则在地址列表中指定的所有地址都允许访问；所有其他地址都被拒绝访问。
  - 如果选择了*Exclude* 按钮，则在地址列表中指定的所有地址都被拒绝访问；所有其他地址都允许访问。
- IP筛选器可以由一个单一地址或某一范围的地址组成。您可以根据需要添加多个IP地址。将地址直接输入在*IP address* 文本输入框,如下：
  - 对于多个单地址条目，在IP地址之间使用一个逗号。逗号前后没有空格。
  - 对于某一范围的筛选，输入起始IP地址，输入破折号，然后输入结束IP地址。
- 如要修改或删除筛选器，请在*IP address* 文本输入框中直接更改。

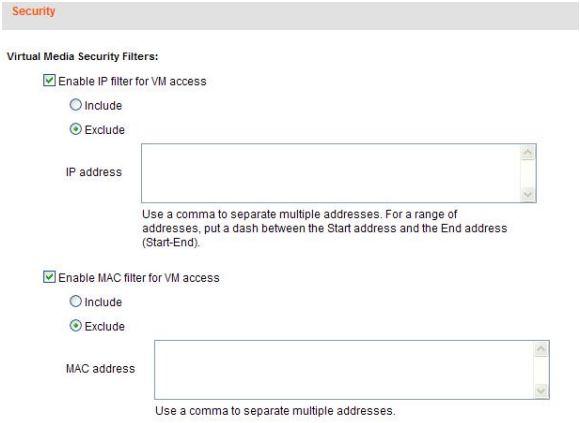
MAC筛选

MAC筛选根据试图连接的计算机的MAC地址控制对CC2000的访问。

- 如要开启MAC筛选，勾选*Enable MAC Filter* 复选框。
  - 如果*MAC at CC2000 login* 启用，当用户试图登入时，CC2000将验证客户PC的MAC地址。否则，地址将只会在试图打开浏览器时被验证。
  - 如果开启了*Include* 按钮，则在地址列表中指定的所有地址都允许访问；所有其他地址都被拒绝访问。
  - 如果选择了*Exclude* 按钮，则在地址列表中指定的所有地址都被拒绝访问；所有其他地址都允许访问。

虚拟媒体安全筛选器

根据试图使用虚拟媒体访问的计算机的IP和MAC地址，IP和MAC过滤也可以用来控制虚拟媒体访问。



- 如要开启虚拟媒体安全筛选器，勾选*Enable IP filter for VM Access* 以及*Enable MAC filter for VM access* 复选框，并根据181页*IP筛选* 和182页*MAC筛选* 的指示完成步骤。

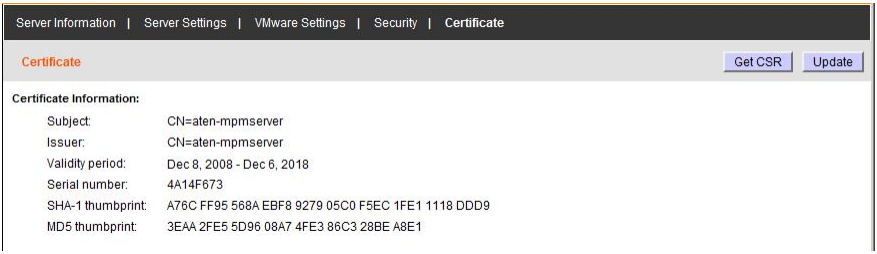
单点登入

如果*单点登录* 启用，通过CC2000认证的用户将在所有系统设备下自动得到验证。他们不必单独在每个设备上进行身份验证。

证书

当通过安全连接（SSL）登入时，签发证书是用来验证用户登入的是他想要访问的网站。*证书* 页用于创建、修改或获得用于此目的的证书。

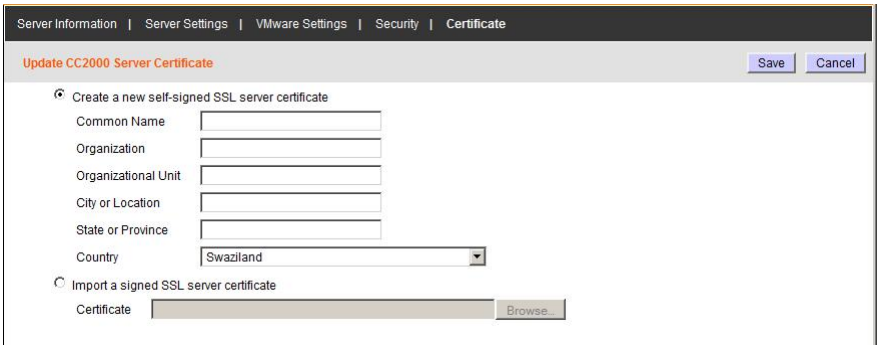
在安装过程中，每一个CC2000都会在类似下图的安装信息页面创建自己的、独立的、自署签名的证书：



更改自签名证书

更改自签名的证书允许您在没有在安装证书中生成的证书中提供额外的信息。改变自签名的SSL证书的方法是新建。要创建一个新的自签名证书，操作以下：

1. 在证书面板的顶部右侧，单击“**Update**更新”。出现以下页面：



2. 选择*Create a new self signed SSL server certificate* 单选按钮，然后根据下表中的信息填写：

字段	描述
Common Name 常用名	此为您所请求的SSL证书的全称域名（FQDN）。 例如: www.yourdomainname.com
Organization 组织	此为您在所在地合法注册的完整法人公司或法人名称。
Organizational Unit 组织单元	需要此证书的公司分支。 如：会计、市场等等。
City or Location 城市或位置	输入完整的城市或位置名。 例如：台北。
State of Province 州或省	输入完整的州名或省份名。
Country 国家	此为组织证书注册地所属国家的代码。 **注意：**这些并不总是对应于常用的缩写词。如果您不确定代码，您可以在线搜索**SSL+国家代码**。

3. 填完字段后，点击**Save**（保存）。

将出现一条消息请您等待数据库更新新的信息。之后网页关闭。

此时您将返回到登入步骤的开始，您必须通过接受安全证书和登入的过程。

导入签名的SSL服务器证书

为了避免用户在每次登入时都要经过证书接受提示，管理员可以选择使用第三方证书授权（CA）签署的证书。

如要使用第三方签字证书，操作如下：

1. 在生成自签名证书后，单击面板右上角的**Get CSR**（证书签名请求）。（见第184页的截图。）
2. 前往您选择的CA网站，使用步骤1生成的证书申请SSL证书。
3. 在CA发送证书后，打开*Server Certificate* “服务器证书”页，单击面板右上角的**Update** “更新”按钮。
4. 选择**Import a signed SSL server certificate**；然后浏览证书文件所在位置并选择。
5. 单击面板右上方的**Save**“保存”。

注意：在本节中提到的证书类型提供同等级别的安全性。更改的自签名证书的优点是它允许您提供更多的信息，而不仅是安装证书。CA第三方证书的优点是，用户不必通过证书接受提示，每次登入时，它提供额外的保证，识别的授权已证明该证书是有效的。

许可证

CC2000许可控制CC2000服务器安装架构允许的节点数量。购买时所带的默认许可证是主级的演示许可证（无次级），允许16个节点。要添加更多的（次要服务器和节点），您必须升级许可证。

当您从系统管理选单中选择*License* “许可证”时，一个类似于下图的页面出现：

此页项目的含义在下面的表格中描述：

项目	描述
Key serial number 密钥序列号	许可密钥的序列号。 **注意**：与您安装CC2000服务器时的软件序列号不同。在密钥上可以找到许可证序列号。
Secondaries 次级	安装的次级设备的总数（高达 31 台 - 取决于许可证购买）。
Nodes 节点	根据许可证购买，架构允许的节点总数。 注意：可以被授权的节点的数量是无限的 - 它取决于许可证购买。
Available Nodes 可用节点	您的许可证所允许的未使用的仍然可用于部署的节点数量。

更新许可证

如要更新许可证：

1. 请联系您的经销商以获得您想要访问的次级设备和节点数量的许可证密钥。
2. 将许可证密钥插到主服务器上的USB端口。
3. 在主面板的右上角单击**Upgrade**“升级”。

注意：1. 一旦升级完成，就不再需要把密钥插入USB端口。移除密钥并将它放置在安全的地方，可能需要它在将来进行更新。

2. 如果USB密钥丢失，请联系您的经销商重新获取。如果您提供密钥的序列号，新的密钥将包含存储在丢失的密钥上的所有信息。

许可证共享

在CC2000架构中授权设备的许可证数量，是通过许可证密钥在主服务器上设置的，并在所有的CC2000服务器之间共享。有关许可证的数量的信息被发送到每台在主服务器上注册的次级服务器（详见第167页，*注册*）。

虽然有可以添加到CC2000管理系统的设备数目没有限制，只有与节点数目相同的许可证数量可以创建管理（详见第86页，*初审程序*）。

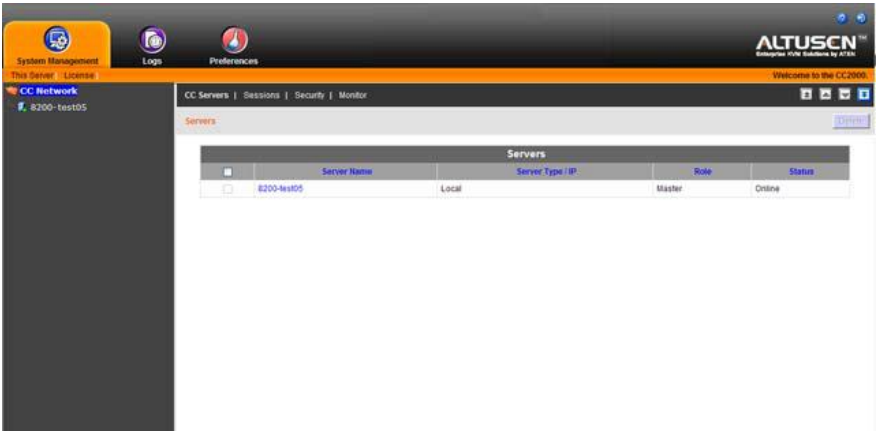
当设备被添加到CC2000管理系统，默认配置为锁定。虽然它们的配置信息是由CC2000保存的，但是无法管理。

锁定端口可以解锁，可以通过选择一个物理端口并点击**Unlock**解锁按钮解锁（见121页，*锁定/解锁端口*），也可通过使端口成为整合设备的一部分解锁（见100页，*添加整合设备*）。

如果所有的许可证都在使用，只有当一个当前解锁的端口被锁定，或整合设备被删除时－从而释放了正在使用的许可证－锁定端口（或新的整合设备）可以使用CC2000管理系统所管理的解锁许可证。

许可证冲突

如果在同一网段上有两台主服务器通过同一许可密钥进行升级，则会发生许可证冲突。第二个安装的CC2000服务器的浏览器GUI，将打开如下图页面：



要确认冲突已发生，请单击**Logs**“日志”选项卡。如下语句将出现在日志文件中：*A license violation has been detected at Primary server. Remote CC server (IP: [the conflicting servers' IP])*。

如果发生这种情况，有多种方法可以解决冲突：

1. 对两台主服务器之一：关机，或停止服务，或断开网络，或卸载CC2000。
2. 注册冲突的CC2000（第二台）与正常服务器（第一台）。注册的CC2000成为次级。（此为假定有可用的次级许可证。）
3. 如果您确实希望有两台独立的CC2000架构，请联系您的经销商为其中一台CC2000服务器购买单独的密钥。

任务

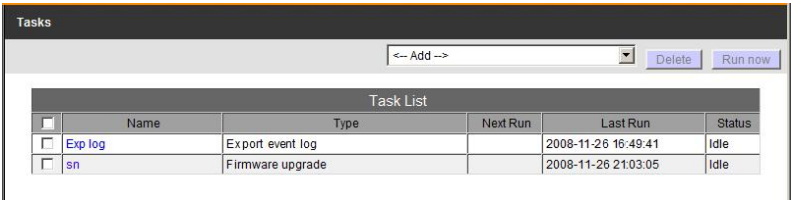
任务选单允许授权管理员执行多个系统维护任务。可以执行的任务由用户类型确定，授权选择在创建用户帐户时选取。包括：

- 备份主服务器数据库

  注意：1. 此任务只适用于主级CC2000

  2. 恢复数据库需要单独的工具和程序。详见第261恢复，*恢复* 。
- 到处时间日志
- 开启控制服务器
- 更新所选设备的固件
- 备份设备配置文件和账户信息
- 到处设备日志
- 到处会话历史

当您在主级CC2000上打开任务页面时，会出现出现如下画面：



注意：这个图像描绘了主服务器的页面。次级服务器的页面是相似的，除了次级有一个预先配置的默认输入，*Replicate Database* （复制数据库），可以复制其连接的主级数据库（见第205页，*复制数据库* ）。

Task List 任务列表表格列出了已配置的所有任务。标题的含义在下面的表格中解释：

标题	说明
Name 名称	配置时赋予的任务名称。
Type 类型	任务类型。
Next Run 下一个运行	如果任务计划被列入时间表，其运行时间将出现在这里。
Last Run 上次运行	表示任务上次运行的时间。
Status 状态	表示任务正在运行或者闲置。

添加任务

如要添加任务，执行如下：

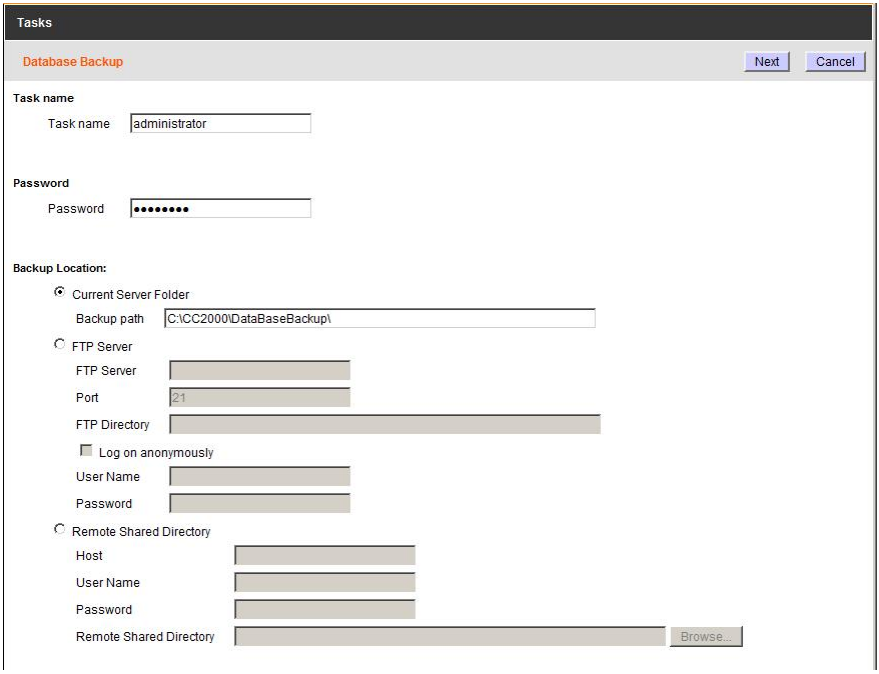
1. 单击*Add*“添加”字段右边的箭头，下拉任务选项列表：

2. 单击想要添加的任务。

根据您所选择的任务，一个有各种各样选择页面将会出现。虽然每一项任务是不同的，大部分的设置程序都是相似的。下面的示例将向您展示您可能遇到的各种任务程序。

备份主级服务器数据库

当您选择*Backup the Primary server database* （备份主服务器数据库）时，将出现以下页面：



1. 输入任务名称，并输入密码。

注意： 1. 此任务只在主服务器可用。

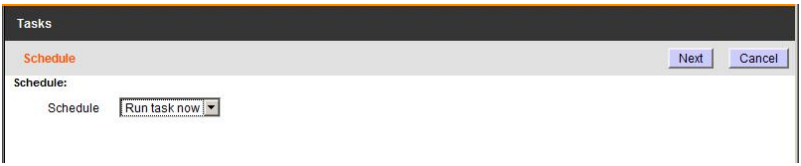
2. 密码是可选的。如果您设置了密码，请记下来并放在一个安全的地方。当恢复数据库时，您将需要它。（如果您没有设置密码，无需密码也可恢复数据库） 详见第261页，*恢复*，了解更多恢复数据库的信息。

3. 密码不能超过8个英文字符。

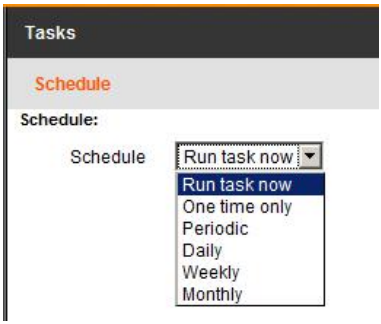
4. 备份文件格式为cbk (*.cbk)。

2.选择要存储备份文件的位置，并相应地填写。默认设置为备份文件被存储在与CC2000相同的本地目录。例如，`C:\CC2000\DataBaseBackup`。

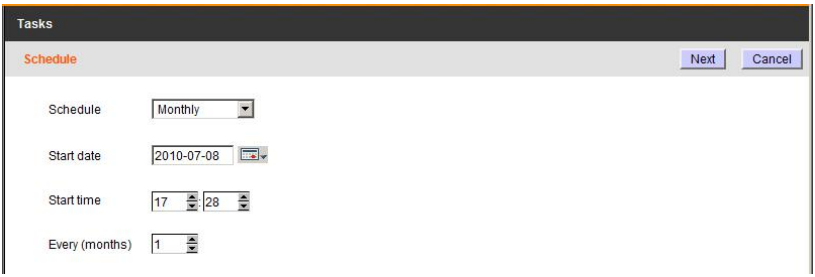
3. 当您已填写了所要的信息时，请单击**Next** “下一步”。将出现 *Schedule*“时间表”页面：



4. 下拉选单查看可用选项。

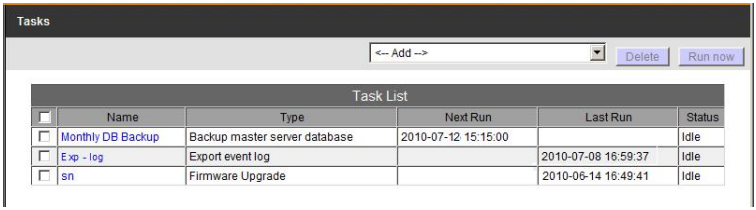


根据您的选择，进一步的时间表选择可能会出现。例如，如果您选择*Monthly* ，将出现一个页面，让您设置每月的时间表：



注意：如果您在备份的时间表中设置了时间（例如每月），但您希望它从这个月开始，请确保您将设置的开始日期或时间比页面上显示的日期或时间晚。由于页面上的时间设置显示了您访问该页面的时间，它可能已经超过了您保存更改的时间通过。这表示下个月之前CC2000不会执行任务。

5. 当您完成了您的日程安排选择时，请单击**Next** “下一步”。任务现在被添加到了主页上的任务列表中。



注意：您可以通过勾选名称前的复选框并单击面板右上方的**Run Now**运行一个任务（或多个任务）。

导出事件日志

选择*Export event log* （导出时间日志），将出现如下页面：

1. 在Task name （任务名称）字段输入任务名称。

注意：*导出事件日志* 操作可在每个独立的服务器上执行。要搜索服务器的记录，您必须查看其特定的文件。您可以通过您给其*任务名称* 来识别这个文件。

2. 选择要存储的导出文件的位置，并相应地填写。默认设置为导出文件被存储在当前CC2000目录下：
`C:\CC2000\CC2000LogExport`。
3. 选择您希望包含在导出文件*Availabel* 可用栏的项目，然后单击**Add** “添加”，将其移动到*Selected* 所选列中。重复步骤添加其他您要包含的日志文件项目。

注意：如要选择多个项目，使用Shift+单击或Ctrl+单击。

4. 要更改*所选* 项目的顺序，请单击要移动的项目，然后单击“**Up**”或“**Down**”移动到想要的位置。
5. *选择导出期间* ，选择**All**所有将导出数据库中的所有记录。要导出特定时间段的记录，选择它下面的单选按钮，并在*From* 和*To* 中设置时间参数。
6. 对于*导出文件语言* ，选择**Default**默认，则导出文件的语言与浏览器相同。如果您想用不同的语言，下拉列表，选择提供的语言之一。
7. 对于*导出文件类型* ，请勾选您选择项目前的单选按钮。如果您选择加密选项之一（AES和DES），在出现的*Password* 字段输入密码。

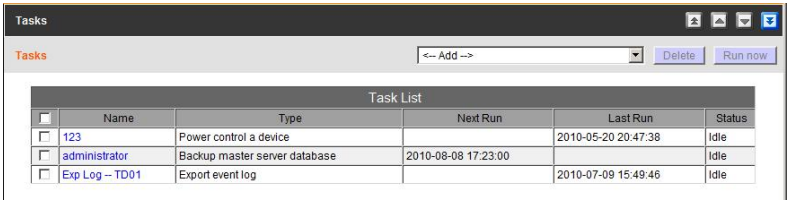
注意：记下密码 – 您将在导入文件时需要（详见第220页，*导入日志* ）。

8. 完成此页面后，单击**Next**“下一步”（面板右上方）以继续。
9. 在出现的页面中作出时间表选择。

注意：时间表选项与*备份主服务器数据库* 任务所描述的类似。如有必要，请参考193页的详细信息。

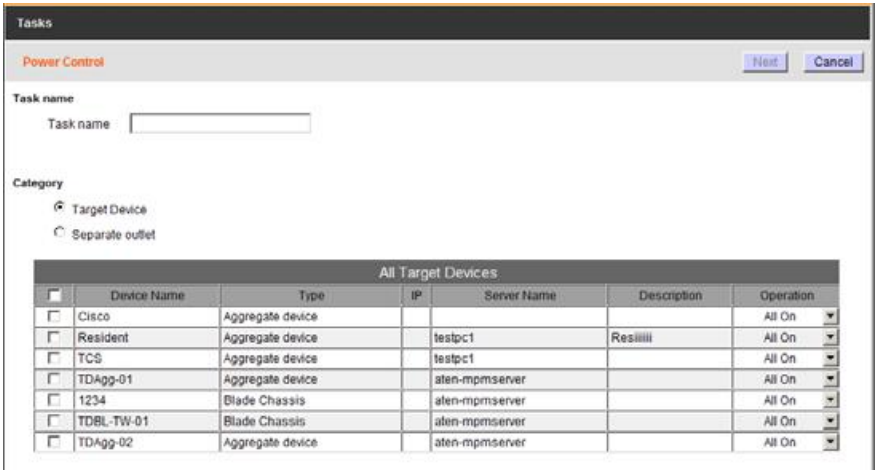
10. 完成时间表选择后，单击**Next**（下一步）。

程序完成后，您将返回到*任务* 主页。，根据您的选择设置的导出事件日志任务现在已经被添加到侧边栏和任务列表：



电源控制设备

此任务允许您设置时间表，自动整体或在端对端基础上开关所选设备的电源端口。当您选择此任务时，将出现“电源控制”页面，以及已经选中的*目标设备* 类别：



如果您更倾向于在单个端口基础上执行任务，请选择*Outlets*（插座）类别。

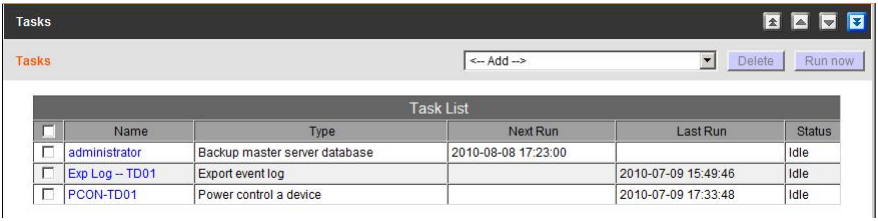
1. 为任务设置名称。
2. 勾选目标设备或者您希望控制的设备，或者在勾选列上方的复选框选中全部。
3. 选择开启或者关闭*Operation* 操作栏。
4. 完成此页面后，单击**Next**（下一步）（面板右上方）以继续。

5. 在出现的*时间表* 页面作出时间表选择。

注意：时间表选项与*备份主服务器数据库* 任务所描述的类似。如有必要，请参考193页的详细信息。

6. 完成时间表选择后，单击**Next**（下一步）。

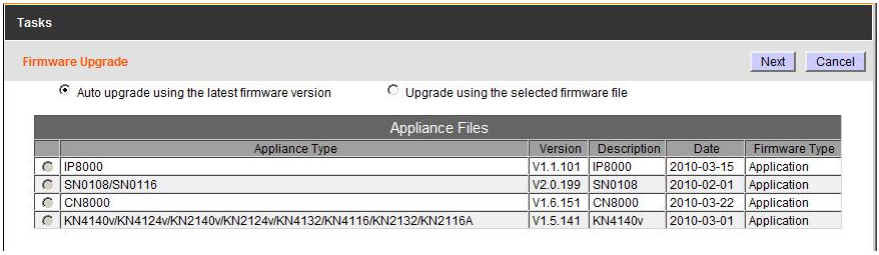
程序完成后，您将返回到任务主页。电源控制设备的任务，根据您的选择设置的*电源控制设备* 任务现已被添加到侧边栏和任务列表：



更新选中的设备固件

这项任务允许您安排架构中设备的固件更新，以使它们可以在最合适的时间进行更新。

选择*Upgrade Selected Appliance Firmware* 后，将出现如下页面：



如要安排选中设备的固件更新，执行如下：

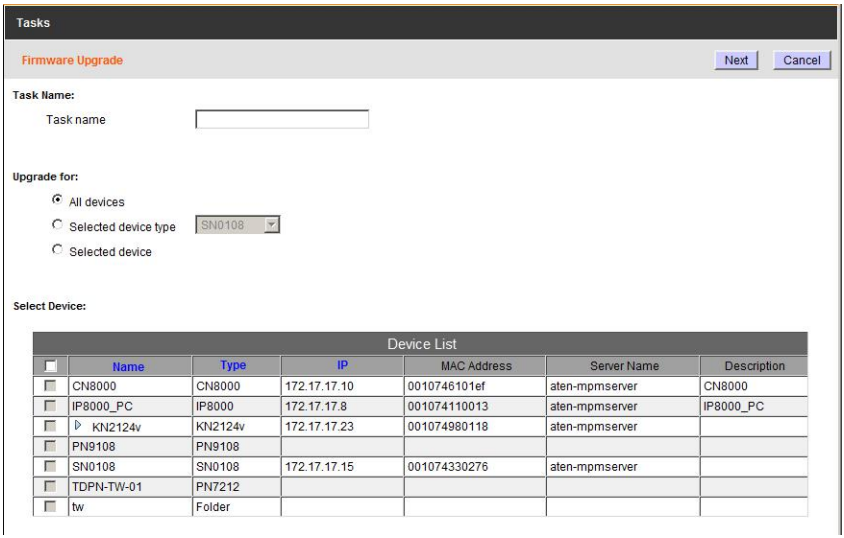
1. 单击单选按钮以选择是否使用保存在CC2000服务器上的最新的更新文件，或使用选中的上传文件进行更新。

注意：1. 和CC2000服务器保存在一起的文件，都是其硬件部分。这些通常为兼容CC2000的最新版本。我们建议使用它们，除非您有特定的原因选择特定的其他文件。

2. 如果您选择*Upgrade with a selected firmware file* 用选中的固件文件更新，更新之前，您必须先上传更新文件。详见第206页，*固件文件* 。

2. 如果您选择*Upgrade with the latest stored version* 使用最新的存储版本更新（推荐），所有的设备都会自动选择升级。如果您选择*Upgrade with a selected firmware file* 用选中的的固件文件更新，请单击要升级的设备类型前面的按钮。
3. 单击**Next**（下一步）（面板右上方）。

固件更新 页面出现：



4. 在*Task name* 字段输入适当的名称描述任务。

5. 单击单选按钮选择接收更新的设备。
6. 如果您选择*Selected Device Type* 选中的设备类型 ，下拉列表并选择设备类型。只有被选中设备类型的设备会接收更新。
7. 如果您选择*Selected device* 选中的设备，勾选您想升级设备前面的复选框（或勾选该列顶部复选框选择全部）。

注意：1. 对于KVM切换器适配器线缆，单击切换器名称前的箭头来选择您想升级的适配器线缆固件。

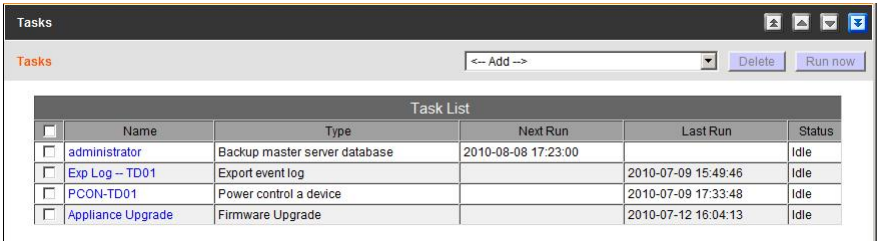
2. 设备列表根据名称、类型和IP分类。

8. 单击**Next**下一步。
9. 在出现的*时间表* 页面进行选择。

注意：时间表选项与*备份主服务器数据库* 任务所描述的类似。如有必要，请参考193页**步骤2**的详细信息。

10. 完成选择后，单击**Next**（下一步）。

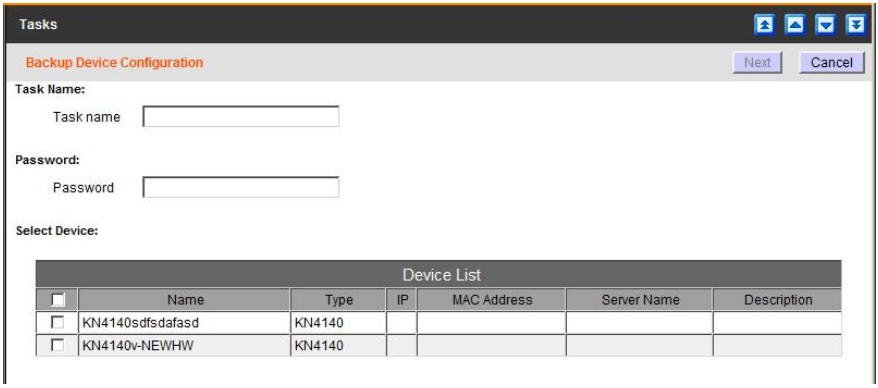
程序完成后，您将返回到*任务* 主页。此任务现已添加到侧边栏和任务列表：



Name	Type	Next Run	Last Run	Status
administrator	Backup master server database	2010-08-08 17:23:00		Idle
Exp Log -- TD01	Export event log		2010-07-09 15:49:46	Idle
PCON-TD01	Power control a device		2010-07-09 17:33:48	Idle
Appliance Upgrade	Firmware Upgrade		2010-07-12 16:04:13	Idle

备份设备配置/账户信息

当您选择*Backup device configuration/account information* 备份设备配置/帐户信息任务后，将出现以下页面：



1. 为任务设置用户名和密码。

注意：请记下密码并将其存放在安全的地方。当恢复配置/帐户信息时，您将需要它。详见第124页，*恢复设备配置* 。

2. 在*Device List*“设备列表”中，勾选要备份的设备名称前面的复选框，然后单击**Next**“下一步”。
3. 在出现的*时间表* 页面中进行选择。

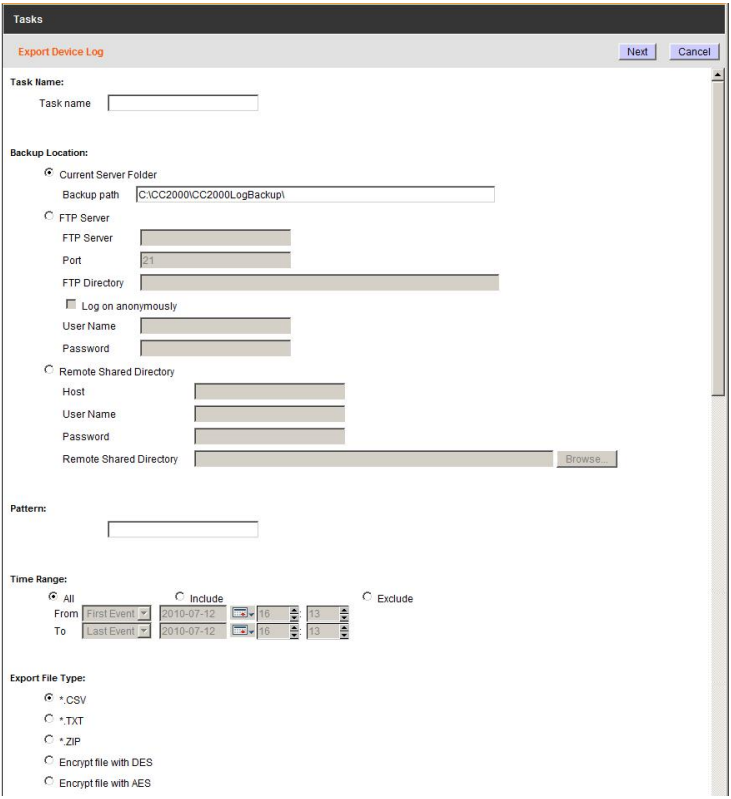
注意：时间表选项与*备份主服务器数据库* 任务所描述的类似。如有必要，请参考193页的详细信息。

4. 完成选择后，单击**Next**“下一步”。

程序完成后，您将返回到任务主页。根据您的选择设置的 *备份设备配置/账户信息*的任务现已被添加到侧边栏和任务列表：

导出设备日志

CC2000充当所有ATEN/Altusen NET™设备的日志服务器，记录数据库中设备发生的系统事件。此任务允许您将设备数据库的内容写入到文件中。当您选择导出设备日志任务时，将出现以下页面：



1. 为任务设置一个合适的名称。例如，如果您想导出所有设备的设备日志，您可以命名为*All-devicelog* ；如果您想导出CN8000设备的设备日志，可以命名为*cn8000-weekly-device-log*。

注意：*导出设备日志* 操作在每台服务器上独立执行，并独立保存在每台服务器上。如要搜索记录，必须在每天服务器上寻找各自文件。

2. 选择要存储导出文件的位置，并相应地填充字段。默认设置是文件被导出到CC2000服务器所在目录。

注意：保存备份文件的服务器目录的路径是在CC2000安装的目录上预先设置的。例如，C:\CC2000\CC2000logbackup。

3. 可以使用*Pattern* 字段作为筛选器来限制日志文件的范围。例如，导出文件只包含CN8000设备的事件信息，并且所有CN8000设备名称中包含*CN8K*，您将在Pattern字段输入CNK8。
4. 时间范围：
   - 选择**All**导出数据库中所有记录。
   - 如要导出某一时间段的记录，选择**Include**单选按钮，并在*From* 和*To* 中设置时间参数；如要导出全部记录而*不包含* 某时间段，选择Exclude 单选按钮并在*From* 和*To* 中设置不希望包含的时间参数。
5. 对于*导出文件类型* ，单击选项前的单选按钮。如果您选择加密选项之一（AES或DES），在*Password* 字段输入密码。

注意：记下密码 – 您将在导入文件时需要（详见第220页，*导入日志* ）。

6. 完成此页后，单击**Next**（面板右上方）以继续。
7. 在出现的页面中进行时间表选择。

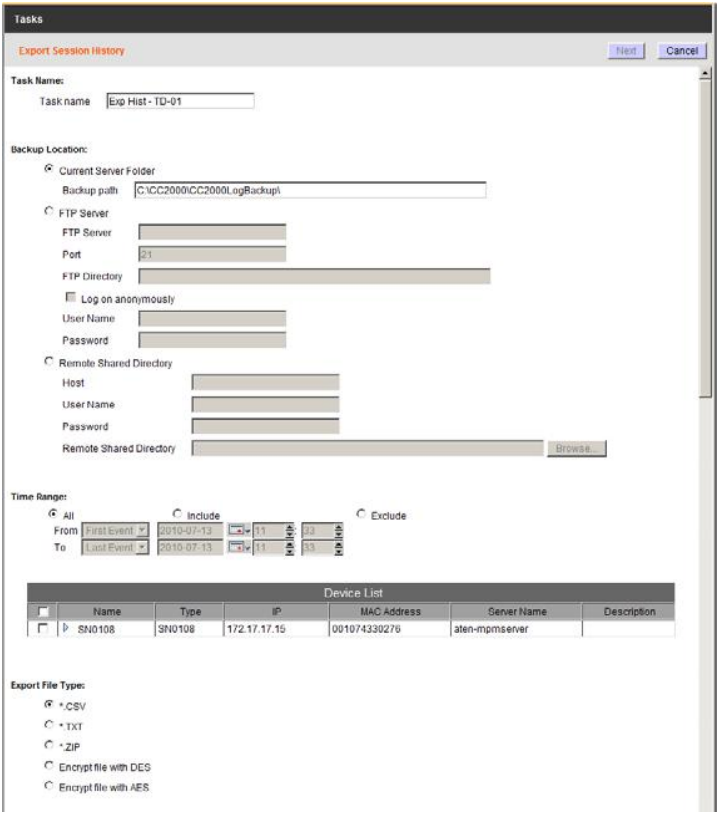
注意：时间表选项与*备份主服务器数据库* 任务所描述的类似。如有必要，请参考193页的详细信息。

8. 完成时间表选择后，单击**Next**（下一步）。

程序完成后，您将返回到*任务* 主页。根据您的选择设置的导出时间日志任务现已被添加到侧边栏和任务列表。

导出会话历史

CC2000保留所有发生的用户会话的记录（详见第225页，会话历史 ）。此功能允许您将每台设备和端口的会话保存为文件。选择*Export session history* 导出会话历史）人物后，如下页面出现：



1. 出设备列表外，此页面与导出设备日志相同。根据从201页开始的*导出设备日志*所给出的信息填充页面其余部分。
2. 对于设备列表，勾选您想要的设备前的复选框（或者勾选全列上方的复选框选择全部）。

   若您希望只导出选中端口的会话历史，不要单击设备复选框，单击设备名称前的箭头，展开端口列表选择端口。

3. 完成此页面后，单击**Next**“下一步”（面板右上方）以继续。
4. 在出现的页面中进行时间表选择。

注意：时间表选项与*备份主服务器数据库* 任务所描述的类似。如有必要，请参考193页的详细信息。

5. 完成时间表选择后，单击**Next**（下一步）。

程序完成后，您将返回到*任务* 主页。根据您的选择设置的导出事件日志任务现已被添加到侧边栏和任务列表。

编辑任务

可以执行两项编辑任务：改变任务时间表，改变任务执行的参数。

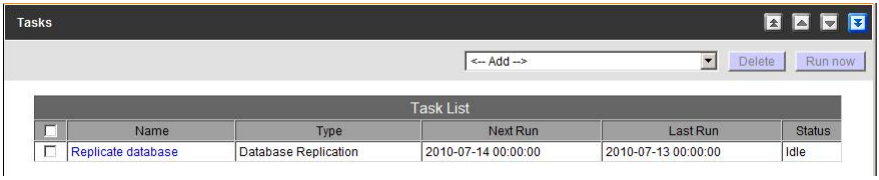
- 如要改变任务时间表，执行如下
  1. 单击名称 – 在侧边栏或任务列表。
  2. 出现*时间表* 页面。按照您的意愿进行变更，然后单击**Save**（保存）。
- 如要改变您想让任务执行的参数，执行如下：
  1. 单击名称 – 在侧边栏或任务列表。
  2. 出现*时间表* 页面。单击界面选单的**Task Properties**（任务属性）。
  3. 任务属性页面出现后，按照您的意愿进行变更，然后单击**Save**（保存）。

删除任务

如果不想执行某任务，勾选其名称前的复选框并单击界面右上方的**Delete**（删除）。

复制数据库

次级服务器的*Tasks* 任务页面与主级服务器类似（详见第190页），除了有预设的默认条目，*Replicate* （复制）。



当您选择*Replicate Database*（复制数据库）时，时间表页面出现。时间表选项与*备份主服务器数据库* 任务所描述的类似。如有必要，请参考193页的详细信息。

注意：1. 每台CC2000服务器拥有其自己的独立数据库，内含配置的账户、日志、设备和访问权限。通过复制，可以发送这些信息，并合并到主级服务器的数据库，并使CC2000管理系统剩下的内容生效。

2. 当次级服务器注册到主级服务器时，其数据库自动复制。

3. 默认为，数据库在00:00自动被复制。您可以使用此页面更改复制时间表，但是注意，把复制时间表的时间间隔设置得果断会对系统性能有不利影响。如果您设置的间隔过长，可能有较长时间数据库不匹配。

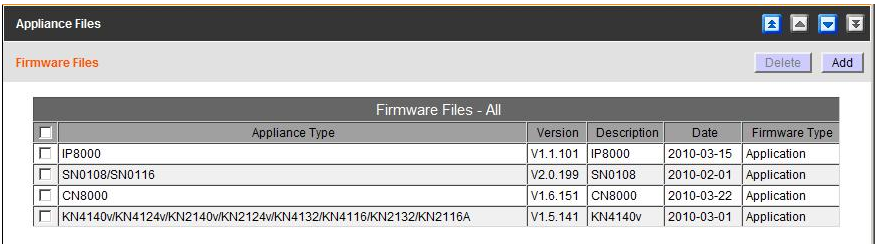
对时间表进行选择后，单击**Save**（保存）。

设备文件

Appliance Files（设备文件）选单用于另个目的：集中化固件管理，保存之前的备份配置文件。

固件文件

固件文件选单将打开*固件文件* 页面，如下面截图所示：



此页面列出了CC2000保存的所有固件更新文件 – 可供您浏览每一个的特定信息。通过把最新的固件更新文件用于此单一位置分布，您可以在CC2000中轻松执行更新，并保证架构中的所有设备在最新的固件版本上操作。

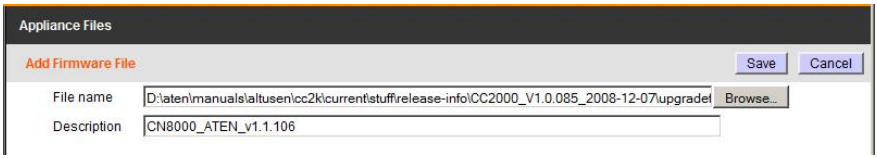
注意： 1. 固件更新在*Tasks*（任务）子选单下执行。详见第190页。

2. 新的固件更新安装包可用时会发布到网站上。请定期访问网站获得最新的安装包和相关信息。

添加固件文件

如要将固件文件添加到列表，执行如下：

1. 在界面右上方，单击Add（添加），弹出Add Firmware File（添加固件文件）页面：



2. 浏览您从我们网站下载后保存的更新文件的位置，选择合适的文件。

3. 对文件进行描述。

4. 单击**Save**（保存）（主界面右上方）完成程序，将固件文件添加到列表。

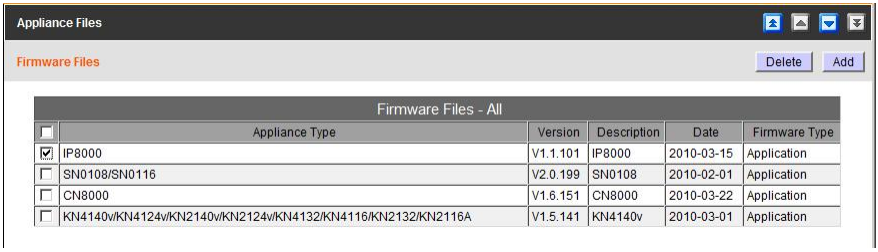
注意：如果固件文件不兼容CC2000（尽管兼容独立运行配置的设备），CC2000不允许加载。

删除固件文件

如要从列表删除固件文件，执行如下：

1. 从侧边栏选择**固件**。

2. 在交互式显示面板中，勾选您向从列表中删除的文件。



	Appliance Type	Version	Description	Date	Firmware Type
☑	IP8000	V1.1.101	IP8000	2010-03-15	Application
☐	SN0108/SN0116	V2.0.199	SN0108	2010-02-01	Application
☐	CN8000	V1.6.151	CN8000	2010-03-22	Application
☐	KN4140v/KN4124v/KN2140v/KN2124v/KN4132/KN4116/KN2132/KN2116A	V1.5.141	KN4140v	2010-03-01	Application

注意：您可以勾选多个文件将其删除，页可以勾选侧裂上方复选框删除全部。

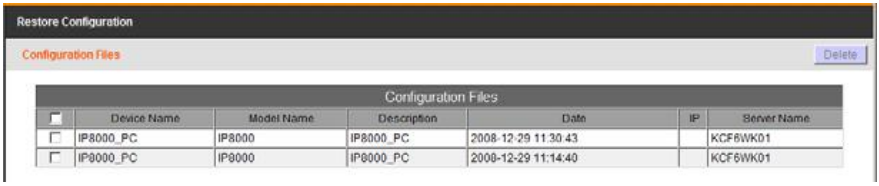
3. 完成选择后，单击界面右上角的**Delete**（删除）。

4. 在出现的信息弹窗中单击**OK**。

配置文件

删除配置文件

单击侧边栏的*Configuration*（配置）弹出*Configuration Files*（配置文件）页面，如下面截图所示：



此页面列出了*备份设备配置/账户信息* 任务中所设定的服务器备份设置（详见第200页），并允许您删除不想保留的文件。

如要删除设备的配置，执行如下：

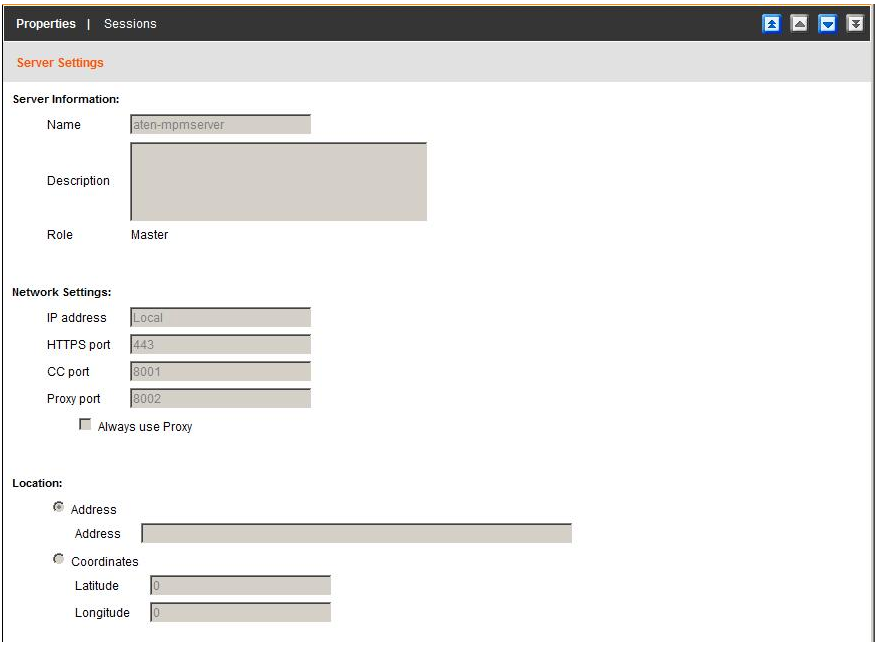
1. 勾选您想删除设置前方的复选框。
2. 单击**Delete**（删除）（界面右上方）。

侧边栏服务器树状图

当从选单栏选中*CC Network*（CC网络）后，单击服务器名称 – 在侧边栏或者交互式显示面板 – 将弹出一个页面，有两个面板选单词条：*Properties*（属性）和*Sessions*（会话）。

属性

属性默认加载页面：



此页面显示的信息反映出服务器的配置设定。只限于查看。变更必须通过*此服务器*选单的*服务器信息* 界面选单作出（见第164页）。

会话

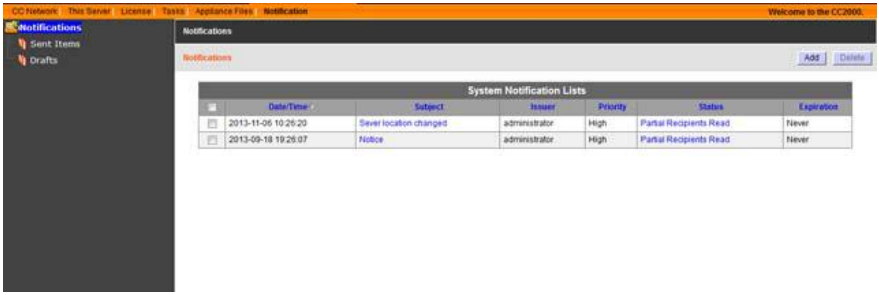
从侧边栏或主界面列表选择特定CC2000后，将出现面板选单，单击会话，弹出一个画面，允许管理员查看所有当前登入到此CC2000的用户，并提供其会话“何人、何处、何时”的相关信息。

此页面也向管理员提供通过选择用户并单击**End Session**（结束会话）轻质退出用户的选项。

注意：结束会话功能只有在选中的服务器为当前登入服务器时有效。

通知

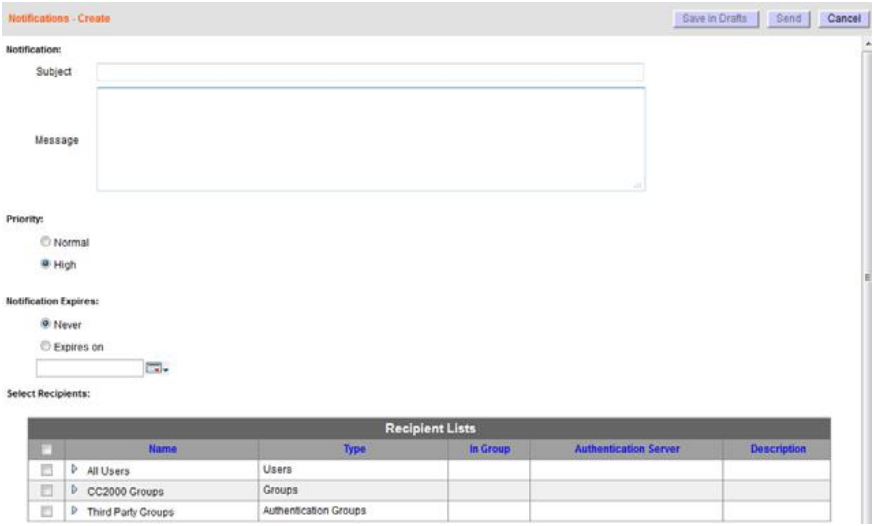
通知 页面允许您向登入到CC2000的用户发送信息。新信息的通知将出现在欢迎信息旁的橘色信息条。通知页面有主界面和侧边栏树状图，如下：



System Notification Lists（系统通知列表）显示所有发出的和存为草稿的信息。从此页面中，您可以**添加**信息；选择和删除信息；单击信息的**Subject**（主题）将其*保存* 或*发送* 为新信息。

如要创建通知信息：

1. 单击**Add**（添加）。出现下图页面：



2. 填充*Subject*（主题）和*Message*（信息）字段。

3. 指定*优先级*。

高优先级信息在用户登入的第一页显示，同时在*欢迎信息* 旁有橘色的信息条，如下：

一般优先级信息在用户登入时，其体形在*欢迎信息* 旁的橘色信息条上显示，如下：

4. 选择*Never*（永不）或*Notification Expires*（通知过期），设置系统信息过期时间。
5. 选择信息接收人。您可以在*名称* 栏展开，选择单个用户。
6. 单击**Save in Drafts**（保存为草稿）或**Send**（发送）。

第八章
日志

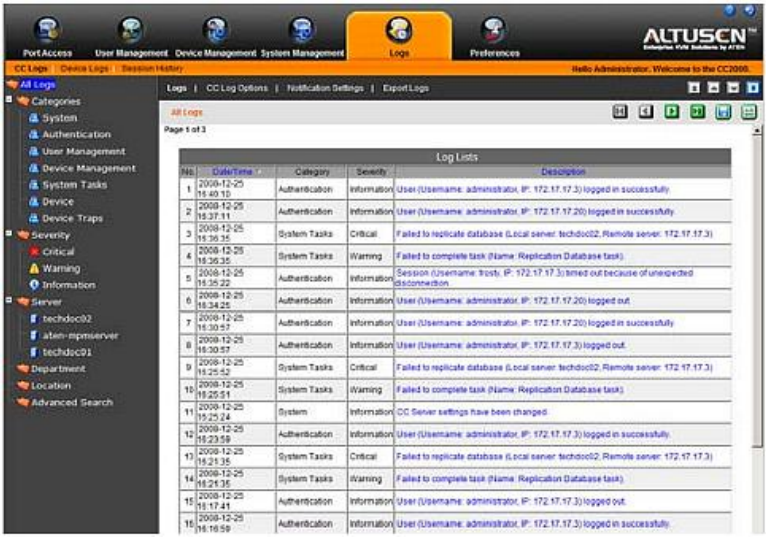
概述

CC2000 保留大量的发生在设备上的所有操作记录。*Logs*(日志)页提供一批强有力的过滤器和功能，这些过滤器和功能允许您浏览和导出日志文件数据，以及指定事件发生时发送邮件通知您。

CC 日志

日志

当点击 Logs 选项卡时，CC2000 打开默认 CC *Logs* 页(*Logs* 在子菜单上)，页面看起来类似如下：



- 默认页面布局按时间顺序从近至远显示关于发生在整个CC2000设备中所有日志服务器上的所有事件。
  - 点击 *Date/Time* 栏标题，则改变排序，标准时间顺序或倒时间顺序。
  - 点击 *Description* 栏标题，则改变排序，标准字母顺序或倒字母顺序。

- 侧栏提供一个过滤功能 – 点击一个项目，以仅显示与其相关的事件。最后的项目，高级搜索，在第 221 页详细描述。

注意：1. 一般来说，空白页说明那个类别没有日志事件记录。

2. 但是，如果*设备陷阱*页(Categories → Device Traps)是空白，这可能说明未启用事件陷阱通知功能。关于启用陷阱通知的信息见第 142 页的*注意* 2。

- 主面板右上方的项行按钮，导航通过侧栏(见第 28 页的*导航按钮*)。
- 底行按钮的首四个按钮，导航通过所列事件的页面。最左边的按钮带您到首页；最右边的按钮带您到尾页；中间的按钮前移或后移一个页面。

注意：当有其可以执行的相关操作时，这些按钮才可用。例如，当有不只一页信息时，且您在首页，“前移”和“尾页”按钮可用，但是“后移”和“首页”按钮不可用。

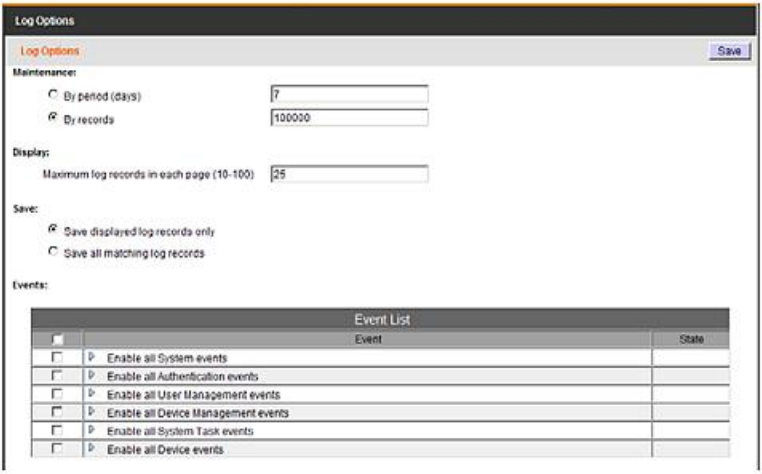
- 点击某项目的 *Description*，打开一个带有关于项目详细信息的页面：

用面板右上方的按钮，在详尽视图中移到前面或后面的项目，或关闭页面并回到*日志*页。

- 将日志列表保存成一个文件，点击有磁带图标的按钮。(只保存显示的列表 – 所有或过滤后的)。
- 打印日志列表，点击有打印机图标的按钮。(只打印显示的列表 – 所有或过滤后的)。

CC 日志选项

CC Log Options(CC 日志选项)页使您控制日志文件的组成和维护。当您选择 **Options** 时，一个类似如下的页面出现：



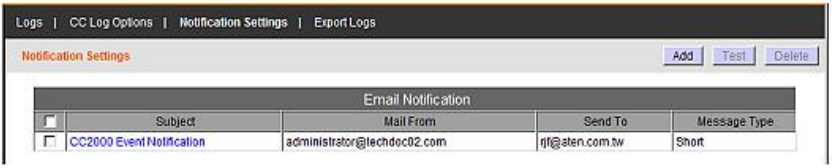
设定项目的含义如下表所描述：

项目	说明
Maintenance (维护)	点击一个单选按钮，选择是根据天数或是根据记录数维护日志数据库，然后选择维护数据库的天数或记录数。当达到此数时，根据“先进先出”的原则丢弃事件。有效范围是 7-90 天，及 1000-100000 条记录。
Display (显示)	设置最多显示在网络页上的事件数。有效范围是 10-100。
Save (保存)	点击一个单选按钮，选择当保存日志文件时，是仅保存显示的事件，还是保存与事件列表中所做选项对应的所有事件(见下面的 *Events*)。

项目	说明
Events (事件)	显示由 CC2000 记录的事件类别列表，并让您选择您要追踪的事件类别。默认启用类别 All。您可以通过点击类别名前面的箭头，并勾选或不勾选各类别中的特定事件，来细调类别内容。

通知设置

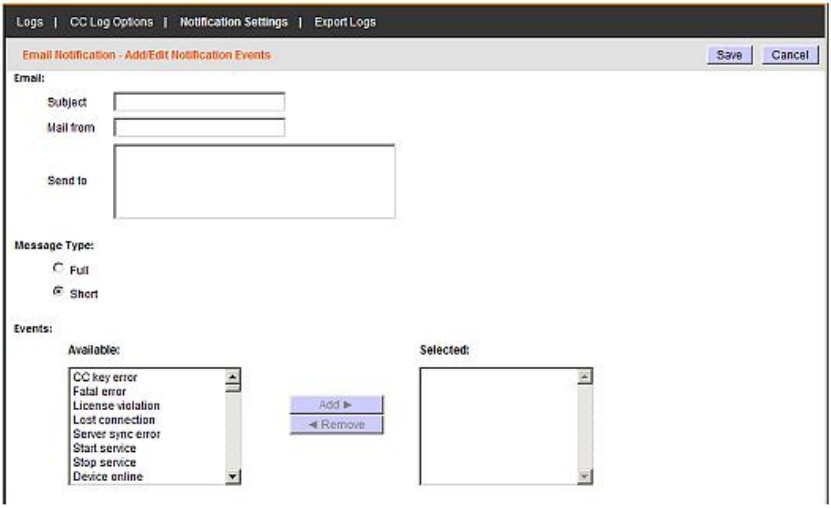
Notification Settings(通知设置)页用来通知特定用户发生在 CC2000 设备上的特定事件。当选择 **Notification Settings**，一个类似如下的页面出现：



添加和设定通知用户

添加用户并指定用户被通知的事件，请按如下操作：

1. 点击面板右上方的 **Add**。*Email Notification - Add/Edit Notification Events* 页出现：



2. 在 *Subject* 区为通知信息键入适当的标题。
3. 在 *Mail from* 区键入其中一位管理员的邮件地址。
4. 在 *Send to* 区键入邮件通知接收人的地址。
5. 选择信息类型是 *Full*(全文)还是 *Short*(简要)。
6. 在 *Available* 区选择您要对其接收邮件通知的事件，然后点击 **Add** 以将其移到 *Selected* 栏。为其它您要对其接收邮件通知的事件重复此步骤。
7. 当填写完此页后，点击 **Save** 以保存设定并返回*通知设置*页。

注意：为了使用户接收事件的邮件通知，SMTP 设置信息必须在 CC2000 的 *SMTP 设置*页(详情请见第 168 页)设定。

修改通知设定

修改通知设定，在 *Email Notification* 表内点击其 *Subject* 名称；在 *Email Notification - Add/ Edit Notification Events* 页上进行您想要的修改；点击面板右上方的 **Save**。

删除通知设定

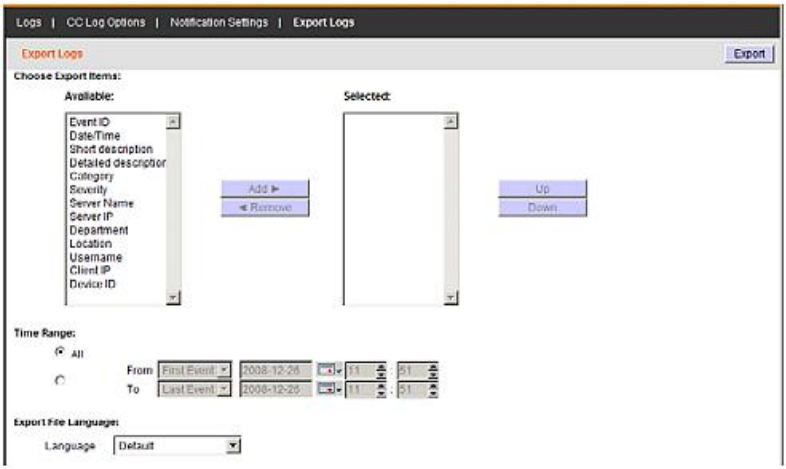
删除通知设定，在 *Email Notification* 表内点击勾选其 *Subject* 名称；点击面板右上方的 **Delete**。

测试通知设定

检查事件通知功能是否正常运行，在 *Email Notification* 表内点击勾选其 *Subject* 名称，然后点击 **Test**。如果系统正常运行，事件通知接收人将接收到事件通知邮件。

导出日志

Export Logs(导出日志)页用来将指定的记录事件保存成一个文件。当选择 **Export CC Logs** 时，一个类似如下的页面出现：

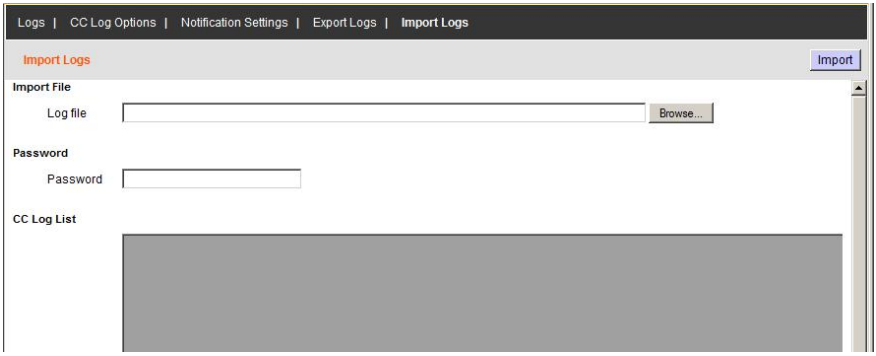


将指定的记录事件保存成一个文件，请按如下操作：

1. 在 *Available* 栏，选择您要包含在导出文件中的日志文件项目，然后点击 **Add** 以将其移到 *Selected* 栏。为其它您要包括的日志文件项目重复此步骤。
2. 修改*被选择*项目的顺序，点击您要移动的项目，然后点击 **Up** 或 **Down** 以修改到您要的位置。
3. 对于 *Time Range*，选择 **All** 则导出数据库中的、针对所选项目的所有记录。要导出特定时间段的记录，选择其下面的单选按钮，并用 *From* 和 *To* 设置时间参数。
4. 对于 *Export File Language*，选择 **Default** 则使文件以您的浏览器所设的语言导出文件。如果您喜欢不同的语言，下拉列表并选择提供的一种语言。
5. 当完成选项后，点击 **Export**(在面板右上方)。
6. 在出现的对话框内，选择“save file”选项。日志文件以 CSV 格式被保存，空白表格程序可读此格式。

导入日志

Import Logs（导入日志）页面用于打开之前保存的日志文件以便查看。选择侧边栏的 *Import Logs* ，如下页面将会出现：



如要导入之前保存的日志文件，按下述操作：

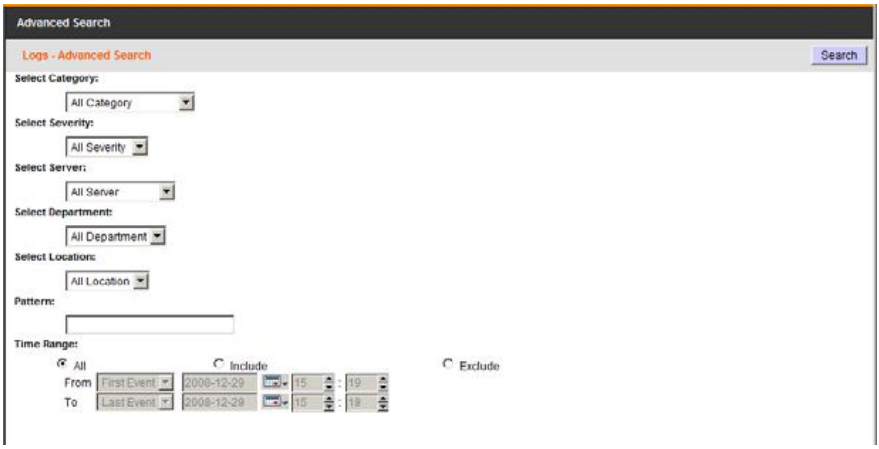
1. 在*Log file*（日志文件）字段输入完整的路径，或者点击**Browse**（浏览）移动到该文件。
2. 如果文件被加密，在*Password*（密码）字段输入创建时使用的密码。
3. 点击面板右上方的**Import**（导入）。

文件导入后，其内容将显示在*CC Log List* 面板中。

高级搜索

通过高级搜索功能，您可以降低每个搜索选项的参数，缩小范围，方便地进行搜索。如要执行高级搜索，请按下述操作：

1. 在侧边栏，点击**Advanced Search**（高级搜索）。将出现如下画面：



2. 下拉您想要选择指定搜索参数的列表。
3. 若您想要搜索特定的字或字符串，在*Pattern* 字段输入，然后选择是否合适的项目。
4. 在*Time Range*（时间范围）中，选择**All**（全部）将搜索数据库中的所有已存记录。如要搜索某一特定时间，点击*Include*（包含）或*Exclue*（不包含），在*From*（从）和*To*（到）中设置时间参数。

注意：1. 如果选择了*Include*（包含），将搜索指定时间范围内的全部事件。
2. 如果选择了*Excluede*（不包含），将只搜索这段时间之外的事件。

---

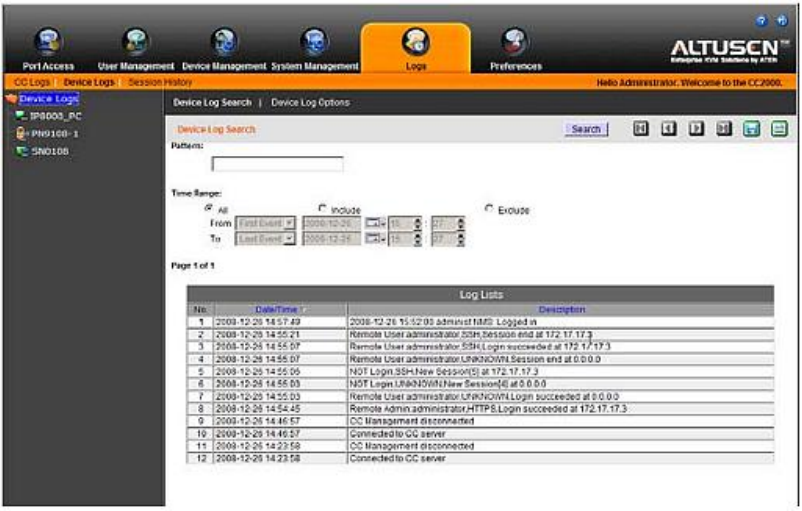
5. 选择完成后，点击**Search**（搜索）（界面右上角）。

搜索结果显示在主界面的日志列表中。

- 如要保存搜索结果为文件，点击磁盘图标按钮。
- 如要打印搜索结果，点击打印机图标按钮。
- 列表类别顺序可以通过点击栏标题更改。

设备日志

CC2000 充当所有 ATEN/ Altusen NET™设备的日志服务器，将发生在设备上的系统事件记录在数据库中。当点击子菜单上的 Device Logs(设备日志)时，*Device Logs Search* 页出现，此页允许您搜索包含特定词或字串的事件。



- 默认布局以倒时间顺序显示整个 CC2000 设备中所有设备的日志信息。
  - 点击 *Date/Time* 栏标题，则改变排序，标准时间顺序或倒时间顺序。
  - 点击 *Description* 栏标题，则改变排序，标准字母顺序或倒字母顺序。
- 侧栏提供一个过滤功能 – 点击一个项目，以仅显示与其相关的事件。
- 主面板右上方的导航按钮(箭头)使您通过日志列表的各页面。最左边的按钮带您到首页；最右边的按钮带您到尾页；中间的按钮前移或后移一个页面。

注意：当有其可以执行的相关操作时，这些按钮才可用。例如，当有不只一页信息时，且您在首页，“前移”和“尾页”按钮可用，但是“后移”和“首页”按钮不可用。

- 将日志列表保存成一个文件，点击有磁带图标的按钮。(只保存显示的列表 – 所有或过滤后的)。
- 打印日志列表，点击有打印机图标的按钮。(只打印显示的列表 – 所有或过滤后的)。

设备日志搜索

搜索日志，请按如下操作：

1. 如果您要搜索特定词或字串，将其键入在 *Pattern* 区。
2. 对于 *Time Range*，选择 **All** 则根据所选样式搜索数据库中的所有记录。要搜索特定时间段的记录，选择 *Include* 或 *Exclude* 按钮，并用 *From* 和 *To* 设置时间参数。

注意：1. 如果选择了 *Include* 按钮，则搜索在此时间范围之内的所有事件。
2. 如果选择了 *Exclude* 按钮，则只搜索在此时间范围之外的事件。

---

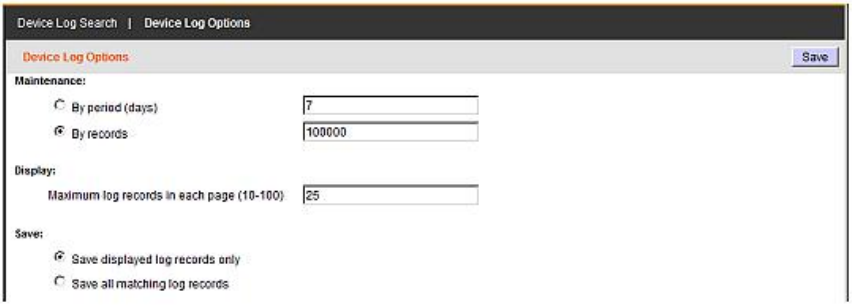
3. 当做完选择后，点击 **Search** (在面板右上方)。

搜索结果显示在主面板中的日志列表内。

- 要将搜索结果保存成一个文件，点击有磁带图标的按钮。
- 要打印搜索结果，点击有打印机图标的按钮。

设备日志选项

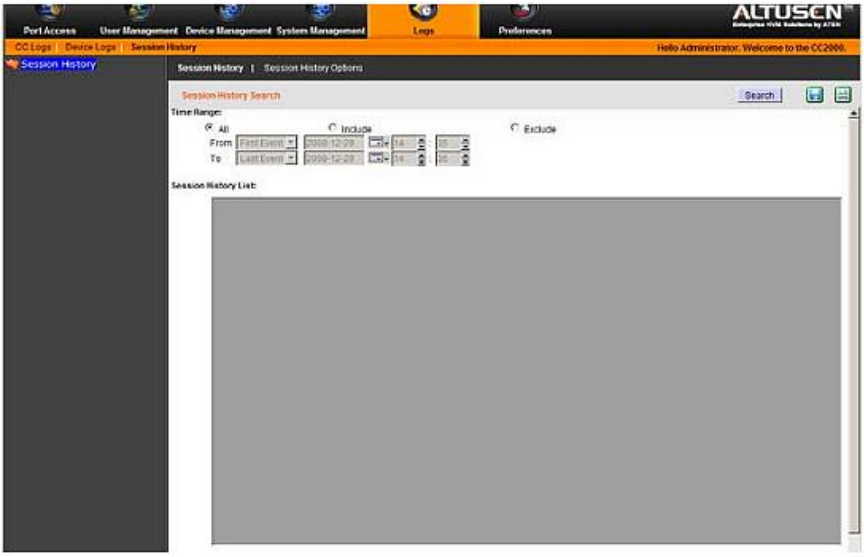
Device Log Options(设备日志选项)页提供关于 CC2000 的设备日志数据库的管理选项，当您选择 **Device Log Options** 时，一个类似如下的页面出现：



- **Maintenance** 允许您选择是根据天数或是根据记录数维护设备日志数据库。点击一个单选按钮以进行选择，然后键入维护数据库的天数或记录数。当达到此数时，根据“先进先出”的原则丢弃事件。
- **Display** 允许您设置最多显示在网络页上的事件数。
- **Save** 允许您将设备日志保存成一个文件：
  1. 先点击一个单选按钮，选择是只保存当前选择的设备日志记录，还是保存所有设备日志记录，然后点击 **Save** (在面板的右上方)。
  2. 在出现的对话框内，选择“save file”选项。日志文件以 CSV 格式被保存，空白表格程序可读此格式。

会话历史

CC2000 保存发生的所有用户会话记录。当点击子菜单上的 Session History(会话历史)时，*Session History Search* 页出现：



会话历史搜索

搜索会话历史记录，请按如下操作：

1. 对于 *Time Range*，选择 **All** 则搜索数据库中的所有记录。要搜索特定时间段的记录，选择 *Include* 或 *Exclude* 按钮，并用 *From* 和 *To* 设置时间参数。

> **注意**：1. 如果选择了 *Include* 按钮，则搜索在此时间范围之内的所有事件。
> 2. 如果选择了 *Exclude* 按钮，则只搜索在此时间范围之外的事件。

2. 当完成时间范围选择后，点击 **Search** (在面板右上方)。

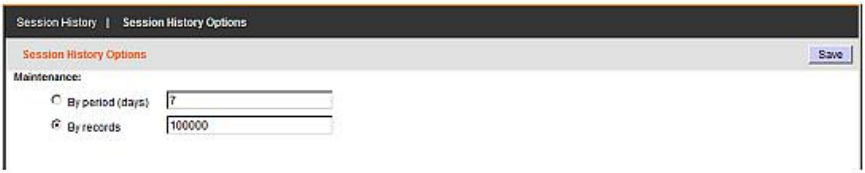
搜索结果显示在主面板中的会话历史列表内。

◆ 将搜索结果保存成一个文件，点击有磁带图标的按钮。

- 打印搜索结果，点击有打印机图标的按钮。

会话历史选项

Session History Options(会话历史选项)页提供关于 CC2000 的会话历史数据库的管理选项，当您选择 **Session History Options** 时，一个类似如下的页面出现：

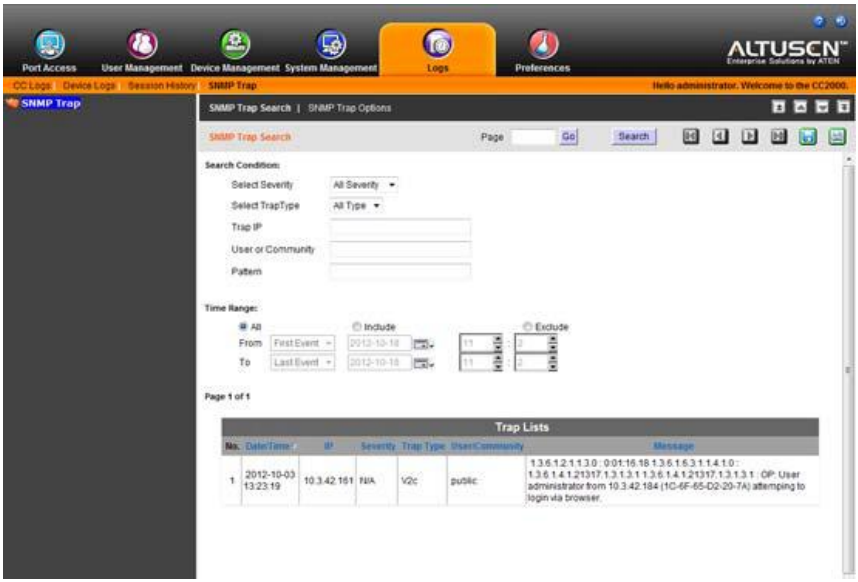


Maintenance 允许您选择是根据天数或是根据记录数维护会话历史数据库。

- 点击一个单选按钮以进行选择，然后键入维护数据库的天数或记录数。当达到此数时，根据“先进先出”的原则丢弃事件。
- 保存设置，点击 **Save** (在面板的右上方)。

SNMP 陷阱

SNMP Trap（SNMP陷阱）选项卡允许您搜索SNMP陷阱事件并设置进一步的选项，以搜索并显示功能。



注意：如要设置哪些SNMP陷阱事件被记录到日志中，在*CC Log Options* 选项卡事件列表中作出选择，详见第215页，*CC日志选项* 。

SNMP陷阱搜索

在选项卡顶部，您可以在陷阱列表搜索指定的页面，或者使用控制键导航到陷阱列表。对于更加精确的搜索，根据下文设置搜索参数：

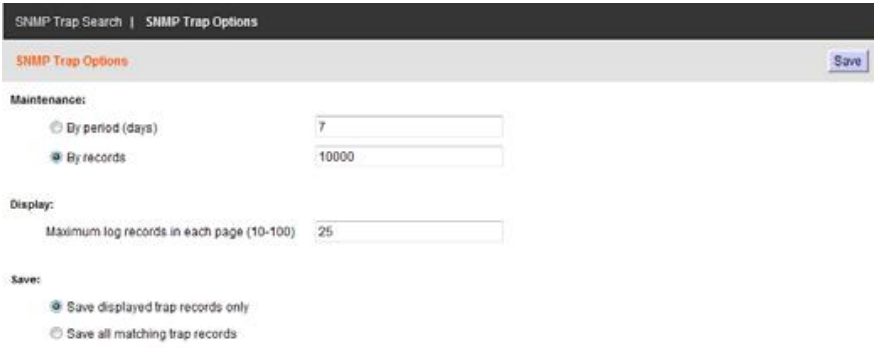
搜索条件

- *选择安全性* – 从下拉选单选择时间安全性。选项为：未知、信息、警告、严重。
- 选择陷阱类型 – 从下拉选单选择陷阱类型。选项为：V1;V2c; V3。
- *陷阱IP* – 输入您想要搜索陷阱事件的指定IP地址。
- 用户或社区 – 输入您想搜索陷阱时间的指定用户或社区。

- 模式 – 输入您想搜索陷阱事件的指定模式。

SNMP陷阱选项

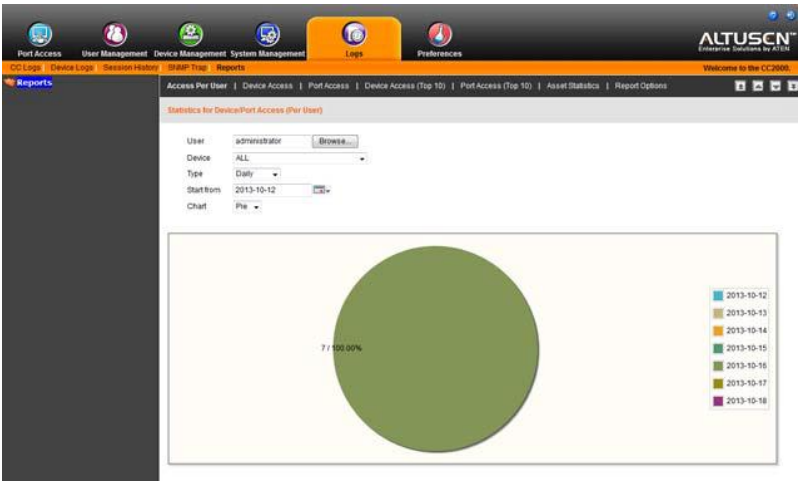
进一步的SNMP陷阱选项可以在此选项卡下配置。



- *维护* – 选择一段时间（天数）或输入记录次数。
- *显示* – 输入显示在每页的日志记录总数（范围10-100）
- *保存* – 您可以选择仅保存显示的陷阱记录或保存所有匹配的陷阱记录。

作出选择后，单击**Save**保存。

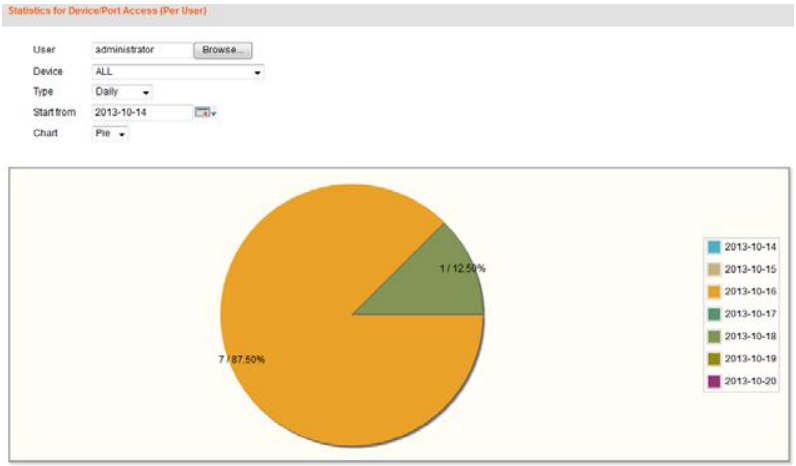
报告



Reports（报告）选项卡允许您查看CC2000架构中的用户和设备的*访问数据*，并且设置如何显示报告。

平均用户访问

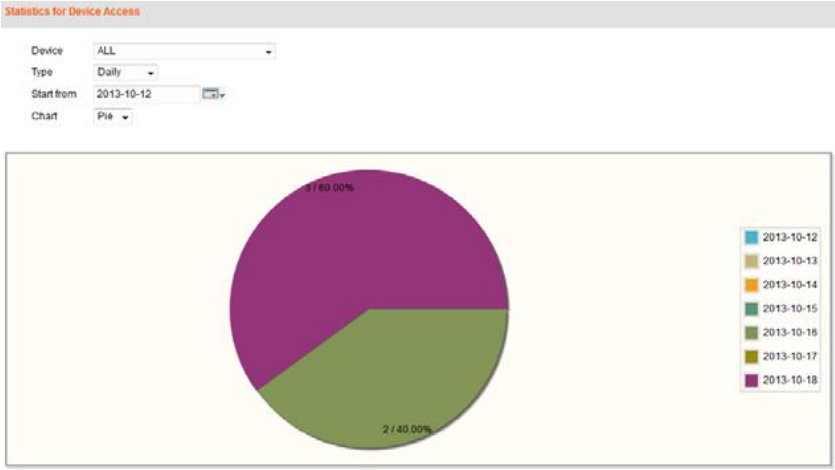
此页面提供*每个用户的设备/端口访问数据*。使用下一页的选项创建饼状图或柱状图，显示您所选择的参数。



项目	描述
User 用户	单击**Browse**（浏览）弹出可以选择用户的列表。使用单选按钮选择用户并单击**OK**，显示其访问数据。
Device 设备	选择 **All** 或单独的端口/设备显示其数据。将根据您所选择的*类型* 显示用户访问设备的数量图像。 在每个表格颜色中显示的数量表示设备被访问的次数（当天/本周/本月/本季/本年）以及整体比例。
Type 类型	选择表格分成的时间。表格会根据所选时间段，显示*设备* 在某端时间内被访问的次数。 ◆ **每天**：显示 7 天内设备每天被访问的次数，从 *Start From*（开始于）的日期开始。 ◆ **每周**：显示 4 周内设备每周被访问的次数，从 *Start From*（开始于）的日期开始。格式 2013-W42 代表 2013 年的第 42 周。 ◆ **每月**：显示每年 12 个月内设备每月被访问的次数，从 *Start From*（开始于）的日期开始。 ◆ **每季**：显示每年 4 个季度内设备每季度被访问的次数，从 *Start From*（开始于）的日期开始。 ◆ **每年**：显示每年 5 年内设备每年被访问的次数，从 *Start From*（开始于）的日期开始。 **注意**：如果设备没有被访问过，不会有数据显示。
Start From 开始于	单击日历，选择在表格中体现的时间段的开始日期。
Chart 表格	选择您想用于显示信息的表格类型： ◆ **饼状图**：根据所选的时间段分配的圆形表格。 ◆ **柱状图**：根据所选的时间段分配的个人柱状图像。 ◆ **全部**：显示饼状图和柱状图表格。
Color/Key 颜色/图解	饼状图表格右侧为颜色编码图解，每一个时间段用一个颜色代表。

设备访问

此页面提供*设备访问数据* 。使用表格中的选项创建饼状图或柱状图，显示您所选择的参数。

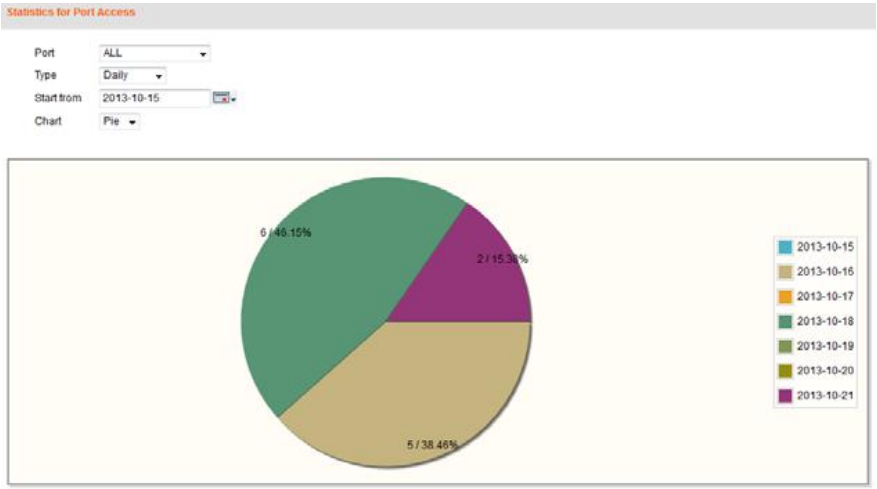


项目	描述
Device 设备	选择 **All** 或单独的端口/设备显示其数据。将根据您所选择的*类型* 显示用户访问设备的数量图像。 在每个表格颜色中显示的数量表示设备被访问的次数（当天/本周/本月/本季/本年）以及整体比例。
Type 类型	选择表格分成的时间。表格会根据所选时间段，显示*设备* 在某端时间内被访问的次数。 ◆ **每天**：显示 7 天内设备每天被访问的次数，从 *Start From*（开始于）的日期开始。 ◆ **每周**：显示 4 周内设备每周被访问的次数，从 *Start From*（开始于）的日期开始。格式 2013-W42 代表 2013 年的第 42 周。 ◆ **每月**：显示每年 12 个月内设备每月被访问的次数，从 *Start From*（开始于）的日期开始。 ◆ **每季**：显示每年 4 个季度内设备每季度被访问的次数，从 *Start From*（开始于）的日期开始。 ◆ **每年**：显示每年 5 年内设备每年被访问的次数，从 *Start From*（开始于）的日期开始。 **注意**：如果设备没有被访问过，不会有数据显示。

项目	描述
Start From 开始于	单击日历，选择在表格中体现的时间段的开始日期。
Chart 表格	选择您想用于显示信息的表格类型： ◆ **饼状图**：根据所选的时间段分配的圆形表格。 ◆ **柱状图**：根据所选的时间段分配的个人柱状图像。 ◆ **全部**：显示饼状图和柱状图表格。
Color/Key 颜色/图解	饼状图表格右侧为颜色编码图解，每一个时间段用一个颜色代表。

端口访问

此页面提供*端口访问数据* 。使用表格中的选项创建饼状图或柱状图，显示您所选择的参数。

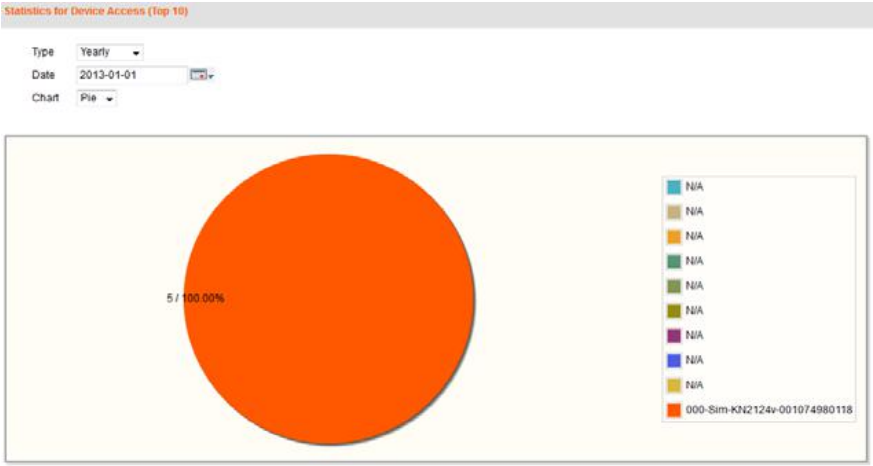


项目	描述
Port 端口	选择 **All** 或单独的端口/设备显示其数据。将根据您所选择的*类型* 显示用户访问*端口* 的数量图像。 在每个表格颜色中显示的数量表示设备被访问的次数（当天/本周/本月/本季/本年）以及整体比例。

项目	描述
Type 类型	选择表格分成的时间。表格会根据所选时间段，显示*端口* 在某端时间内被访问的次数。 ◆ **每天**：显示 7 天内端口每天被访问的次数，从 *Start From*（开始于）的日期开始。 ◆ **每周**：显示 4 周内端口每周被访问的次数，从 *Start From*（开始于）的日期开始。格式 2013-W42 代表 2013 年的第 42 周。 ◆ **每月**：显示每年 12 个月内端口每月被访问的次数，从 *Start From*（开始于）的日期开始。 ◆ **每季**：显示每年 4 个季度内端口每季度被访问的次数，从 *Start From*（开始于）的日期开始。 ◆ **每年**：显示每年 5 年内端口每年被访问的次数，从 *Start From*（开始于）的日期开始。 **注意**：如果端口没有被访问过，不会有数据显示。
Start From 开始于	单击日历，选择在表格中体现的时间段的开始日期。
Chart 表格	选择您想用于显示信息的表格类型： ◆ **饼状图**：根据所选的时间段分配的圆形表格。 ◆ **柱状图**：根据所选的时间段分配的个人柱状图像。 ◆ **全部**：显示饼状图和柱状图表格。
Color/Key 颜色/图解	饼状图表格右侧为颜色编码图解，每一个时间段用一个颜色代表。

设备访问（前10）

设备访问数据 – 前10 页面显示总访问量前10的设备以及被访问次数。使用表格中的选项创建饼状图或柱状图，显示您所选择一种或两种参数。

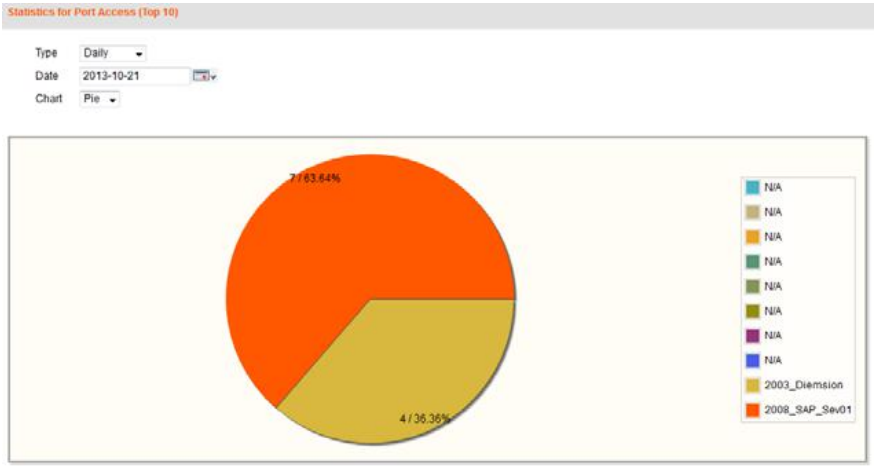


项目	描述
Type 类型	选择表格分成的时间。表格会根据所选时间段，显示在某端时间内总访问量前 10 的设备及被访问的次数。 ◆ **每天**：显示某天内前 10 的设备及访问次数 ◆ **每周**：显示某一周内前 10 的设备及访问次数 ◆ **每月**：显示某一月年前 10 的设备及访问次数 ◆ **每季**：显示某一季度内前 10 的设备及访问次数 ◆ **每年**：显示某一年内前 10 的设备及访问次数
Date 日期	单击日历，选择表格中要体现的时间（日/周/月/季/年）。

项目	描述
Chart 表格	选择您想用于显示信息的表格类型： ◆ **饼状图**：根据所选的时间段分配的圆形表格。 ◆ **柱状图**：根据所选的时间段分配的个人柱状图像。 ◆ **全部**：显示饼状图和柱状图表格。
Color/Key 颜色/图解	饼状图表格右侧为颜色编码图解，每一个时间段用一个颜色代表。

端口访问（前10）

端口访问数据 – 前10 页面显示总访问量前10的端口以及被访问次数。使用表格中的选项创建饼状图或柱状图，显示您所选择一种或两种参数。

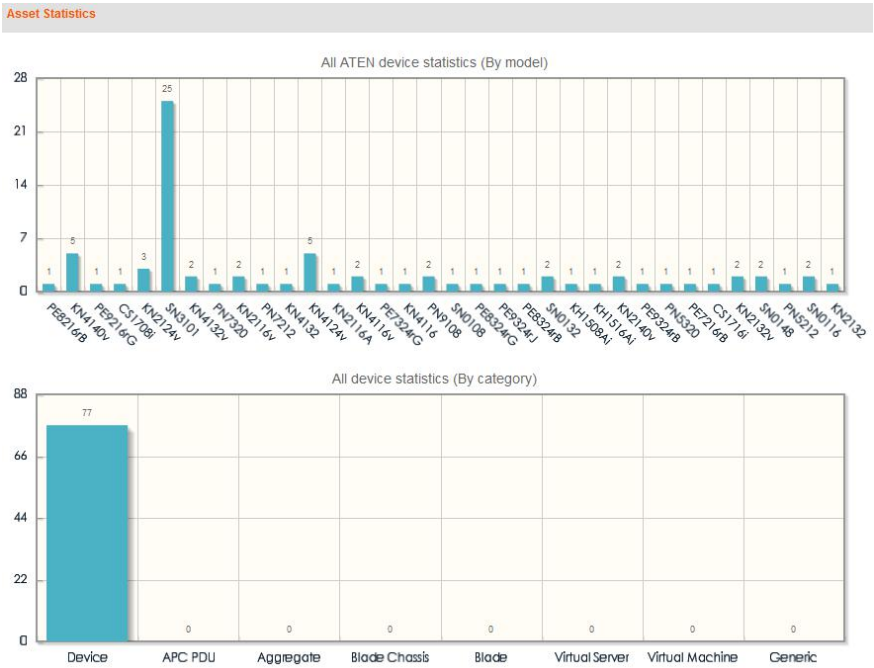


项目	描述
Type 类型	选择表格分成的时间。表格会根据所选时间段，显示在某端时间内总访问量前 10 的端口及被访问的次数。 ◆ **每天**：显示某天内前 10 的端口及访问次数 ◆ **每周**：显示某一周内前 10 的端口及访问次数 ◆ **每月**：显示某一月年前 10 的端口及访问次数 ◆ **每季**：显示某一季度内前 10 的端口及访问次数 ◆ **每年**：显示某一年内前 10 的端口及访问次数
Date 日期	单击日历，选择表格中要体现的时间（日/周/月/季/年）。

项目	描述
Chart 表格	选择您想用于显示信息的表格类型： ◆ **饼状图**：根据所选的时间段分配的圆形表格。 ◆ **柱状图**：根据所选的时间段分配的个人柱状图像。 ◆ **全部**：显示饼状图和柱状图表格。
Color/Key 颜色/图解	饼状图表格右侧为颜色编码图解，每一个时间段用一个颜色代表。

资产数据

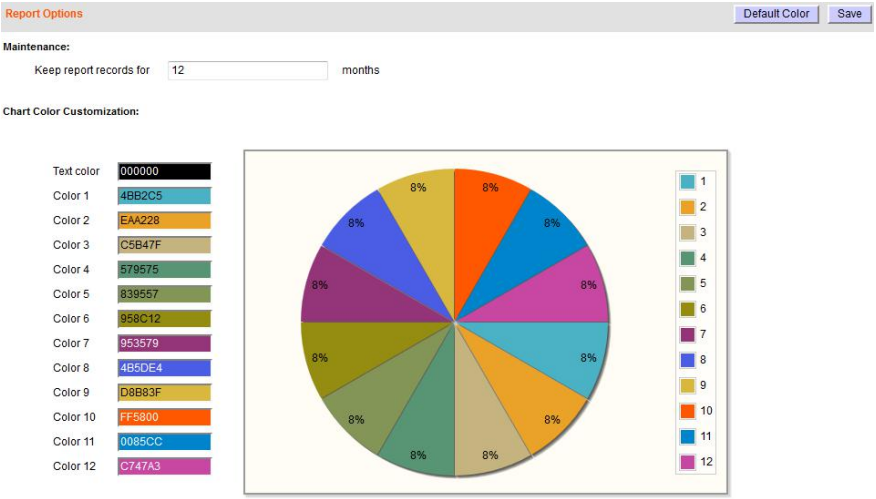
资产数据 页面显示添加到CC2000架构的所有自残，在两个图标中显示：*ATEN设备数据*（型号）*和所有设备数据*（类别）。



ATEN设备数据显示当前连接到CC2000架构中的ATEN设备型号。**所有设备数据**显示连接到CC2000架构中的所有设备类别：*设备（ATEN设备）*、*SPC PDU*、*整合*、*刀片机箱*、*虚拟服务器*、*虚拟机和通用设备*。

报告选项

此页面提供定制报告颜色和保存报告记录的选项。



项目	描述
Mantainance 维护	输入您希望系统删除前保留数据记录的月数。
Chart Color Customization 图标颜色定制	◆ 文本颜色：单击方框弹出一个小窗口，选择您希望在报告内用于文本显示的颜色。 ◆ 颜色 1~12：单击方框弹出一个小窗口，选择您希望在图表中用于文本每项图解的颜色。 **注意**：选择颜色后，右侧的测试图表会有所变化，方便您看到效果。
Default Color 默认颜色	单击使所有颜色返回默认设置。
Save 保存	单击应用变更的图表颜色。

附录 A
技术信息

安全说明

概述

- 请阅读所有说明，并作为以后参考。
- 请遵循设备上的所有警告与指示。
- 勿将本设备放置于任何不平稳的平面上（如推车、架子、或桌子等），如果本设备掉落，会造成严重的损坏。
- 请勿在接近水的地方使用本设备。
- 请勿将本设备放置于散热器或是暖气设备旁边或其上方。
- 本设备外壳配有槽孔以散热及通风，为了确保操作中防止过热，勿将开孔处堵塞或遮盖住。
- 本设备不可放置于柔软的表面上（如床、沙发、毛毯等），这将会堵塞风扇开孔，同样也不能放在密封的环境下，除非已提供了适当的通风，才可以放置。
- 请勿将任何液体洒在设备上。
- 清洁前必须将本设备电源从墙上的插座上拔除，请勿使用任何液状或沫状的擦拭剂，请使用湿布清洁。
- 请按照标签上的电源类型使用本设备，如果您不确定电源类型是否可用，请联系经销商或当地的电力公司。
- 本设备配有3脚接地型插头，此为安全性目的。如果您无法将其插入插座上，请联系电工替换原有的电源插座。请勿试图将接地型插头功能去除，并遵循本地/全国接线代码。
- 请勿将任何东西放置于电源线或连接线上，并将电源线与连接线的布线路径安排好，避免被其绊倒。
- 如果设备使用了延长线，确保所有使用该线的产品总电量不超过该线的电流承载量。确保所有插至墙壁插座的产品电流总量不超过15 安培。

- 请选用突波抑制器、调节器或不断电系统（UPS）等设备，以帮助避免您的系统受突然、瞬间增加及减少的电量。
- 请将系统的连接线与电源线妥善固定好，确保无任何东西压在线缆上。
- 连接或卸载热插拔电源时，请遵循如下指导：
  - 安装此电源前，连接电源线到此电源。
  - 卸载此电源前，拔掉电源线。
  - 如果系统有多个电源，通过从所有电源拔掉所有电源线，来切断系统电源。
- 勿将任何物体透过外壳的槽孔塞进机器里，有可能会接触到危险的电压点或造成零件短路而导致火灾或触电的风险。
- 请勿尝试自行修理本设备，请找合格的服务人员以取得支援服务。
- 如果有以下情况发生，请将本设备的电源从墙上的插座上拔除并将其交予合格的服务人员修理。
  - 电源线或插头损坏或磨损
  - 液体被洒入本设备
  - 本设备被雨、水淋到
  - 本设备掉落或外壳已经损坏
  - 本设备功能出现明显的变化
  - 按照操作指示后，本设备无法正常操作
- 仅针对操作指示中所涵盖的控制功能进行调整，其它不适当的操作可能会造成损害，以致于需要合格的人员更庞大的作业才能修复。

机架安装

- 在机架上进行工作之前，请确保固定设备都安全地固定在机架上，并延伸至地板，且整个机架的重量可散布在地板上。 开始机架安装之前，在单一机架上安装前端及侧边的固定设备或是在联合多个机架上安装前端固定设备。
- 请从下而上装载机架，且先装载最重的东西。
- 从机架上延伸设备出来时，请确保机架平稳和稳定。
- 当按着设备滑轨释放弹簧闩及将设备滑入或滑出机架时，请当心，该滑动的轨道可能会夹到您的手指。
- 设备放到机架上后，请小心地拉动滑轨至锁定位置，然后将设备滑入机架。
- 不要过载为机架供电的交流电支路；整体机架的承载量不要超过支路电量的百分之八十。
- 请确保机架中的设备良好通风。
- 当您维护机架上其它设备时，请勿踩踏或站在任何设备上。

技术支持

中国

电子邮件支持	请电邮您的问题和不明之处发邮件： support@aten.com
在线支持 ◆ 技术支持 ◆ 故障排除 ◆ 文件 ◆ 软件更新	1. Altusen 客户可通过我们的电子支持中心获得在线技术支持。 **http://support.aten.com** 2. 我们的网站提供在线故障排除(描述最常见的问题并提供可能的解决方案)、在线文件(包括电子用户手册)和适用于您产品的最新驱动器和固件。**http://www.aten.com.cn**
电话支持	400-6820-600

当您联络我们时，请预先准备下列信息以方便我们快速地为您服务：

- 产品型号、序号和购买日期。
- 您的电脑设置，包括操作系统、修订层级、扩充卡和软件。
- 错误出现时，任何显示在屏幕上的错误信息。
- 导致错误的操作顺序。
- 其它任何您觉得有帮助的信息。

USB 验证密钥规格

功能		密钥
作业环境	操作温度	0 – 40 °C
	储存温度	-20 – 60 °C
	湿度	0 – 80% RH
机体属性	组成	金属和塑料
	重量	14 克
	尺寸	8.36 × 2.27 × 1.36 厘米

支持 CC2000 的 ATEN/ Altusen IP 产品

如下是能够被CC2000远程集中控制中心设备管理的ATEN/AltusenIP产品的列表：

- CN8000; CN8600
- CS1708i; CS1716i
- KH1508i; KH1516i; KH1508Ai; KH1516Ai
- KL9108; KL9116
- KL1508Ai; KL1516Ai
- KN1000
- KN1108v / KN1116v
- KN2108; KN2116
- KN2116A; KN2132; KN4116; KN4132[2]
- KN2116v; KN2124v; KN2132v; KN2140v; KN4116v; KN4124v;
- KN4132v; KN4140v[2]
- KN4164V, KN8132V, KN8164V
- KN9008; KN9016
- KN9108; KN9116
- PN0108[3]; PN9108
- PN5212; PN5320; PN7212; PN7320
- SN0108A; SN0116A; SN0132; SN0148
- SN0108; SN0116; SN9108; SN9116; SN3101

智能PDU

- EC1000
- EC2004
- PE5108; PE5208
- PE5220s
- PE5340s
- PE6108

- PE6208; PE6216
- PE6324
- PE7108; PE7208
- PE7214
- PE7328
- PE8108
- PE8208; PE8216
- PE8324
- PE9222
- PE9330
- PE7216r (ARM-based)
- PE7324r (ARM-based)
- PE8216r (ARM-based)
- PE8324r (ARM-based)
- PE9216r (ARM-based)
- PE9324r (ARM-based)

注意：1. 这些是撰写手册时支持的设备。请访问我们的网页，以查看自从手册出版后是否另有支持的设备。

2. 这些切换器可用作母设备，以堆叠下面的部分提到的切换器。

3. CC2000 不直接支持 PN0108 – 其只支持菊式串连到 PN9108 的 PN0108。

支持的 KVM 切换器

完全支持的可用于堆叠串联设备中的KVM切换器如下表：

- KH88
- KH89
- KH1508/ KH1516
- KH1508A/ KH1516A
- CS9134
- CS9138

注意：设备在第二层级外不能再堆叠。

设备 ANMS 设置

从设备的 ANMS 设置页启用设备的 CC 管理，请按如下操作：

1. 登录设备。
2. 参考下表，以打开 ANMS 页。
3. 在 ANMS 页，点击复选框以启用 CC 管理，然后键入管理设备的 CC2000 服务器的 IP 地址和设备端口号(见第 15 页的*设备端口*)。

VPNs

基本上，VPN (虚拟专用网络)是一个用公共网络(通常是因特网)将几个站点连接起来的专用网络。它一般包括几个 WAN。许多公司创建自己的 VPN 以提供两个站点之间的安全网络连接。但是，VPN 的缺点是网络是安全的，而吞吐量可能较低。

如果用 VPN 来连接几个 CC2000 管理系统中的站点，只有绝对有必要管理此系统的 CC2000 服务器才是单一主服务器－而不是用标准因特网部署的必要的主和从 CC2000 服务器的网络。但是，我们建议部署至少一台 CC2000 从服务器，以便给连接的设备提供冗余服务。

部署额外 CC2000 从服务器的另一个好处是，通过均衡网络流量，它们可以提供更高效的操作和管理。

防火墙

当几台 CC2000 位于不同防火墙之后时，必须在服务器上指定如下服务端口，在防火墙上必须打开相应端口。

1. CC 端口

注意：各 CC2000 服务器可以有不同的设置，(例如，8001 在服务器 1 上；8005 在服务器 2 上)。但是，在防火墙上打开的端口必须对应 CC 端口设置(8001 在服务器 1 的防火墙上；8005 在服务器 2 的防火墙上)。

2. CC2000 主服务器的 HTTPS 端口
3. CC2000 代理端口(见下面部分的 *CC2000 代理功能*)
4. CC2000 从服务器的 HTTPS 端口(可选项)

注意：1. CC2000 客户端工作站可以打开网络浏览器会话到同一防火墙之内的 CC2000 从。与设备中其它 CC2000 服务器(在防火墙之外)的通讯和访问通过 CC 端口和代理端口进行－因此无需 HTTPS 端口。但是，这样做有一个缺点，您不能在防火墙之外的设备上执行设备设定。

2. 如果您喜欢防火墙之外的 CC2000 客户端工作站能够直接打开网络会话到防火墙之内的从服务器，您可以打开此端口。

CC2000 代理功能

CC2000 代理功能涉及位于防火墙之后的 CC2000 服务器。对于防火墙之外的 CC2000 客户端工作站访问防火墙之内的由 CC2000 服务器管理的 KVM 和串口设备，必须在这些服务器上启用 CC2000 代理功能，指定做代理端口的端口必须在防火墙上打开。

注意：1. 当代理端口尚未被指定和打开时，防火墙之外的 CC2000 客户端工作站可以打开与防火墙之内的 CC2000 服务器进行的网络浏览器会话，而 CC2000 服务器管理的 KVM 和串口控制端设备的连接界面不能被打开。

2. 如果未启用代理功能，且您仍要访问设备，您必须打开设备要求的、防火墙上的所有服务端口(HTTPS、Program、虚拟媒体、Telnet、SSH 等等)。

名称、描述和范围参数

下表列出在 CC2000 管理系统中的名称、描述和范围的参数和默认值：

注意：1. 除非指定了不同值，否则可以任何支持的语言输入区域条目。
2. 1 字节= 1 个英文数字字母字符。

类别		长度 / 范围	默认值
用户	登录名	多达 16 个英文数字字母字符。最少字符数基于帐户策略设置(见第 135 页的 *CC2000 验证*)。 不能用如下字符：/ \ **[ ] : ; | = , + * ? < > @ " '**	
	窗口名	多达 32 字节。 不能用如下字符：**" '**	
	密码	0-16 个英文数字字母字符。最少字符数基于帐户策略设置(见第 135 页的 *CC2000 验证*)。 0 意味着无密码验证。	
	描述	多达 256 字节。	
	会话超时时间	1-99 分钟。	3 分钟
	意外连接中断超时注销	2-10 分钟。	2 分钟
	邮件	多达 256 字节。 **From**：0-64 **To**：0-128 **Subject**：1-128	
群组	名称	2-32 字节 不能用如下字符：**" '**	
	描述	多达 256 字节。	

类别		长度 / 范围	默认值
用户类型	名称	2-32 字节。 不能用如下字符：" '	
	描述	多达 256 字节。	
验证 服务器	服务器名称	2-32 字节。 不能用如下字符：" '	
	描述	多达 256 字节。	
	浏览器方式	对于用户名和密码无限制。 **注意**：如果有太多字符，对 CC2000 性能有负面影响。	
CC2000 验证	用户名 最少	多达 16 个英文数字字母字符。最少字符数基于帐户策略设置(见第 75 页的 *CC2000 验证*)。 不能用如下字符：/ \ **[ ] : ; | = , + * ? < > @ " '**	6
	密码 最少	0-16 个英文数字字母字符。最少字符数基于帐户策略设置(见第 75 页的 *CC2000 验证*)。 0 意味着无密码验证。	6
	密码过期	天数无限制。	
设备	名称	0-32 字节	
	描述	多达 256 字节。	
	联络名称	字节数无限制。	
	电话号码	字节数无限制。	
	邮件通知	字节数无限制。	
虚拟设备	名称	1-32 字节	
	描述	多达 256 字节。	
ATEN/ Altusen 通用设备	名称	1-32 字节	
	描述	多达 256 字节。	
文件夹	名称	1-32 字节。	
	描述	多达 256 字节。	

类别		长度 / 范围	默认值
部门/位置	名称	1-32 字节。	
	描述	多达 256 字节。	
任务	所有任务名称	字节数无限制。	
	主数据库 备份密码	0-8 字节。 0 意味着无密码验证。	
	导出设备日志样式	字节数无限制。	
CC 日志选项	按时间段	7-90 天	
	按记录数	1000-100000	
	每页记录数	10-100	
日志通知设置	主题	1-128 字节。	
	邮自	多达 64 字节。	
	发至	多达 128 字节。	
用户偏好：网络选项	显示窗口名称	0-32 字节。	

受信认证

概述

当您尝试从浏览器登录设备时，安全警告信息会出现，通知您设备的认证未被信赖，并询问您是否要继续。

此认证可被信赖，但由于从Microsoft的受信认证列表中并未找到该认证名称，因此将出现警告。您可忽视警告并点击**Yes**以继续。

注意：为避免用户每次登录时必须经过的认证接受提示，您可以使用第三方权威(CA)，以获得一个签名认证。详情请见第 186 页的*导入签名的 SSL 服务器认证*。

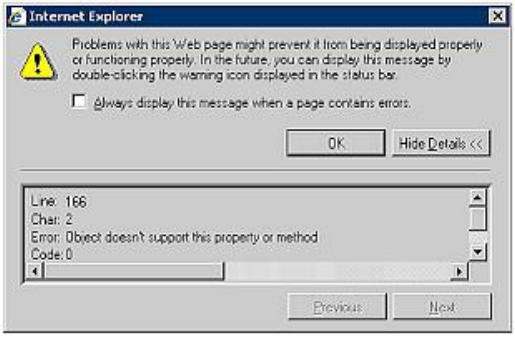
故障排除

问题	解决操作
尝试安装 CC2000 软件时，出现如下错误信息：“CC2000 is already installed. Please uninstall it first”	CC1000 和 CC2000 不能存在于同一服务器。安装 CC2000 前必须先卸载 CC1000。详情请见第 11 页的*卸载 CC1000*。
安装 CC2000 后，几分钟后出现如下错误信息：Error 1067	此错误信息由操作系统生成，它说明 CC2000 服务不能运行。要解决此问题，请尝试如下步骤： 1. 重启电脑。 2. 看您的电脑是否符合运行 CC2000 的最低要求(见第 6 页的*服务器要求*)。 3. 如果有以前的 CC2000 版本，且您正在以新安装而不是更新，来安装此版本，此错误信息可能说明您未从旧版本卸除所有文件(见第 21 页的*卸载 CC2000*)。遵循其中提到的的步骤卸载 CC2000，然后重装。
键入 CC2000 网站的 IP 地址，但是不能打开 CC2000 登录页面。	1. CC2000 仅允许 HTTPS 请求。来自浏览器的 HTTP 请求自动转向到 HTTPS 请求。HTTP 默认端口是 80；HTTPS 默认端口是 443。如果任一这些端口被管理员设置为其它值，端口号必须作为 URL 字串的一部分输入。 例如，CC2000 的 IP 地址是 10.10.10.10，SSL 端口已被设置为 8443，那么在浏览器输入的 URL 字串应该是： `https://10.10.10.10:8443` 2. 运行在 CC2000 服务器上的其它服务正在使用默认端口。用 CC2000 工具(见第 259 页)修改端口设置。 3. 确保 CC2000 服务正在运行。如果您运行 Windows，见第 17 页的*安装后检查*；如果您运行 Linux，见第 20 页的*安装后检查*。

问题	解决操作
登录对话框语句的语言不是我在 CC2000 用户偏好中设置的语言。	登录页的语言优先功能先看您的浏览器设置了什么语言，再看您的操作系统语言。您登录后，CC2000 将以您在用户偏好中设置的语言显示。详情请见第 32 页的*网络选项*。
不能登录 CC2000。	请确保您的用户名和密码正确。
当尝试登录时，出现如下信息：“Login failed. You are attempting to log in from a computer that already has a browser session open.”	Netscape 和 Firefox (以及其它基于 Mozilla 的浏览器)针对与同一服务器的多连接，分享相同的会话 ID。一旦已有用同一会话 ID 的会话打开时，CC2000 将拒绝登录请求。 或是：1）结束当前打开的会话并再次登录；2）从不同电脑登录；或是 3）用一个非基于 Mozilla 的浏览器登录。 **注意**：这种情况也出现在运行于 Windows98 的某些 IE 版本。
登录时，浏览器生成 *CA Root certificate is not trusted*，或 *Certificat Error* 回应信息。	从 Microsoft 的受信认证列表中并未找到该认证名称。但是，认证可被信任。详情请见第 252 页的*受信认证*。
登录 CC2000 后，没有端口访问选项卡或端口访问页。	您未被授权访问任何端口。请与您的 CC2000 管理员核查，以获得访问您负责的端口的授权。
登录 CC2000 后，不能打开我要访问的设备的页面。	请与您的 CC2000 管理员核查，找出您是否被授权访问此设备。
登录 CC2000 时，出现的唯一页面是系统管理选项卡，其仅有两个菜单条目：*本服务器*和*许可证*。	许可证冲突出现。关于解决此问题的详细说明，见第 189 页的许*可证冲突*。
未收到事件陷阱情况的邮件通知。	1. 检查邮件服务器设置是否已在 CC2000 管理器正确指定。 2. 检查在相关设备设置中指定的邮件地址是否已正确设置。 3. 检查针对相关设备的事件陷阱设置是否已正确指定。
当尝试从树形图访问我的通用设备时，没有反应。	通用设备通过设备的 IP 地址直接被访问。如果 IP 地址已修改(例如，由于 DHCP 修改)，那么点击旧 IP 地址将不会连接在新地址的设备。请确定设备的新 IP 地址并相应地修改其设置。

问题	解决操作
不能找到我要添加的设备。	1. 确保 CC2000 管理器在运行，且所有服务已成功启动。 2. 确保在设备的 ANMS 设置中，已启用 CC 管理并正确指定。
当添加 Cat 5e KVM 切换器时，可同时添加所有端口吗？	是的 – 只要所有端口连接了 KVM 适配器，且它们的设备在线。详情请见第 96 页的注意。
端口的图标说明端口在线，但是它所属的设备的图标说明它离线。不能访问设备或端口。	这说明设备的固件不支持 CC2000 的这个版本。将设备的固件更新为最新版本。
连接我的 CC2000 从服务器的设备不出现在主服务器的 Available Devices 列表。	1. 检查设备是否已被添加。如果是，它不出现于列表。 2. 点击各从的 Show Available Devices 按钮。 3. 试过步骤 2 后，如果设备不出现，检查设备的 ANMS 设置，以确保已启用 CC 管理，且正确指定您要设备被其识别的 CC2000 的 IP 和端口地址。 4. 试过步骤 2 后，如果设备出现了，则可能有网络问题。执行 Replicate Database to the 主 功能。详情请见第 205 页的*复制数据库*。
我的 ATEN/Altusen 设备不被 CC2000 识别。	1. 问题设备可能不被 CC2000 管理系统支持。关于支持的设备列表，见第 243 页的*支持 CC2000 的 ATEN IP/Altusen 产品*。 2. 设备的固件必须被更新为最新版本，以便能够运行 CC 管理。
进行设置修改后，点击 Save，**HTTP Status 500 – error** 页出现。	您可能在输入设置时出错。这是 Apache Tomcat 错误信息，当 Apache Tomcat 接收毫无意义的设置时，此信息出现。要恢复运作，选择任何其它选项卡，然后回来进行修改 – 请确保输入有效设置。
设置 CC2000 进行“No timeout”操作，但它却超时注销。	此修改直到您下次登录时才生效。

Q1：当我打开一个浏览器时，网络页不显示或不正常运行，且我收到类似如下的错误信息：



1. 重置IE安全设置，以启用Active Scripting、ActiveX controls和Java applets。

   通过默认，IE6和IE5.x的一些版本为Restricted Sites Zone采用“高”安全等级设置，而Microsoft Windows Server 2003为Restricted Sites Zone和Internet Zone两者都采用“高”安全等级设置。您可能要启用Active Scripting、ActiveX controls和Java applets。要启用Active Scripting、ActiveX controls和Java applets，请遵循如下步骤：

   a) 启动IE。
   b) 在Tools菜单，点击Internet Options。
   c) 在Internet Options对话框，点击Secuity。
   d) 点击Default Level。
   e) 点击OK。

2. 核实Active Scripting、ActiveX controls和Java applets未受阻。

   如果有些电脑运行，有些不运行，则核实您电脑上的IE或其它程序，如杀毒程序或防火墙，未设定为阻塞Scripts、ActiveX controls和Java applets。

3. 核实您的杀毒程序未设置成扫描Temporary Internet Files或Downloaded Program Files文件夹。

4. 删除所有与Internet相关的临时文件。

   要从您的电脑删除所有与Internet相关的临时文件，请遵循如下步骤：

   a) 启动IE。

   b) 在Tools菜单，点击Internet Options。

   c) 点击General选项卡。

   d) 在Temporary Internet files下，点击Settings。

   e) 点击Delete Files。

   f) 点击OK。

   g) 点击Delete Cookies。

   h) 点击OK。

   i) 在History下，点击Clear History，然后点击Yes。

   j) 点击OK。

5. 确保您安装了最新版本的Microsoft DirectX。

   关于如何安装最新版本Microsoft DirectX的信息，请访问如下微软网站：

   http://www.microsoft.com/windows/directx/default.aspx?url=/windows/directx/downloads/default.htm

6. 确保您安装了最新版本的Java JRE。

   关于如何安装最新版本Java JRE的信息，请访问Java网站：www.java.com。

此页刻意留白

附录 B
CC2000 工具

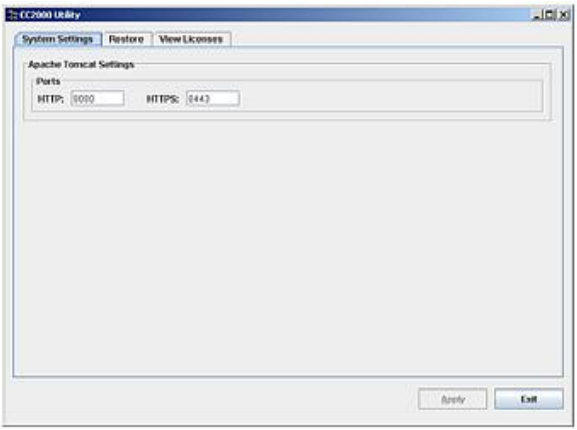
概述

CC2000工具作为CC2000安装操作的一部分安装。它允许您从CC2000运行的电脑桌面设定大量CC2000参数，而无需激活浏览器GUI。

在Windows中，要运行此程序，打开*Start*菜单；导航至CC2000条目(Programs → CC2000)，然后选择CC2000 Utility(CC2000工具)：

在Linux中，作为系统管理员，到**/home/CC2000/Runable**目录，然后运行CC2000_Utility文件。

当您运行此程序时，一个类似如下的窗口出现：



此工具提供三个选项卡：*System Settings* (系统设置)；*Restore* (恢复)；和*View Licenses* (浏览许可证)。各选项卡在下面的部分描述。

系统设置

Apache Tomcat是服务CC2000网络页的程序。CC2000的安装程序要您指定Apache Tomcat监听网络请求的端口。

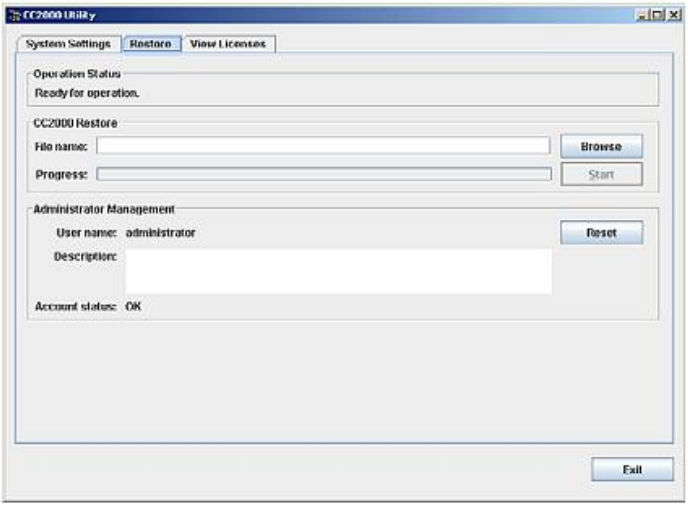
- *HTTP*是Apache Tomcat监听的常规端口。默认为80。如果您使用不同的端口，用户必须在其浏览器的URL中指定此端口号。
- *HTTPS*是Apache Tomcat监听的安全端口。默认为443。如果您使用不同的端口，用户必须在其浏览器的URL中指定此端口号。

如果您设置的端口发生端口冲突，且不能打开网页，您可以用此工具修改端口设置。

完成设置后，点击**Apply**以保存修改。

恢复

点击Restore选项卡，打开一个类似如下的对话框：

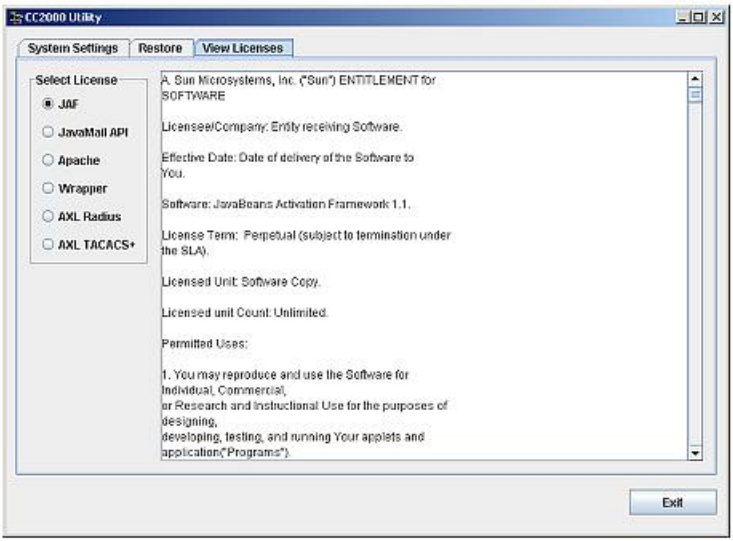


对话框分为三个面板，如下表所描述：

面板	描述
Operation Status (操作状态)	您可以使用此面板检查 CC2000 服务是否正常运行。
CC2000 Restore (CC2000 恢复)	此项用来将 CC2000 的主服务器数据库恢复为以前保存的版本(见第 192 页的*备份主服务器数据库*)。点击 **Browse** 以导航到文件所在位置。选择文件后返回对话框后，点击 **Start** 以开始操作。操作的进度显示在 *Progress* 区。
Administrator Management (管理员管理)	点击 **Reset** 则将默认的系统管理员的帐户返回至默认值(administrator / password)。如果此帐户被锁定(见第 161 页的*锁定策略*)，其自动解锁。

浏览许可证

View Licenses选项卡让您浏览与CC2000包装相关的许可证。要浏览某许可证，点击其单选按钮。

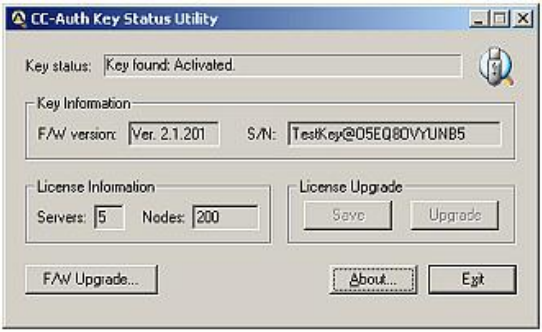


附录 C
验证密钥工具

概述

验证密钥工具(CCAuthKeyStatus.exe)是访问和更新包含在CC2000验证密钥中的信息和数据的程序。*CCAuthKeyStatus.exe*可在CC2000包装附带的CD上找到。

当您运行此程序时，一个类似如下的窗口出现：



密钥状态信息

窗口的三个部分提供关于密钥状态的信息：

部分	用途
Key Status (密钥状态)	告知您密钥是否被找到以及它是否被激活。如果密钥未被找到，或未被激活，请联系经销商。
Key Information (密钥信息)	显示密钥的当前固件版本和序列号。
License Information (许可信息)	显示密钥许可的服务器的数量(主和从)和节点的数量。
License Upgrade(许可更新)	这些按钮用来执行离线许可升级。
F/W Upgrade(固件更新)	这个按钮是用来升级认证密钥的固件。

密钥工具

License Upgrade和F/W Upgrade部分提供允许您更新密钥固件(F/W Upgrade)及更新许可证授权的服务器数和节点数(License Upgrade)的工具。许可证更新将在以后的版本中被执行。

密钥固件更新

CC2000验证密钥的固件可以更新。当新固件版本发行时，更新文件被发布到我们的网站。请定期查看网站，以找到与之相关的最新文件和信息。

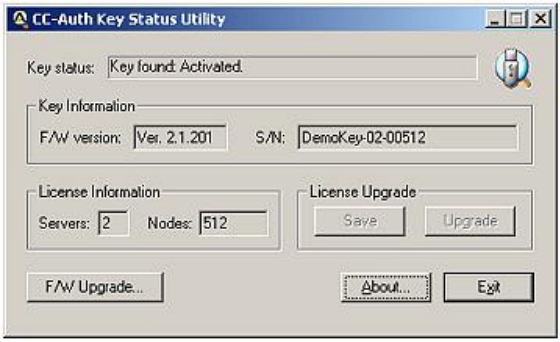
开始更新

更新您的固件，请按如下操作：

1. 到我们的网站，下载新固件文件到您电脑上的方便位置。
2. 插入验证密钥，运行*密钥状态工具*(CCAuthKeyStatus.exe)。

> **注意：** 1. *CCAuthKeyStatus.exe* 仅在 Windows 下运行。
> 2. *KeyStatus.exe* 可在 CC2000 包装附带的 CD 上找到。应将此文件拷贝到您电脑上的方便位置。

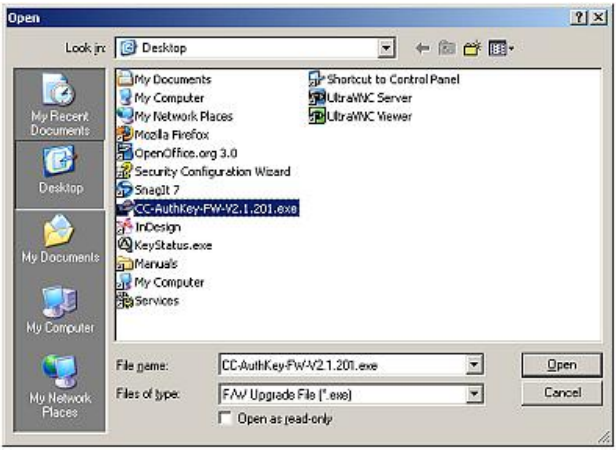
3. 在出现的窗口，点击**F/W Upgrade...**



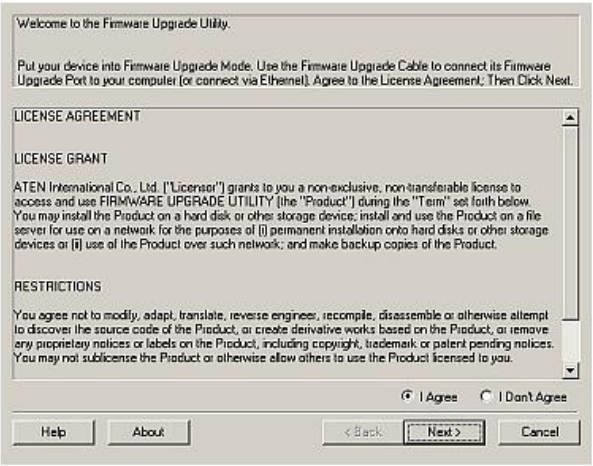
(续下页)

(接上页)

4. 在出现的*File Open*对话框，选择固件更新文件，然后点击**Open**。



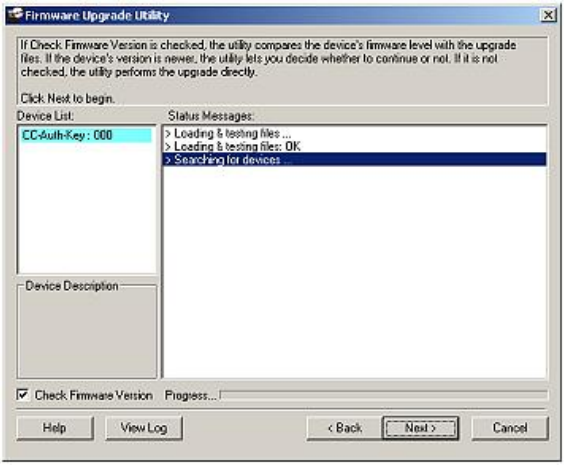
5. 阅读并*同意*许可证协议(启用*I Agree*单选按钮)。



(续下页)

(接上页)

6. 工具搜索您的设备。当找到您的设备时，它将其列于*设备列表*面板。



注意：如果启用了 *Check Firmware Version*，工具比较设备的和更新文件的固件级别。如果发现设备的版本比更新版本高，它打开一个对话框，通知您这种情况，并请您选择 Continue (继续)或 Cancel (取消)。

如果未启用 *Check Firmware Version*，工具安装更新文件，而不检查其级别。

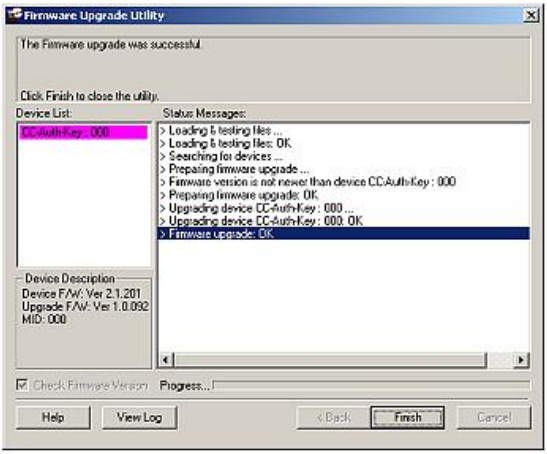
点击**Next**以继续。

(续下页)

(接上页)

更新成功

更新完成后，一个对话框出现，通知您更新成功：



点击**Finish**以关闭固件更新工具。

密钥许可更新

概述

CC系列有一项功能，允许最终用户（客户端）更新自己的认证密钥，以反映增加了他们的许可数量。 密钥许可升级可以由客户或由经销商/分销商来执行，可以通过因特网浏览器会话（在线升级），或通过一个独立的实用程序（离线升级）。

客户先通知其经销商/分销商要升级的许可数量。经销商/分销商然后与Altusen销售代表下订单，指定添加的许可数量。订单处理后，Altusen销售代表发送一个确认和授权电子邮件给经销商/分销商，执行升级的必要细节。

注意：每个密钥必须以单独的订单进行处理。

以下有2种方式更新密钥：

- **在线**：执行升级的钥匙插入在计算机的USB端口和一个浏览器会话中打开直接升级的关键。 如果在客户端进行升级，经销商/分销商为他提供了电子邮件授权细节;如果经销商/分销执行升级时，客户端提供了他与认证密钥。
- **离线**：基于Windows的密钥状态工具用于提取密钥的信息，并将其写入到一个密钥信息的数据文件。 然后密钥信息数据文件在一个浏览器会话产生许可升级文件。许可升级文件生成后，密钥状态工具再次使用该升级文件的信息写入许可证密钥。

在线更新

客户联系其经销商订下单更新。每一个订单必须有单独的密钥。经销商与Altusen销售代表完成更新订单后，会受到一封确认和授权邮件，类似于下面的例子：

> 您的订单已经准备处理。请前方http://xxx.xxx.x.xxx更新您的密钥许可证。
>
> 登入信息：
>
> - 用户名: myname2
> - 密码: mypassword5678
>
> 订单信息：
>
> - 订单ID：1017000700（认证编号：2068919892）。此订单要求新增7台服务器和20500节点。

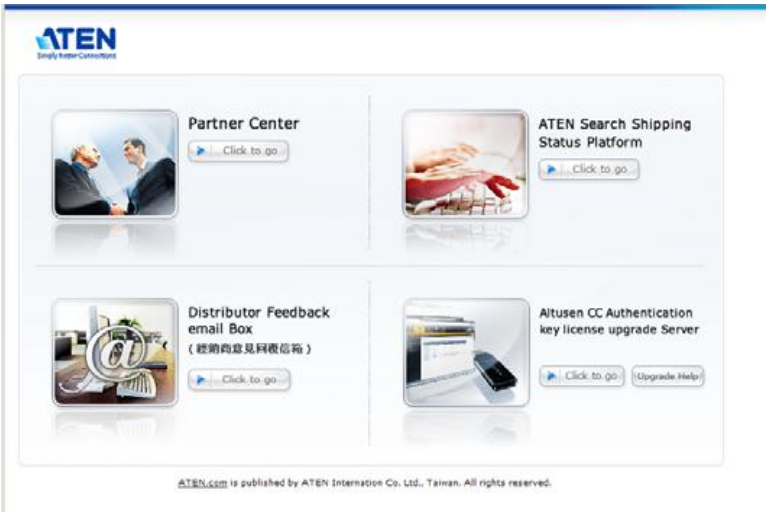
客户和经销商都可以执行更新。如果经销商执行，客户要向经销商提供许可证密钥；如果客户执行，供销商要将确认邮件发给客户。

如要执行在线更新，按下述操作：

1. 将认证密钥插入电脑的USB端口。
2. 打开浏览器，并登入到电子邮件中提到的网址。

> **注意**：如有要求，接受证书。

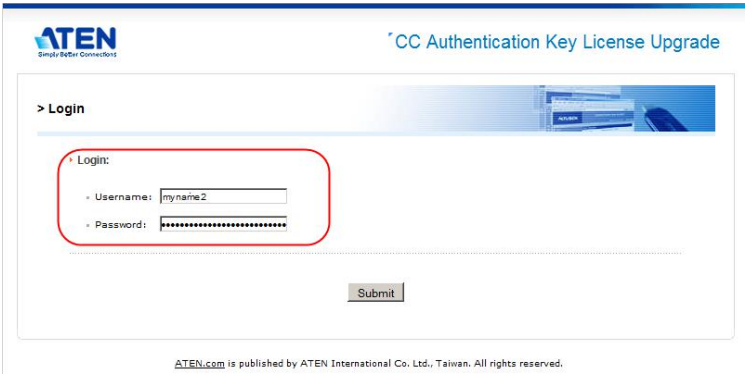
ATEN *合作伙伴中心*页面 出现。



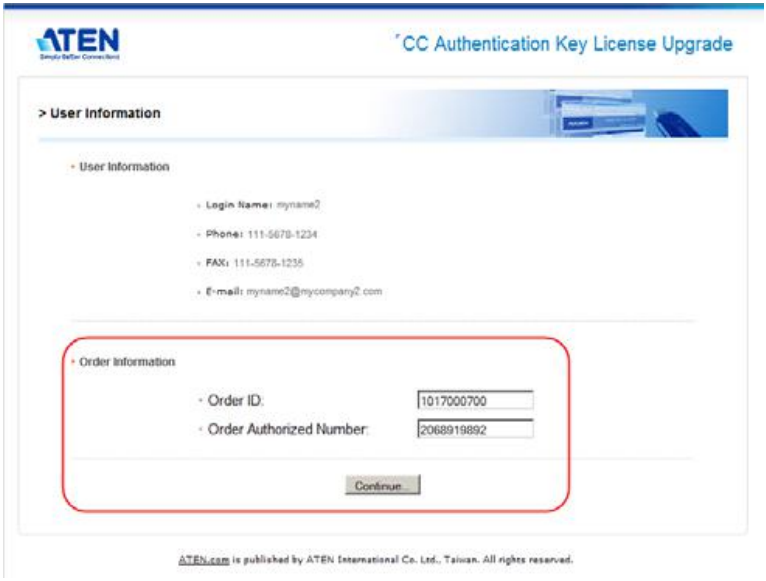
3. 密钥许可证更新面板位于右侧下方。单击**Click to go**（单击访问）按钮开始更新程序。

注意：1. 您可以单击*Upgrade Help*（更新帮助）按钮打开在线帮助，执行更新。
2. 如有要求，接受证书。

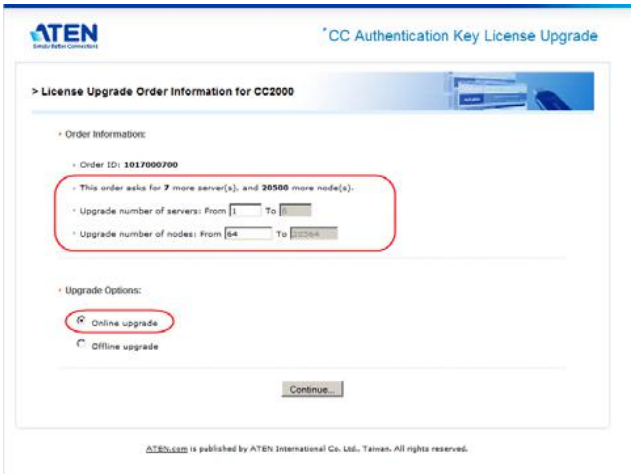
4. 更新登入页面出现后，用认证邮件中提到的用户名和密码登入。



5. 在出现的界面里，输入适用更新的订单ID号和订单认证号，然后单击**Continue**（继续）。

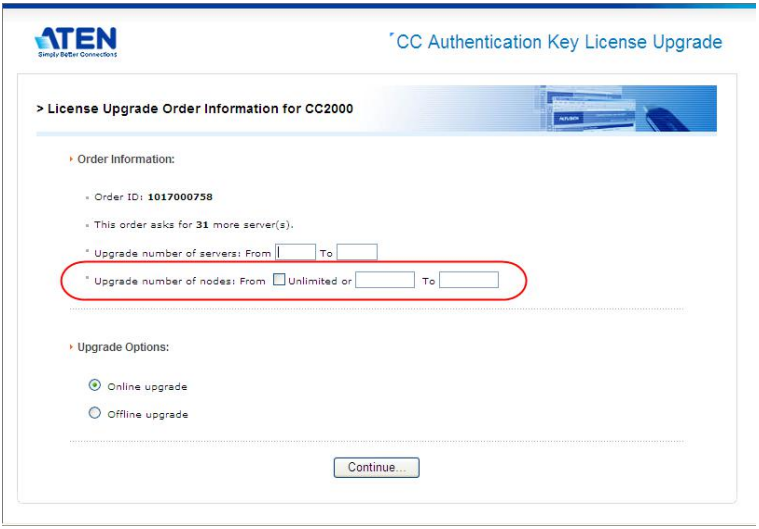


6. 在证书更新订单信息界面，在From字段输入当前的证书编号（To字段会被自动填入），然后选择**Online upgrade**（在线更新）。



注意：您可以使用密钥状态工具（CCAuthKeyStatus.exe）查看当前许可证编号。

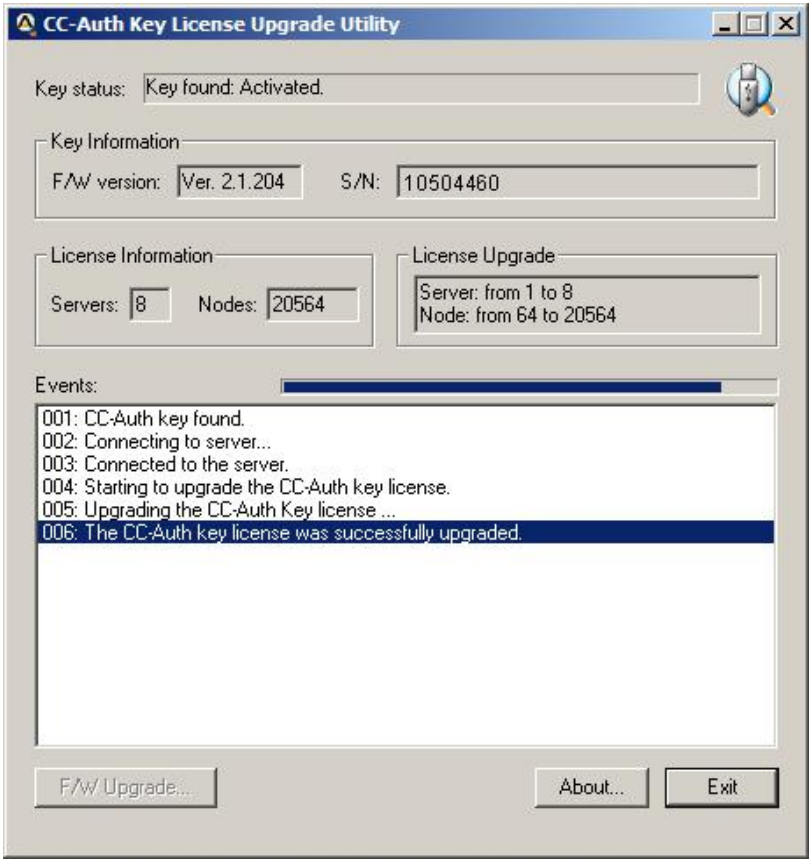
如果只更新服务器许可证，更新订单信息页面类似于下图。如果节点许可证已经被设置为*unlimited*（无限制）,勾选复选框；否在需要在From字段填写适当的节点编号：



7. 单击**Continue**（继续）。
8. 经销商的CC认证密钥许可证更新画面出现后，单击**Download**（下载）。
9. 当浏览器询问如何对文件（KeyUpgrade.exe）执行操作时，选择*Save to dis*（保存到磁盘）。
10. 不要关闭浏览器；前往文件下载的位置并打开文件。

注意：本步骤必须在下载KeyUpgrade.exe文件的同一网页会话完成。否则更新不会成功。

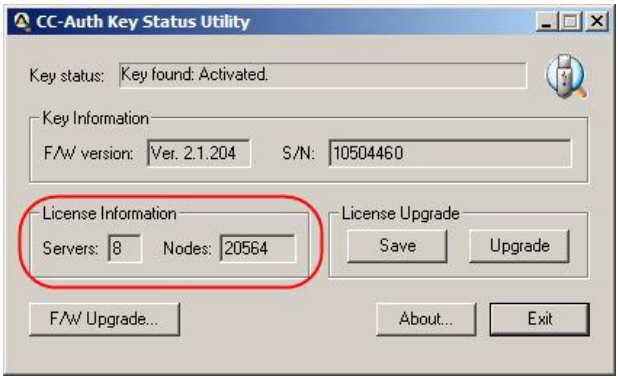
更新工具出现并开始更新。执行的操作在主面板中报告：



11. 更新完成后，会弹出一个窗口，通知您更新成功。单击**OK**关闭弹窗。浏览器屏幕会提供更新总结：

12. 单击**Logout**（注销）退出。

您可以使用密钥状态工具（CCAuthKeyStatus.exe）确认密钥上的许可证已经改变，以证实更新成功：



更新成功

更新成功后，经销商会从Altusen受到一封电子邮件，通知其更新已经在线完成。例如：

您的订单（订单ID：1017000700）已经通过在线工具成功完成。

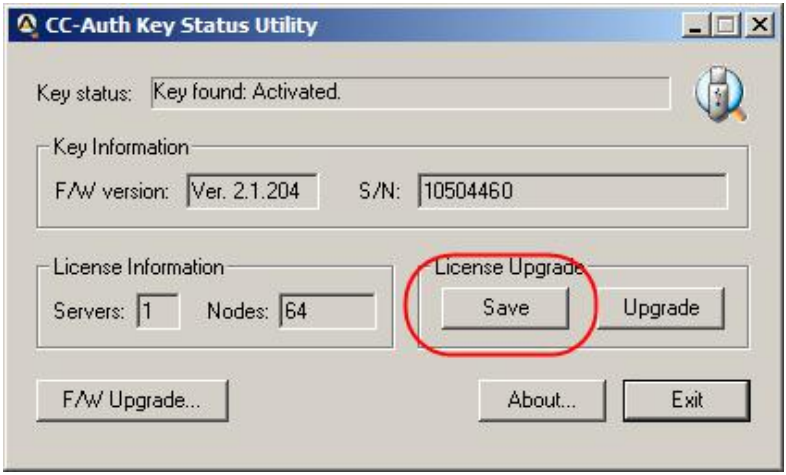
密钥：（PSN：10504460）服务器数量已经从1更新到8，节点数量从64更新到20564.

离线更新

离线更新可由经销商或终端用户客户执行。此种更新方式的好处是，客户不必放弃使用密钥，只需将密钥信息数据文件通过电子邮件发送给经销商，并收到密钥更新文件回馈。

准备步骤

1. 插入认证密钥后，执行*密钥状态工具* 。
2. *许可证更新* 面板对话框出现，单击**Save**（保存）创建一个*密钥信息数据文件*（KeyUpload.dat）。



注意：密钥信息数据文件要在密钥状态工具的同一目录下创建。

密钥信息数据文件创建后，客户需要将其发送给经销商。

执行更新

当经销商/分销商把把更新订单交与销售Altusen代表后，他们会收到一封确认和授权电子邮件，例如：

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

Login Information:

- Username: myname3
- Password: mypassword3

Order Information:

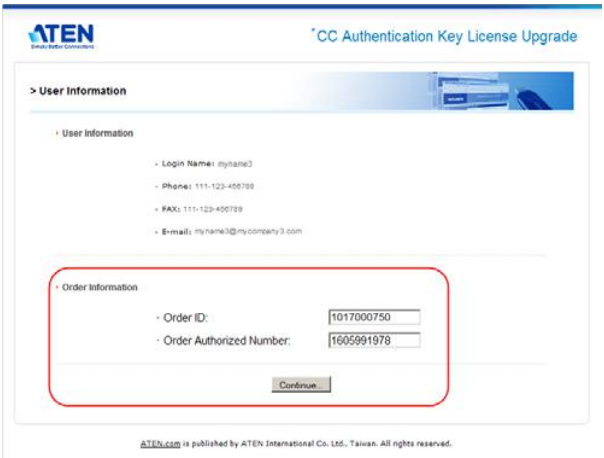
- Order ID: 1017000750 (authorized number: 1605991978). This order requests 1 more server(s) and 448 more node(s)

请按如下操作执行更新：

1.请按照在线更新的步骤1-3(详见第269页)

2.当出现登录画面时，请输入授权邮件里提供的用户名和密码。

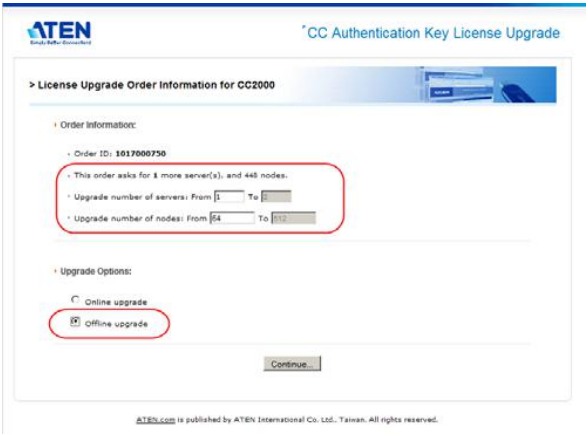
3. 在出现的画面中，输入适用更新的订单ID编号和订单认证编号，然后单击 **Continue**（继续）。



4. 许可证更新订单那信息画面出现后，在*From* 字段输入当前的许可证编号。*To* 字段会被自动填充。

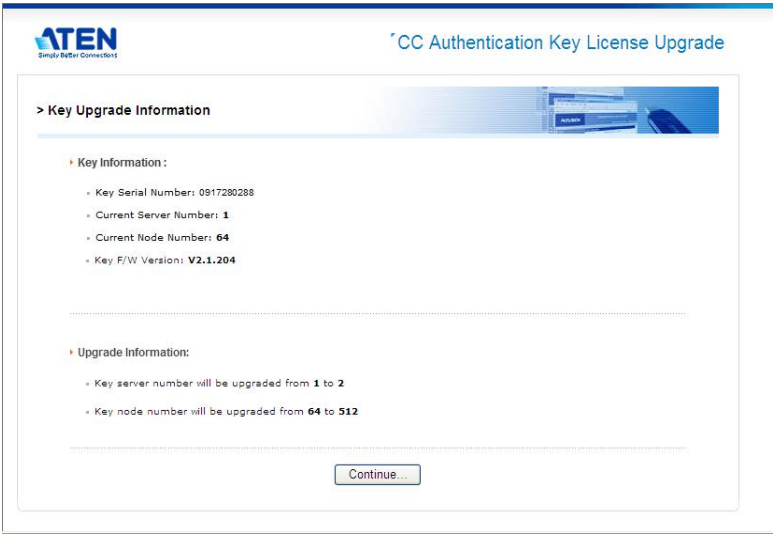
注意：如有必要，您可以使用密钥数据工具（CCAuthKeyStatus.exe）查看当前许可证编号。

5. 选择此为离线更新，然后单击**Continue**（继续）。



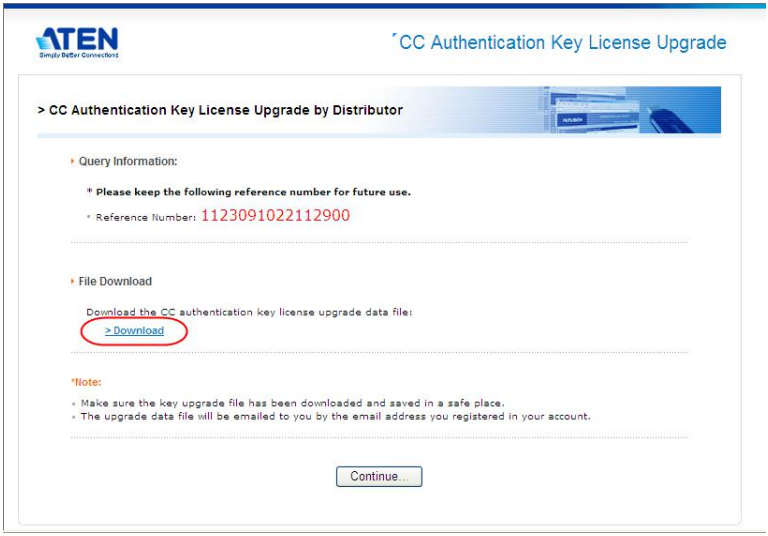
6. 更新密钥信息画面出现后，单击**Browse**（浏览）；加载*准备步骤* 中生成的KeyUpload.dat文件；然后单击**Continue**（继续）。

7. 出现的下一个画面总结更新进展。



单击**Continue**继续。

8. 在接下来出现的湖面里，单击**Download**下载密钥许可证更新数据文件（KeyUpgrade.dat）。



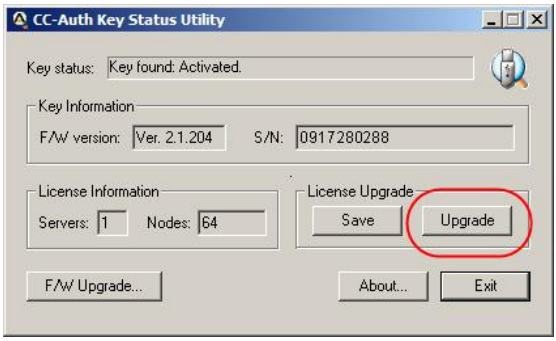
9. 当浏览器询问如何处理密钥更新文件时，选择*Save to disk*（保存至磁盘）。
10. 在出现的确认弹窗中单击**Yes**。出现一个订单总结页面。
11. 单击**Logout**（注销）退出。

注意：1. 如果要更新多个密钥，您可以重新命名KeyUpgrade.dat文件以便区分（保留*dat* 扩展名）。

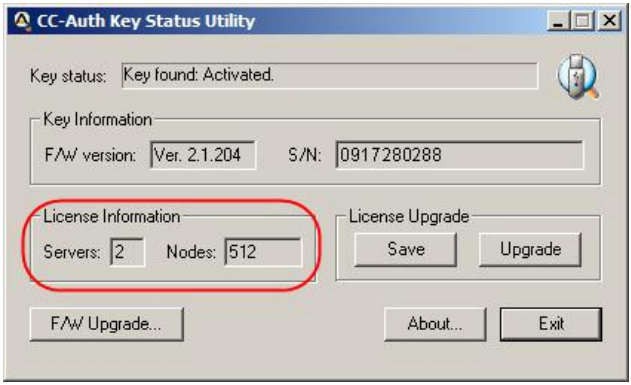
2. 如果客户执行更新，经销商需向客户提供KeyUpgrade.dat文件。

12. 再次运行*密钥状态工具* 。

13. 在许可证更新界面，单击**Upgrade**（更新）。



14. 在出现的对话框中，找到更新文件（KeyUpgrade.dat）并选择。
    - 单击**Open**（打开）后，会弹出一个窗口，说明更新成功。
    - 许可证信息界面的许可证编号数字改变，说明更新成功。



离线更新失败

如果离线更新失败，可能因为密钥更新文件（KeyUpgrade.dat）在文件传送过程中崩溃。有两种方式：

- 下载密钥更新文件后，经销商会受到一封邮件，包含细节以及更新文件的副本，以防原始文件传送出现问题 – 如下面的例子：

  离线更新电子邮件回应：

  附件为您的CC认证密钥。请使用附件中的文件更新您的CC-Auth密钥。

  密钥信息：

  *固件版本：2.1.204

  *序列号：0917280288

  许可证更新信息：

  *并发服务器从1台更新到2台

  *并发节点从64个更新到512个

  确认信息：

  *用户名：newname

  *密码：1123091022112900

  如果您有任何关于更新CC认证密钥许可证的问题，请使用上述用户名和密码登入http://xxx.xxx.x.xxx在线确认。

  您可以重复步骤11（运行密钥状态工具）和12（单击更新）- 此次使用经销商邮件附件中的密钥更新文件（KeyUpgrade.dat）副本。

- 如果上述方法没有解决问题，*离线邮件更新回应* 中的信息可以用于在线更新。经销商向终端用户提供认证细节，或者终端用户向经销商提供密钥。

订单过期

Altusen向经销商发送确认/认证邮件通知其订单准备处理时，有两周时间可以执行订单。如果在这段时间订单未被处理，客户将收到两封邮件，提醒客户订单仍未发送：

1. 您的订单将于一周后过期……
2. 您的订单将于一天后过期……

如果订单在截止日期时仍未被处理，将有一封最终邮件，提醒经销商订单过期，如下：

您的订单已经过期并被取消……

如果您仍希望添加许可证，您必须重新下订单。

此页刻意留白

附录 D
外部验证服务

概述

除了自己内部的*用户/密码*验证程序，CC2000还支持外部验证，即第三方验证服务。如果为用户指定了第三方服务，CC2000用加密的HTTPS (SSL)连接，将登录信息转移到正确的服务进行验证。CC2000支持如下第三方外部验证服务器：LDAP、LDAPS、Active Directory、RADIUS、TACACS+和Windows NT Domain。

被核准的服务

如下服务已被测试并核准可与CC2000搭配使用：

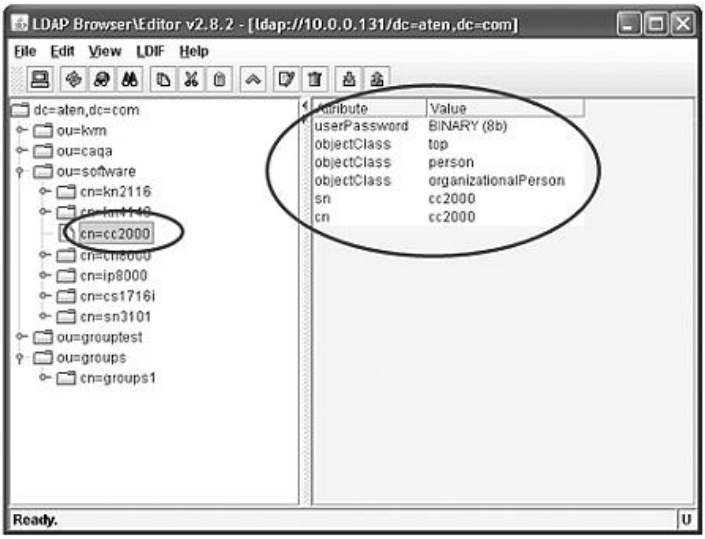
- AD Server：Microsoft Windows Server 2003
- LDAP：Microsoft Windows Server 2003；OpenLDAP
- RADIUS：针对Windows Server 2003的Microsoft IAS；FreeRADIUS
- TACACS+：Microsoft Windows Server 2003 (ClearBox)
- Microsoft Windows NT Domain

LDAP/LDAPS – OpenLDAP 设置示例

在本示例中，外部服务器采用OpenLDAP；它的IP地址是192.168.10.100；它的服务端口是389，且服务器管理员已在OpenLDAP目录中创建了一个名称为*cc2000ldap.ldif*的文件，其包含如下内容：

```
dn: cn=cc2000,ou=software,dc=aten,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
cn: cc2000
sn: cc2000
userPassword: password
```

LDAP管理员可以用LDAP浏览器检查LDAP定义。他应该看到类似如下的窗口：



CC2000管理员得到此信息以用于*添加外部验证服务器*操作中(见第77页的*LDAP/LDAPS*)。在本示例中，各区将填写如下信息：

IP：192.168.10.100

Port：389

BaseDN：dc=aten,dc=com

UserRDN：ou=software

Key attribute：cn

Object class：person

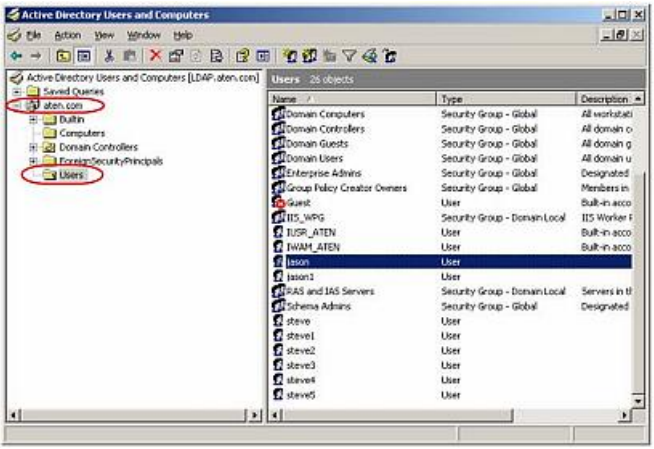
Full name attribute：sn

LDAP/LADPS验证服务器被添加后，CC2000管理员可以用Browse按钮，浏览*software*目录中的所有用户名。

Active Directory 设置示例

在本示例中，外部服务器是Windows Server 2003系统上的Active Directory；它的IP地址是192.168.10.100。请按如下设定Windows Server 2003中的Active Directory：

1. 打开Start → Control Panel → Administrative Tools → Active Directory Users and Computers → Domain (本例中是aten.com) → Users。一个类似如下的窗口出现：



CC2000管理员得到此信息以用于*添加外部验证服务器*操作中(见第78页的*Active Directory*)。在本示例中，各区将填写如下信息：

IP：192.168.10.100

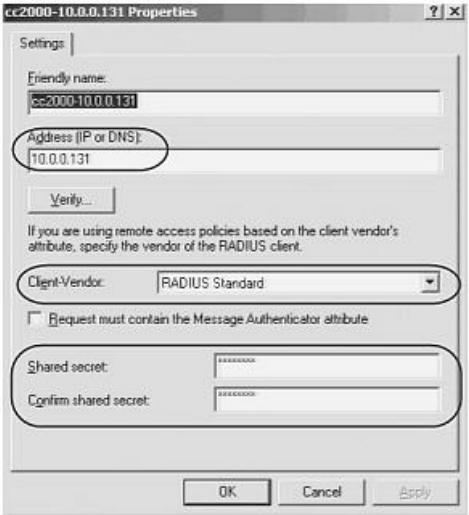
UserRDN：cn=users

Active Directory验证服务器被添加后，CC2000管理员可以用Browse按钮，浏览*Users*目录中的所有用户名。

RADIUS 设置示例

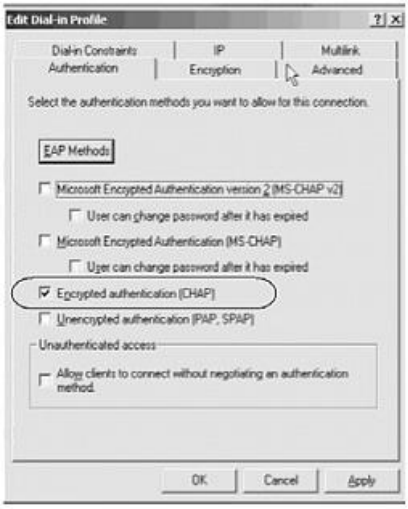
在本示例中，外部服务器是RADIUS：Windows Server 2003的Microsoft IAS；它的IP地址是10.0.0.100。请按如下设定RADIUS：

1. 打开Start → Control Panel → Administrative Tools → Internet Authentication Services。
2. 在出现的窗口，右击**RADIUS Client**。
3. 选择**New RADIUS Client**。
4. 在出现的窗口，键入*名称*。例如：cc2000-10.0.0.131，然后点击**Next**。一个类似如下的窗口出现：



5. 在本示例中，CC2000的IP是*10.0.0.131*；Cient-Vendor是*RADIUS Standard*。对于*Shared secret*，用**password**。
6. 点击OK后，您返回到Internet Authentication Services窗口。在左面板，点击**Remote Access Policies**；在主面板右击**Use Windows authentication for all users**；选择*Properties*。

7. 在出现的窗口，点击**Edit Profile**按钮，然后选择**Authorization**选项卡。一个类似如下的窗口出现：



8. 在本示例中，我们使用CHAP进行加密授权。

CC2000管理员得到此信息以用于*添加外部验证服务器*操作中(见第138页的*RADIUS和TACACS+*)。在本示例中，各区将填写如下信息：

IP：10.0.0.100

Authentication type：CHAP

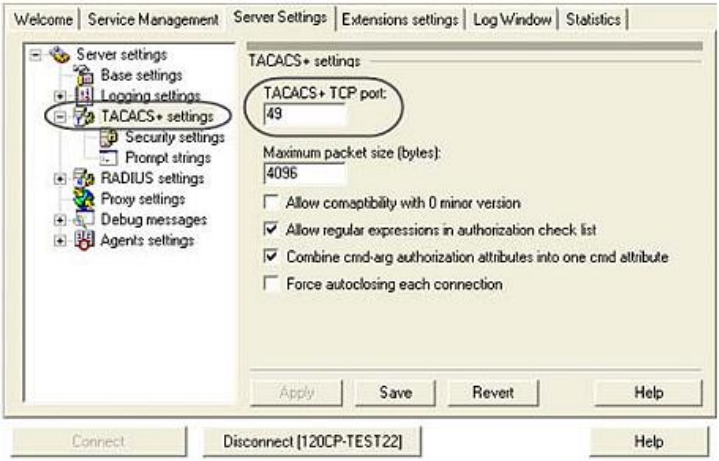
Shared secret：password

RADIUS验证服务器被添加后，当CC2000管理员添加用户帐户时，他必须使用在RADIUS服务器上、在Open Start → Control Pane l → Administrative Tools → Computer Management → Local Users and Groups → Users for the Login names下设定的名称。

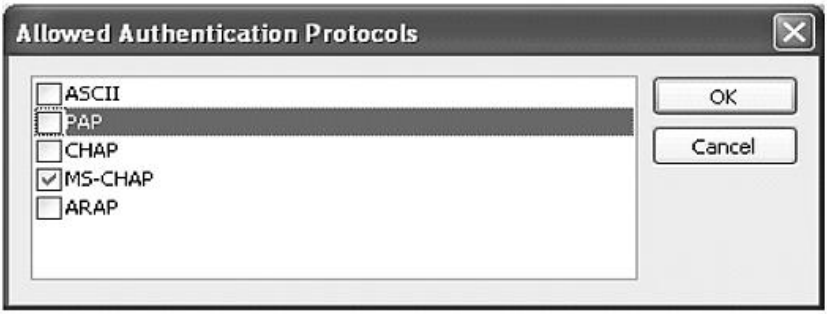
TACACS+设置示例

在本示例中，外部服务器是TACACS+：Windows Server 2003 (ClearBox)的Microsoft IAS；它的IP地址是10.0.0.100。请按如下设定TACACS+：

1. 打开Start → All Programs → ClearBox RADIUS TACACS+ Server → Server Manager。
2. 在出现的窗口，右击**Connect**。
3. 键入当您安装ClearBox RADIUS TACACS+ Server时设置的密码。
4. 在出现的*ClearBox Server Configurator*窗口，选择**Server Settings**选项卡。一个类似如下的窗口出现：



5. 在本示例中，TACACS+服务端口是49.
6. 打开Start → All Programs → ClearBox RADIUS TACACS+ Server → Configurator。
7. 在出现的窗口，在左面板，选择Realms → def；然后选择**Authentication**选项卡。
8. 点击**Allowed Protocols...**按钮。一个类似如下的窗口出现：



9. 在本示例中，我们使用**MS-CHAP**进行允许的验证操作。
10. 您返回到*ClearBox Server Configurator*窗口。在左面板，选择Data Sources → users。
11. 在出现的窗口的主面板，有一个MS Access输入区，其带有一个指定*general.mdb*文件的路径。包含在此区的帐户是通过MS Access生成的。

CC2000管理员得到此信息以用于*添加外部验证服务器*操作中(见第78页的*RADIUS和TACACS+*)。在本示例中，各区将填写如下信息：

IP：10.0.0.100

Port：49

Authentication type：MSCHAP

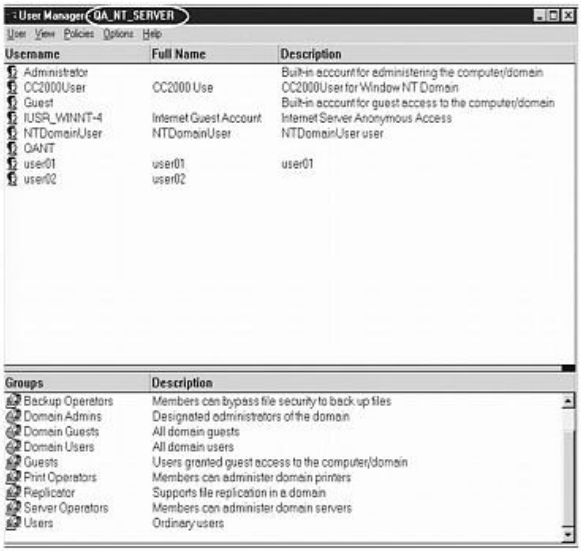
Shared secret：the password that you set when you installed the ClearBox RADIUS TACACS+ Server

TACACS+验证服务器被添加后，当CC2000管理员添加用户帐户时，他必须使用在TACACS+服务器上的*general.mdb*文件中设定的名称。

NT Domain 设置示例

在本示例中，外部服务器是Microsoft Windows NT Domain；它的域名是QA_NT_SERVER。请按如下设定NT Domain：

打开Start → Programs → Administrative Tools (Common) → User Manager for Domains。一个类似如下的窗口出现：



CC2000管理员得到此信息以用于*添加外部验证服务器*操作中(见第139页的*Windows NT Domain*)。在本示例中，各区将填写如下信息：

Domain name：QA_NT_SERVER

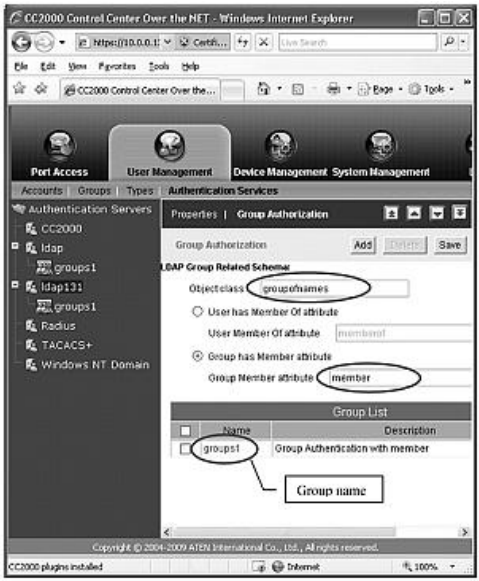
NT Domain服务器被添加后，当CC2000管理员添加用户帐户时，他必须使用在*User Manager for Domains*下设定的名称。

LDAP 群组授权设置示例

示例 1

在本示例中，外部服务器是在第195页的LDAP/LDAPS设置示例中显示的Windows Server 2003的OpenLDAP；

1. 在CC2000 User Manager选项卡下，选择Authentication Services → Authentication Servers。
2. 选择OpenLDAP服务器；然后点击**Group Authorization**。
3. 点击*Group has Member attribute*单选按钮。
4. 点击**Add** (在面板右上方)。
5. 在本示例中，要添加**groups1**群组。一个类似如下的窗口出现：



OpenLADAP管理员用此名称(此示例中的*groups1*)，在OpenLDAP之下，按如下步骤创建一个群组，群组的名称与在CC2000服务器上创建的群组名称相同：

1. 打开*core.schema*文件。我们关注的默认设置如下：

   attributetype (2.5.4.31 NAME '***member***'

   DESC 'RFC2256: member of a group'

   SUP distinguished Name)

   objectclass (2.5.6.9 NAME '***groupOfNames***'

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

   SUP top STRUCTURAL

   MUST (***member*** $ cn)

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

2. 编辑*cc2000ldap.ldif*文件以为groups 1添加一个定义，并使cc2000用户帐户处在groups 1之后，按如下编辑：

   dn: cn=***groups1***,ou=groups,dc=aten,dc=com

   objectclass: ***groupofnames***

   member: cn=***cc2000***,ou=software,dc=aten,dc=com

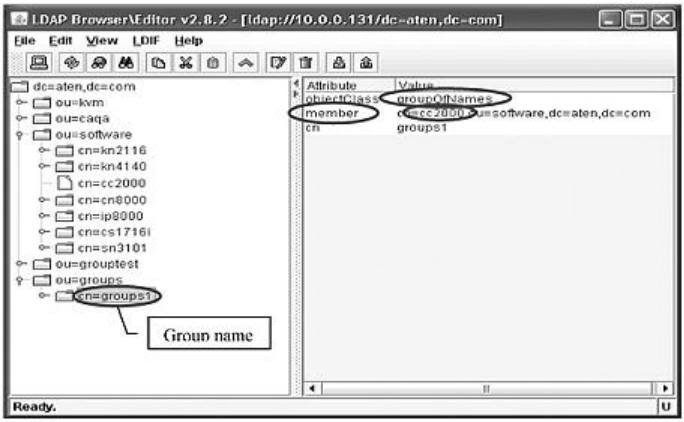
   cn: ***groups1***

注意：1. dn: cn=之后的输入应该是创建在 CC2000 服务器上 Group Authorization 之下的实际群组名称(见第 82 页的*群组授权*)。

2. objectclass:之后的输入应该与在 CC2000 服务器上创建群组时为 Object class 输入的名称一致。修改此文件中的默认条目以与之一致。

3. *member: cn*=之后的输入应该是实际用户登录名。

3. 您可用LDAP浏览器检查群组定义。您应该看到类似如下的窗口：



4. 上述示例已添加了一个成员 – cc2000 – 到groups 1群组。要添加其他成员到群组，请编辑文件以包括这些成员。例如：

   member: cn=***cc2000-1***,ou=software,dc=aten,dc=com

   member: cn=***cc2000-2***,ou=software,dc=aten,dc=com

一旦完成这些操作，通过了LDAP/LDAPS服务器验证的CC2000用户，根据分配给群组的权限被授权。

示例 2

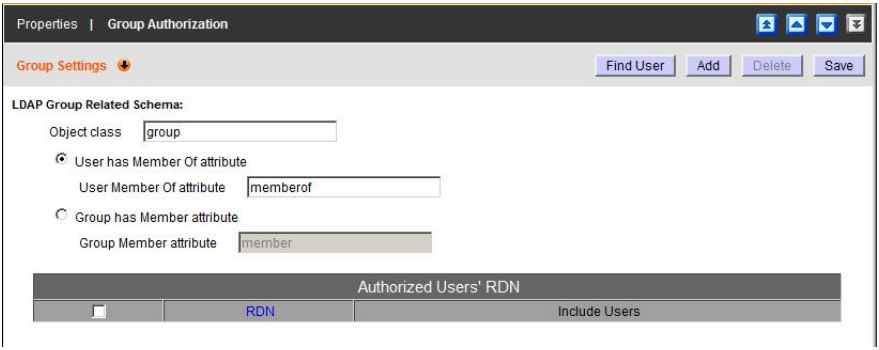
通过默认，OpenLDAP仅为与群组相关的架构支持*Group has Member attribute*设置 – 这是在示例1中使用的设置。

其它LDAP服务器使用的替代设置 – *User has Member Of attribute* – 也可通过延伸架构在OpenLDAP下被支持。

在本示例中，外部服务器是在第283页的LDAP/LDAPS设置示例中显示的Windows Server 2003上的OpenLDAP。

1. 在CC2000 User Manager选项卡下，选择Authentication Services → Authentication Servers。
2. 选择OpenLDAP服务器；然后点击**Group Authorization**。
3. 点击*User has Member Of attribute*单选按钮。

4. 点击**Add** (在面板右上方)。
5. 在本示例中，添加**groups1**群组。窗口应该看起来类似如下：



OpenLDAP管理员用此名称(此示例中的*groups1*)，在OpenLDAP之下按如下步骤创建一个群组，群组的名称与在CC2000服务器上创建的群组名称相同：

1. 打开*core.schema*文件。按如下延伸架构：

```
attributetype ( 1.2.840.113556.1.2.102
    NAME 'memberof'
    DESC 'RFC2256: member of a group'
    SUP distinguishedName )
objectclass ( 1.2.840.113556.1.5.9
    NAME 'person'
    SUP organizationalPerson
    STRUCTURAL
    MUST ( cn )
    MAY ( userPassword $ description $ sn $ mail $ memberof ) )
```

2. 编辑*cc2000ldap.ldif*文件，以添加一个用户帐户到*groups1*群组，按如下编辑：

   dn: cn=***cc2000test***,ou=software,dc=aten,dc=com

   objectclass: top

   objectclass: ***person***

   objectclass: organizationalPerson

   cn: cc2000test

   sn: cc2000test

   memberof: cn=***groups1***,ou=groups,dc=aten,dc=com

   userPassword: password

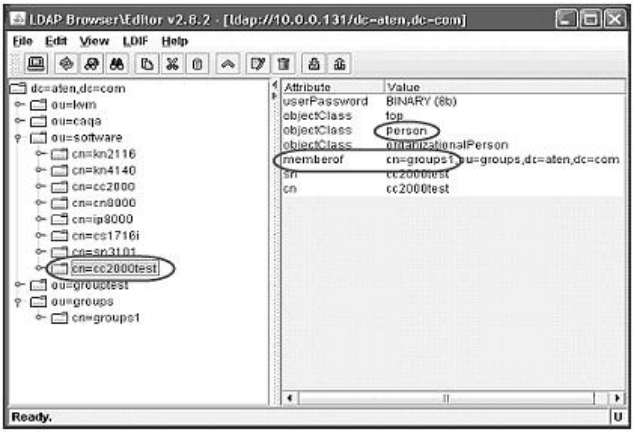
注意： 1. dn: cn=之后的输入应该是实际用户登录名。

2. objectclass:之后的输入应该与在被延伸的架构中为 NAME 输入的名称一致。

3. memberof: cn=之后的输入应该是创建在 CC2000 服务器上 Group Authorization (见第 82 页的*群组授权*)之下的实际群组名称。。

---

3. 您可用LDAP浏览器检查群组定义。您应该看到类似如下的窗口：



4. 为您要添加到群组的各用户帐户重复步骤2。

一旦完成这些操作，通过了LDAP/LDAPS服务器验证的CC2000用户，根据分配给群组的权限被授权。

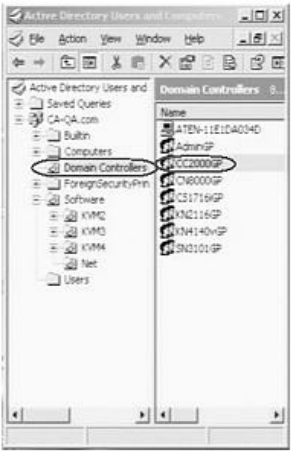
Active Directory 群组授权设置示例

在本示例中，外部服务器是在第285页Active Directory设置示例中显示的Windows Server 2003上的Active Directory；

1. 在CC2000 User Manager选项卡下，选择Authentication Services → Authentication Servers。
2. 选择Active Directory服务器；然后点击**Group Authorization**。
3. 在本示例中，要添加**CC2000GP**群组。

Active Directory管理员用此名称(此示例中是**CC2000GP**)，在Active Directory之下按如下步骤创建一个群组，群组的名称与在CC2000服务器上创建的群组名称相同：

1. 打开Start → Control Panel → Administrative Tools → Active Directory Users and Computers → Domain (此示例中是CA-QA.com)。
2. 在左面板，右击**Domain Controllers**；选择**New**；选择**Group**。
3. 在出现的对话框，键入群组的名称(此示例中是CC2000GP)。一个类似如下的窗口出现：



4. 在右面板，右击**CC2000GP**；选择**Properties**；选择**Members**。一个类似如下的窗口出现：

5. 点击**Add**。

出现的对话框让您添加成员到群组。从在*Users*文件夹(见先前窗口的左面板)找到的帐户中选择成员。

MOTP 设定

有关MOTP服务器和设置的详细信息，请使用以下链接或二维码：

www.aten.com/CC2000-OTP

如需设置SMTP服务器的帮助信息，请参考CC2000登录页的OTP文件。