CommandCenter®

NOC

Administrator Guide

Release 5.4

CCNOC-0D-E
June 2006
255-80-5301-00

This page intentionally left blank.

Copyright and Trademark Information

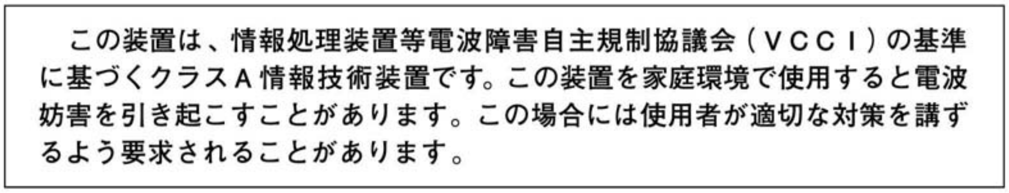
This document contains proprietary information that is protected by copyright. All rights reserved. No part of this document may be photocopied, reproduced, or translated into another language without express prior written consent of Raritan Computer, Inc.

© Copyright 2006 Raritan, CommandCenter, RaritanConsole, Dominion, and the Raritan company logo are trademarks or registered trademarks of Raritan Computer, Inc. All rights reserved. Java is a registered trademark of Sun Microsystems, Inc. Internet Explorer is a registered trademark of Microsoft Corporation. Netscape and Netscape Navigator are registered trademarks of Netscape Communication Corporation. All other marks are the property of their respective owners.

FCC Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

Japanese Approvals



この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, non-Raritan modification of the product, or other events outside of Raritan's reasonable control or not arising under normal operating conditions.

For assistance in the North or South America, please contact the Raritan Technical Support Team by telephone (732) 764-8886, by fax (732) 764-8887, or by e-mail tech@raritan.com

Ask for Technical Support – Monday through Friday, 8:00am to 8:00pm, Eastern.

For assistance around the world, please see the last page of this guide for regional Raritan office contact information.

Safety Guidelines

To avoid potentially fatal shock hazard and possible damage to Raritan equipment:

- Do not use a 2-wire power cord in any product configuration.
- Test AC outlets at your computer and monitor for proper polarity and grounding.
- Use only with grounded outlets at both the computer and monitor. When using a backup UPS, power the computer, monitor and appliance off the supply.

Default Login User ID/Password

The default username for CC-NOC is **admin** and the password is **raritan**. It is recommended to change this immediately.

Rack Mount Safety Guidelines

In Raritan products which require Rack Mounting, please follow these precautions:

- Operation temperature in a closed rack environment may be greater than room temperature. Do not exceed the rated maximum ambient temperature of the appliances (see **Appendix A: Specifications**).
- Ensure sufficient airflow through the rack environment.
- Mount equipment in the rack carefully to avoid uneven mechanical loading.
- Connect equipment to the supply circuit carefully to avoid overloading circuits.
- Ground all equipment properly, especially supply connections, such as power strips (other than direct connections), to the branch circuit.

Contents

Figures

Chapter 1: Introduction

The primary function of a CommandCenter NOC (CC-NOC) is to manage nodes in your network. Nodes are discovered automatically if their IP address is within the managed range of addresses. In addition to network discovery, a CC-NOC also provides service management, a database of network information, a rules engine, a notification engine, and a web server. A CC-NOC can also be instructed to collect statistics from your Windows systems, monitor network traffic for intrusion attempts and bandwidth performance, and scan your systems for vulnerabilities.

Within this document, the term "CC-NOC" refers to the following models:

- CommandCenter NOC 100
- CommandCenter NOC 250
- CommandCenter NOC 2500N
- CommandCenter NOC 2500M
- CommandCenter NOC 2500S

All configuration tasks are performed on a CC-NOC 100, CC-NOC 250, or CC-NOC 2500N.

Note: *When information is related to a particular model, it will be explicitly noted.*

Stand-alone Appliances

A CC-NOC can operate in a stand-alone environment where the appliance itself provides complete functionality, for example, network discovery, polling, windows management, traffic analysis, vulnerability scanning, and intrusion detection on one box.

These CC-NOC appliances can operate in a stand-alone environment and typically are deployed in smaller networks or satellite offices:

- CC-NOC 100
- CC-NOC 250

For instructions on deploying and configuring a CC-NOC 100 or CC-NOC 250, see Raritan's *CommandCenter NOC Deployment Guide*.

Distributed 2500 Series Appliances

A CC-NOC can also operate in a distributed environment where the functionality, for example, network discovery, polling, windows management, traffic analysis, vulnerability scanning, and intrusion detection is dispersed among different appliances. These CC-NOC appliances can operate in a distributed environment:

- CC-NOC 2500N: Used for configuration of other appliances, network discovery, polling, vulnerability scanning, and outages.
- CC-NOC 2500M: Used for Windows Management.
- CC-NOC 2500S: Used for Intrusion Detection and Traffic Analysis.

For instructions on deploying and configuring a CC-NOC in a distributed environment, see Raritan's *CommandCenter NOC Deployment Guide*.

Note: *A CC-NOC 2500N can be deployed by itself without a CC-NOC 2500M or CC-NOC 2500S if the functionality offered by those appliances is not needed.*

CommandCenter Secure Gateway (CC-SG)

A CC-SG provides single-point access and control for managed Raritan devices, target servers and infrastructure devices. A CC-NOC can be deployed in conjunction with a CC-SG. Please see Raritan's *CommandCenter Secure Gateway Administrator Guide* for initial instructions on how to configure the CC-SG to register for CC-NOC events and to enable the exchange of notifications between the two appliances.

User PC Preparation

To access CC-SG and any targets managed by CC-SG, the browser must have the correct version of Sun JRE, such as rev 1.4.2.05. See **Compatibility Matrix** under **Firmware Upgrades** for CC-SG on www.raritan.com/support for details.

For CC-SG, pop-up blockers should be disabled as well as any firewall software such as XP SP2 that is enabled by default.

Remote Authentication

CC-NOC users can be authenticated remotely by CC-SG to provide an enhanced seamless mode of operation and Single Sign-on (SSO) access to CC-SG targets. With one-click access to CC-SG and SSO access to targets, a CC-NOC user can move easily between systems.

Mapping of User Groups

With remote authentication, all CC-NOC logins will be securely routed to and resolved by CC-SG for remediation. The CC-NOC receives the CC-SG user groups the CC-NOC user is a member of and maps these groups to any of its local groups, that is, Admin, User, Executive. If a user belongs to more than one group, the highest privileged group will be used. When a CC-NOC user accesses a CC-SG target, the access rights, permissions, and policies are based on their user group membership.

***Note**: Before mapping the groups on CC-NOC, the user groups must have already been created on CC-SG or imported from an external authentication server, such as Active Directory.*

Local Authentication

By default, CC-NOC users will be locally authenticated if remote authentication is not configured. Local authentication is also used if remote authentication is configured but the CC-SG is unavailable or if the password was incorrect.

If "local authentication" is used, then CC-NOC users will have to login to CC-SG to gain access to targets. They will be prompted for a CC-SG login and password, which will be checked against the local CC-SG user database.

***Note**: The **admin** account on CC-NOC is always authenticated locally, regardless where all other users are authenticated.*

Intended Audience

Three types of users (Administrator, User, Executive User) can access CC-NOC. This document is intended for users who assume an **Administrator** role. Administrators perform configuration tasks on a CC-NOC 100, CC-NOC 250, or CC-NOC 2500N, such as configuring intrusion detection, windows management, vulnerability scans, etc. Tasks that are available to users with a **User** or **Executive User** role are described in Raritan's *CommandCenter NOC User Guide*, which describes tasks such as viewing intrusion detection events, window management events, etc. Administrators can also perform all tasks that are available to a User or Executive User.

Features Described in this Document

These features are covered in the following chapters:

- Remote Device Monitoring and Polling (automatic discovery of devices, servers, workstations)
- Single device Discovery
- Traffic Analysis
- Intrusion Detection
- Windows Management of Servers, Workstations via Windows Management Instrumentation (WMI)

- Vulnerability Scanning
- Event Viewing and Searching
- Performance Monitoring per category or device
- Integration with CC-SG where CC-SG is notified of events within the subscribed discovery range.
- Scheduled Outages
- User, Views, and Category Configuration
- License Upload
- Event, Outage Notification
- Asset Management
- Reports (Outage, Availability, Inventory, Delta Inventory, Vulnerability, Security, SNMP)
- Tools – Network Tools (ping host, port test, trace route to host, profile route to host)
- Tools – Admin Tools (export & download configuration files, download log files, check disk utilization, send incident report, generate diagnostics file)
- Advanced Admin - Support Tools (Appliance Health, Restore to Factory Defaults, Backup/Restore Capabilities)

Terminology/Acronyms

Terms and acronyms found in this document include:

- **Assets** – capital assets in an organization can be tracked. Tracking your assets is useful for keeping abreast of equipment repairs as well as network or system related moves, additions, or changes. Asset inventory tracking facilitates generating on-demand reports of hardware and software to enable greater productivity, financial accountability, and end-user satisfaction. Asset records can be created manually, imported from a pre-existing list, and exported to a CSV file for Excel record keeping. Assets can also be associated with a discovered node in your network.
- **CommandCenter Secure Gateway (CC-SG) –** single-point access and control for your managed Raritan devices, target servers, and other network infrastructure devices connected to CC-SG.
- **CSV** – comma-separated value files are simple database files that can be easily imported into a spreadsheet or database program so that you can generate custom reports. This export functionality is available from any view of the Event Browser.
- **DHCP** – (Dynamic Host Configuration Protocol). A TCP/IP protocol that dynamically assigns an IP address to a computer.
- **DNS** – (Domain Name System). An Internet service that translates domain names into IP addresses.
- **Duty Schedule** – is a schedule that reflects a user's work hours. When a duty schedule is defined for a user, notifications will be sent to that user only if it occurs within the time frame that is specified in the duty schedule.
- **Events** – events include SNMP traps which can be forwarded to third-party tools (HP OpenView). Events also are generated by components of the Windows operating system and are recorded in the Events log, for example, Netlogin service, login failures, Windows Installer. Events are records of significant occurrences in your network, on your systems, or within the CC-NOC. An event is either outstanding, that is, not addressed nor acknowledged. The Events Browser allows you to gain insight as to what is going on in the network, whether it is network management, intrusion detection, or Windows management. Events have severities – critical, major, warning, normal, cleared, or indeterminate. Intrusion Detection Events have categories, for example, successful admin privilege gain, and Denial of Service. Events can be exported in a CSV format for Excel. When an event is triggered, it can send a notification to a recipient if configured for that recipient. Events can be queried and the queries can be saved. A CC-NOC allows you to threshold events as well.

- **ICMP –** (Internet Control Management Protocol) ICMP is used by the CC-NOC to discover devices in your network and is documented in RFC 792.
- **In-band –** going through the TCP/IP network to control a target by accessing the target directly. KVM, Serial, and Generic devices can be accessed via these in-band applications: **RemoteDesktop Viewer**, **SSH Client**, **VNC Viewer**.
- **Intrusion Detection** – monitors and analyzes system events for attempts to access system resources in an unauthorized manner.
- **Inventory** – see Assets.
- **NetBIOS** – Network Basic Input/Output System is a program that allows applications on different computers to communicate within a local area network. It was created by IBM for its early PC Network, later adopted by Novell and Microsoft. NetBIOS is used in Ethernet, token ring and Windows NT networks. It does not support a routing mechanism, so applications communicating on a wide area network must use another "transport mechanism" (such as TCP/IP) rather than, or in addition, to NetBIOS.
- **Network Management** – proactively monitors, collects, and maintains all devices and services on a network.
- **Notices** – see Notifications.
- **Notifications** – a notice that is sent to one or more recipients via email, pager, etc. and is based on an event being triggered. A CC-NOC provides default notifications. You can control the content of a notification message. A CCNOC evaluates each event against the configured notifications rules and if it matches one or more rules, a notification is sent. To receive a notification, a user has to be added to a notification group. Notices can be outstanding or acknowledged.
- **NFS** – (Network File System) Standard for accessing files on a remote computer appearing as a local volume.
- **Outage** – instances where successive attempted polls of a given service have timed out and a “node lost service” event was created. Each entry is assigned a unique Outage ID, a sequential numeric identifier to uniquely identify a given outage. That ID, coupled with the node label for the node experiencing the outage, the address of the impacted interface, the service name, and the time the outage occurred are all tracked within the Outages Browser. At the onset of an outage, all calculations for reporting purposes, for example, Availability calculations in the Web Console and Availability Report reflect the current service as down until a future poll is successful. When a service experiencing an outage is successfully polled, a “node regained service” event will terminate the outage and assign an “Up” date and timestamp, which is used as the end of the outage for service level availability calculations.
- **Out-of-band** – using applications such as Raritan Remote Console (RRC), Raritan Console (RC), or Multi-Platform Client (MPC) to correct or troubleshoot a KVM or serial managed target in your network**..**
- **Pollers** – programs that collect service information from infrastructure devices and servers, for example, web, NTP, and email and create *service down* messages.
- **Port Scan** – is the probing for openings and availabilities in a network. Attackers generally use port scanning utilities to probe targets and make a list of all open ports on a device. They will send specific attacks to open ports hoping to exploit a vulnerability on the target. Port scanning is detectable by monitoring traffic on the target machine. Scan Level 1 Vulnerability Scanning uses port scanning methods to search target systems for open ports. However, normal and legitimate activity, such as DNS and NFS, often resembles the activity of an attacker executing a port scan against a target and may produce false-positive port scan events. Those servers performing those services should be excluded from port scanning activity.
- **Proxy host** – a system that facilitates connectivity between the CC-NOC and your managed Windows servers and workstations. The proxy forwards WMI data from the servers and workstations to the CC-NOC.
- **Signature** – a fingerprint of network traffic that signals an attack.
- **SMB** – (Server Message Block) The communications protocol used by Windows-based operating systems to support sharing of resources across a network to discover systems.

- **SSO** – Single Sign-On. With Single Sign-on (SSO) access to CC-SG targets, CC-NOC users can connect to targets seamlessly, without having to sign onto CC-SG as long as remote authentication has been configured.
- **System Vulnerabilities** – unpatched systems, older known vulnerable server daemons on your system that can be exploited by harmful network traffic.
- **TAP** – (Telocator Alphanumeric Protocol) A standard protocol enabling modems to send text messages to pager systems. The CC-NOC can use TAP services to send notifications as text messages to pagers.
- **Users** – a CC-NOC has these three types of users:
  Administrators who have configuration access to the machine.

  Users who have access to everything on a CC-NOC except administrative configuration.

  Executive Users who have read-only access to only a few key reports that show the network health at a high level.
- **Views** – the combination of categories, for example, Database Servers, Routers, Email Servers, and Network Interfaces that users will see when logging into a CC-NOC. Views are customizable and provide a way to map users to the categories that they are most interested in.
- **Vulnerability Scan** – the CC-NOC can be configured to scan for vulnerabilities, for example, unpatched systems and older known vulnerable server daemons within a network. Harmful traffic can be exploited by intruders to gain access to restricted information, can alter the flow of data through your network, or even disable important services on your network. Vulnerability scanning provides this type of information about your network devices—detection and diagnosis of vulnerabilities, deep detection of all open ports and services, and logging of all available information that may benefit intruders. Scanning for vulnerabilities assists administrators in resolving security concerns. For example, an administrator may decide to apply patches and software updates to fix known security holes, shut down unwanted or unnecessary services, remove access to sensitive information in your network, or change security settings and passwords to make them more difficult to crack. For more information on vulnerabilities, including CVE entries, go to http://www.cve.mitre.org.
- **WMI** – (Windows Management Instrumentation) WMI, also known as WBEM, is Microsoft’s technology for providing a consistent systems management interface to their platform.

Licensing Explained

As devices are discovered in your network, data is collected from the device and the device is then assigned a license. License types include Infrastructure, Server, Workstation, and Promoted Workstation. Administrators can change a license from one type to another. The following explains each license type.

Infrastructure

In order for a device to be assigned an infrastructure license, it must be discovered as a node and support one of the following "infrastructure" level services:

FTP	SMTP	Oracle
DHCP	LDAP	Sybase
DNS	MSExchange	Informix
NotesHTTP	Citrix	SQLServer
HTTP-Management	DominoIIOP	MySQL
HTTPS	Router	Server
IMAP	Switch-Hub	POP3
Postgres		

An infrastructure device is eligible for the following functionality:

- Capability scans once every 24 hours for new services and/or inventory information
- Service availability polling
- SNMP performance data collection
- SNMP performance thresholding

You can transition a device with an Infrastructure license to any of the following licensed states:

- Workstation
- Server (if the device is a Windows system which supports WMI)
- Promoted Workstation
- Unmanaged

Server

Only Windows systems which support Windows Management Instrumentation (WMI) are eligible to be assigned a Server license. In addition to supporting WMI, the system must be a server system based on its operating system role retrieved via WMI to be auto-licensed as a server.

A server device is eligible for the following functionality:

- Capability scans once every 24 hours for new services and/or inventory information
- Service availability polling
- SNMP performance data collection
- Windows performance data collection
- SNMP performance thresholding
- Windows performance thresholding

You can transition a device with a Server license to any of the following licensed states:

- Workstation
- Infrastructure (if the device is a node)
- Promoted Workstation
- Unmanaged

Workstation

A Workstation license can be assigned to any type of device, be it a Windows or non-Windows system. For example, a Linux box which is discovered as a node and which does not support any of the infrastructure services will be assigned a Workstation license. Similarly, a desktop Windows system will be assigned a Workstation license.

A workstation device is eligible for the following functionality:

- Capability scans once every 24 hours for new services and/or inventory information

You can transition a device with a Workstation license to any of the following licensed states:

- Server (if the device is a Windows system which supports WMI)
- Infrastructure (if the device is a node)
- Promoted Workstation
- Unmanaged

Promoted Workstation

Promoted Workstation licenses provide a mechanism for you to obtain additional polling and performance data from a troublesome device on a temporary basis without taking up a Server or Infrastructure license. The only way for a device to be assigned a Promoted Workstation license is to assign the license through the web user interface. There are a total of five promoted workstation licenses available with a CC-NOC appliance.

A promoted workstation device is eligible for the following functionality:

- Capability scans once every 24 hours for new services and/or inventory information
- Service availability polling
- SNMP performance data collection
- Windows performance data collection
- SNMP performance thresholding
- Windows performance thresholding

You can transition a device with a Promoted Workstation license to any of the following licensed states:

- Workstation
- Server (if the device is a Windows system which supports WMI)
- Infrastructure (if the device is a node)
- Unmanaged

Chapter 2: General and Advanced Administration

Power Down CC-NOC

If running CC-NOC on the V1 platform and if it loses AC power while it is up and running, the V1 unit remembers its last power state. Once AC power is restored, the V1 unit automatically reboots. However, if a V1 unit loses AC power when it is turned OFF, the V1 unit will remain powered off when AC power is restored.

Important: Do not hold the POWER button for four or more seconds to forcibly power down CC-NOC, particularly when CC-NOC is up and running. The recommended way to power down CC-NOC is to use the following procedure.

To power down the CC-NOC:

1. Remove the bezel and firmly tap the POWER button.
2. Wait for approximately one minute while CC-NOC gracefully powers down. You can monitor the progress on the console that is attached to the KVM port.
3. If removing the AC power cord, let the power down process completely finish before removing the power cord. This is required for CC-NOC to complete all transactions, close the databases, and place the disk drives into a safe state for power removal.

Appliance Shutdown/Restart

The **System Shutdown** and **System Restart** buttons are one way that your CC-NOC can be shut down or restarted. You can also shutdown and restart a CC-NOC while using a serial connection – see Raritan's *CommandCenter NOC Deployment Guide*. While the CC-NOC is designed to be an appliance, it must store information about your environment in a local database. Thus, it should be treated with the same sensitivity as a database server. Loss of power or hard shutdowns of the device can result in database corruption and data loss.

1. Click on the **Admin** tab in the top navigation bar.
2. Click either **System Shutdown** or **System Restart**.

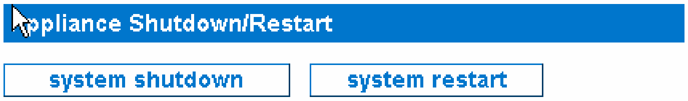


Figure 1 Appliance Shutdown/Restart

Typically, these options are used if you experience a loss of power and need to shutdown the device while still running off a backup energy source. Contact Technical Support if you have additional questions regarding these options or your particular situation.

Appliance Network Settings

These are the network settings that can be revisited since they were initially configured with the serial connection and the First-Time Configuration Wizard – see Raritan's *CommandCenter NOC Deployment Guide*:

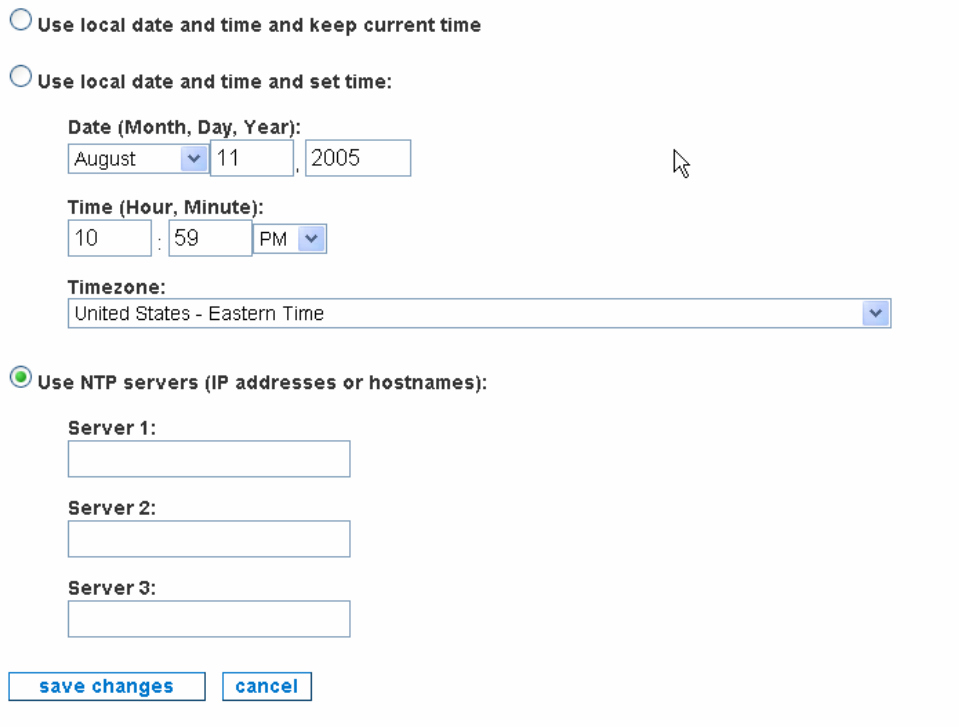
- Date and Time
- Network Connection
- ISP Gateway
- Email Communication
- Nameserver Address

Configure Date and Time

This page allows you to modify the current time zone and set the local time or configure a network time protocol (NTP) server with which to synchronize the local time.

***Note**: If a CC-NOC 250 or 2500N is powered down for more than six hours, upon booting back up, you will be asked to validate if the time settings are correct.*

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Appliance Network Settings**.
3. Click **Configure Date & Time**.



○ Use local date and time and keep current time

○ Use local date and time and set time:

Date (Month, Day, Year): August 11, 2005

Time (Hour, Minute): 10 : 59 PM

Timezone: United States - Eastern Time

● Use NTP servers (IP addresses or hostnames):

Server 1:

Server 2:

Server 3:

Figure 2 Configure Date and Time

4. Click the radio button **Use local date and time and keep current time** to leave the local time as it is.
5. To set the local time on the CC-NOC, click the radio button **Use local date and time and set time**. The time will be reset when you continue to the next step.
6. Click the drop-down arrow and select your **time zone** from the select box. The list is sorted first by country (two character code), then an order within the country that makes some geographical sense, and puts the most populous zones first, where that does not contradict the geographical listing. Please select the zone that is nearest to your location.
7. Click **Use NTP servers** to turn on the NTP client. NTP is a network service that is used to synchronize times between computers on a network. You will be required to provide at least one NTP server if you select this option. If **Use NTP servers** is currently selected and you would like to stop using the NTP client, choose either of the two options above depending on whether or not you want to keep the current time or reset the time.

***Note:** If you select **Use NTP servers**, you should install a NTP server in your environment.*

8. Click **save changes**.

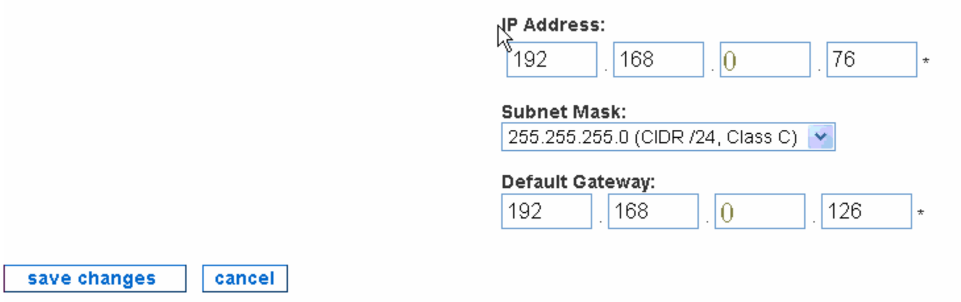
Configure Network Connection

This page allows you to change the fixed IP address associated with this appliance. This IP address was configured when setting up the initial configuration using a serial connection – see Raritan's *CommandCenter NOC Deployment Guide*.

The CC-NOC mimics the traffic generated by a user trying to access various services throughout the network. This mandates that the CC-NOC also has a network address and other supporting information to connect to other network devices. DHCP is *NOT* an alternative, as other devices will always need to know exactly what address the CC-NOC is using.

Note: *Be careful when using this interface as you can render the appliance unreachable via the network by your users as well as by Technical Support.*

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Appliance Network Settings**.
3. Click **Configure Network Connection**.



IP Address: 192 . 168 . 0 . 76 *

Subnet Mask: 255.255.255.0 (CIDR /24, Class C)

Default Gateway: 192 . 168 . 0 . 126 *

Figure 3 Configure Network Connection

4. Type network settings, such as TCP/IP address, network mask, and default gateway.
5. Click **save changes**.

Change the ISP Gateway Address

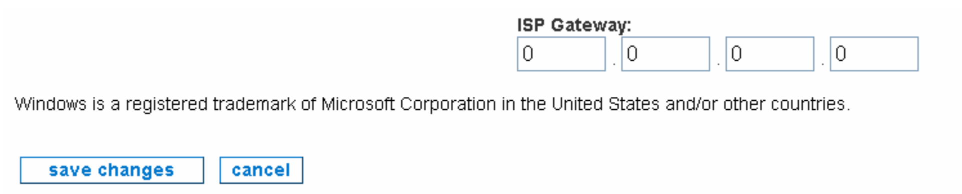
This page provides a way to manipulate the address monitored for inclusion in the Internet Connectivity category. The CC-NOC handles your ISP gateway as a special case. If configured here, your ISP gateway can be monitored for availability and reported on independently. If applicable, specify the TCP/IP address of your gateway. If you do not have this information, your ISP should be able to provide it or you can get it by tracing the route to the internet from a machine on the managed network.

- **UNIX Machine:** Run `traceroute www.yahoo.com` and look for the first TCP/IP address or DNS name that is outside of your local network and appears to belong to your ISP. Consider the possibility of WAN interfaces showing up in this trace.
- **Microsoft Windows Machine:** Run `tracert www.yahoo.com` and look for the first IP address or DNS name that is outside of your local network and appears to belong to your ISP.

Note: *Note that this field is* ***not*** *required. If configured, the ISP gateway takes one infrastructure license. Type an address of* ***0.0.0.0*** *if you do not wish to supply an ISP address.*

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Appliance Network Settings**.

3. Click **Change the ISP Gateway Address**.



ISP Gateway: 0 . 0 . 0 . 0

Windows is a registered trademark of Microsoft Corporation in the United States and/or other countries.

Figure 4 Configure Network Connection

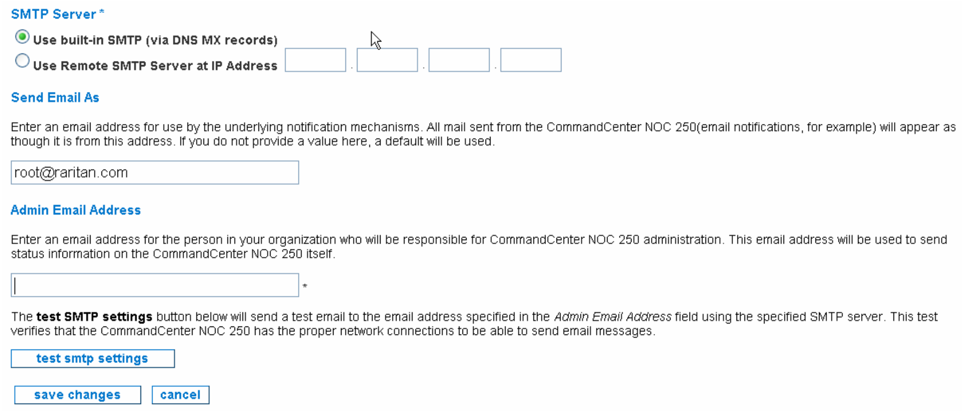
4. Type the IP address of the ISP gateway or type an address of **0.0.0.0** if you do not wish to supply an ISP address.
5. Click **save changes**.

Outgoing Email Communication

This page provides an interface to change the From: email address in notifications, as well as the SMTP relay settings. These settings affect how the CC-NOC communicates with you. Keep the information current and make sure you use valid email addresses to ensure correct status information reaches the administrator.

To send email notifications, the CC-NOC needs to know how to send email. If allowed, the CC-NOC will use its local SMTP service to send email. Some networks, however, will not accept email from unknown sources. If this is the case, please provide the IP address of an SMTP server below.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Appliance Network Settings**.
3. Click **Outgoing Email Communication**.



SMTP Server *

● Use built-in SMTP (via DNS MX records)

○ Use Remote SMTP Server at IP Address . . .

Send Email As

Enter an email address for use by the underlying notification mechanisms. All mail sent from the CommandCenter NOC 250(email notifications, for example) will appear as though it is from this address. If you do not provide a value here, a default will be used.

root@raritan.com

Admin Email Address

Enter an email address for the person in your organization who will be responsible for CommandCenter NOC 250 administration. This email address will be used to send status information on the CommandCenter NOC 250 itself.

*

The **test SMTP settings** button below will send a test email to the email address specified in the *Admin Email Address* field using the specified SMTP server. This test verifies that the CommandCenter NOC 250 has the proper network connections to be able to send email messages.

Figure 5 Configure Outgoing Email Communication

4. To send email notifications, the CC-NOC needs to know how to send email. If allowed, the CC-NOC will use its local **SMTP service** to send email. Some networks, however, will not accept email from unknown sources. If this is the case, provide the IP address of an SMTP Server in the proper field and select the proper Use section.
5. The email address specified in **Send Email As** details the email address the underlying notification mechanisms will use. All mail sent from the CC-NOC, for example, email notifications will appear as though it is from this address. If you do not provide a value here, a default will be used (root@localhost.com).
6. The admin email address specified in **Admin Email Address** should be the email address of the person in your organization who will be responsible for CC-NOC administration. This

email address is a required field and will be used to send status information on the CC-NOC itself.

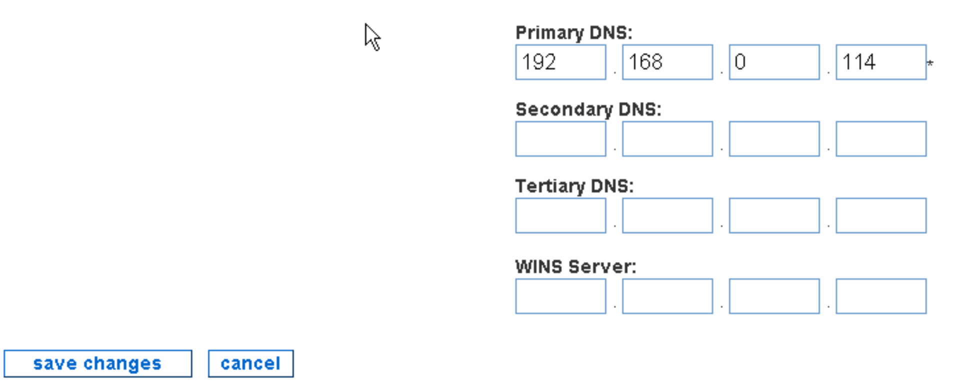
7. Clicking **test SMTP settings** sends a test email to the email address specified in the **Admin Email Address** field using the specified SMTP server. This test verifies that the CC-NOC has the proper network connections to be able to send emails.
8. Click **save changes**.

Change Nameserver Addresses

This page allows you to configure the addresses of your DNS (up to 3) and/or WINS servers. DNS servers allow systems to translate IP addresses into meaningful names. Please type at least one DNS server that the CC-NOC can reach efficiently. Place your fastest local servers near the top of the list.

WINS servers are used in NetBIOS and Windows networking environments to resolve NetBIOS names across subnet boundaries. If you are managing several subnets that contain machines with NetBIOS names and have a WINS server that manages the names of the machines, please type the address of the WINS server in the spaces provided.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Appliance Network Settings**.
3. Click **Change Nameserver Addresses**.



Primary DNS: 192 . 168 . 0 . 114 *

Secondary DNS: . . .

Tertiary DNS: . . .

WINS Server: . . .

Figure 6 Configure Nameserver Addresses

4. Type addresses for primary (required), secondary, tertiary DNS servers, and WINS server.

Note: *The WINS Server that you can specify here is used by a CC-NOC 100, CC-NOC 250, or CC-NOC 2500N. This is a separate WINS server that can be configured for a CC-NOC 2500M – please see* ***Chapter 4: Configuring Windows Management*** *for additional information.*

5. Click **save changes**.

Network Management Configuration

This page allows you to configure features that affect what network devices you manage and how you manage them. Network management proactively monitors, collects, and maintains all devices and services on a network.

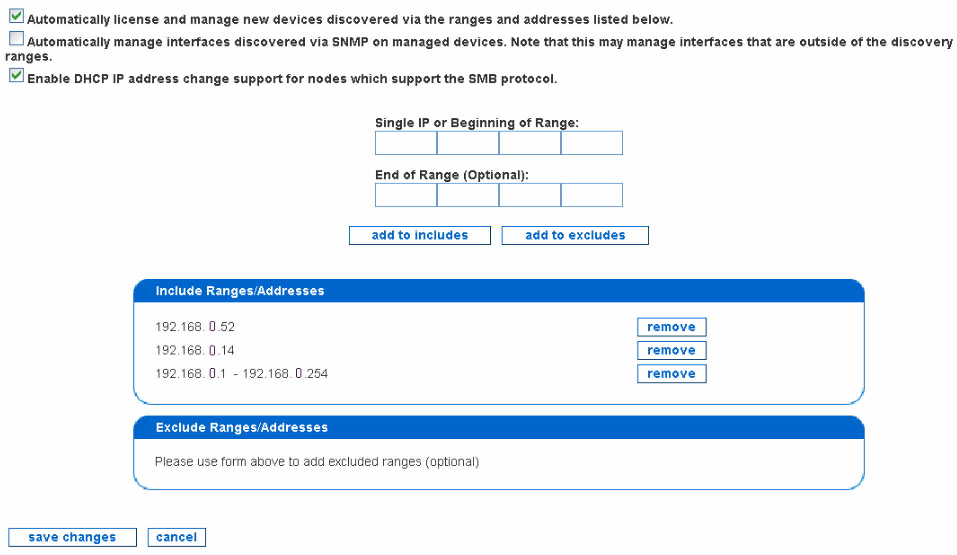
Edit Discovery Ranges

This page allows you to modify your initial configuration settings, see Raritan's *CommandCenter NOC Deployment Guide*, determining which specific addresses or address ranges should or should not be included for discovery. Once discovered, each system is cataloged as either a Server, Infrastructure, Workstation, or Promoted Workstation device. In this page, you can also set a flag that determines whether or not any newly discovered devices are automatically licensed and managed or not. CC-NOC discovers devices via this discovery range, single device discovery – see section **Discover a Single Device** later in this chapter, incoming traps, and through the

WMI management range – see **Specifying Windows Management Ranges** in **Chapter 4: Configuring Windows Management** for details. Typically, you would want the discovery range specified here to overlap with the WMI management range.

Note: *A CC-NOC discovers devices in the network using ICMP protocol. Once discovered, further data (for example, operating system) is collected from the device and the device is then assigned a license, that is, Infrastructure Device license, Server license, or Workstation license.*

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Network Management Configuration**.
3. Click **Edit the Discovery Ranges**.



☑ Automatically license and manage new devices discovered via the ranges and addresses listed below.

□ Automatically manage interfaces discovered via SNMP on managed devices. Note that this may manage interfaces that are outside of the discovery ranges.

☑ Enable DHCP IP address change support for nodes which support the SMB protocol.

Single IP or Beginning of Range:

End of Range (Optional):

Include Ranges/Addresses

192.168. 0.52

192.168. 0.14

192.168. 0.1 - 192.168. 0.254

Exclude Ranges/Addresses

Please use form above to add excluded ranges (optional)

Figure 7 Edit Discovery Ranges

4. Type IP addresses or ranges and click either **add to includes** or **add to excludes**– this will add them to the appropriate list. You can only add one IP or range at a time. If you would like to remove one from the list, click **remove** to the right of its listing. When you are done, click **save changes**. Use these examples:

- To discover a range, type the first address and the last address and click **add to includes**. Ranges may span multiple networks. If there are any ranges or addresses that cannot or should not be discovered, make sure to add an entry to **add to excludes** them – see below. If using CC-SG in conjunction with CC-NOC, this range works with the range configured in CC-SG – see the *CommandCenter Secure Gateway Administrator Guide* for details. To stop CC-NOC from monitoring a device, it can be *unmanaged* – see section **Manage, Unmanage, Rescan, or Delete Devices** in **Chapter 2: General and Advanced Administration**.
- To discover a specific IP address, type the address in "Begin" and leave "End" blank. Click **add to includes** to add it to the list. Typically, these are nodes that fall outside of ranges, like any servers that the company may have co-located off-site.
- To exclude a range, type the first address and the last address and click **add to excludes**. Ranges may span multiple networks. In most cases, you will only specify a range that falls inside of a range you are already including.
- To exclude a specific IP address, type the address in "Begin" and leave "End" blank. Click **add to excludes** to add it to the list. It is recommended to exclude DHCP ranges since they can change IP addresses, which can appear as false outages.

Important! Ensure your discovery range is not too wide, for example, entering multiple Class B address ranges. This consumes large amounts of resources and may reduce the performance of CC-NOC. Also, it is recommended to keep the default "Automatically license and manage new devices discovered via the ranges and addresses listed below" checked. This avoids devices being discovered more than once.

5. Click **Enable DHCP IP address…** for DHCP nodes that support Server Message Block (SMB), the communications protocol used by Windows-based operating systems to support sharing of resources across a network, to discover systems. This protocol tracks the nodes by hostname so if their IP addresses change, it will not generate false outages.

***Note**: Excludes take priority over Includes. Therefore, if you have an Included range inside an Excluded Range, the Included range will not be read as included (as you have already excluded it). To avoid this problem, limit Excluded ranges - example: You have one Server that has an IP address within a subnet you are not managing. Instead of excluding the whole range and including that one IP address, build two (2) Exclude lists - one up to that address, and another starting with the address immediately preceding and going to the end of that range*

Example

You can, however, exclude specific IP addresses within an Included range - say for a specific Server you do not want managed. For example, you include this range of IP addresses: 192.168.0.1 to 192.168.0.255. Within that range, you can specify one IP address we do not want managed (192.168.0.210). You also included a specific IP outside of the range we specified (192.168.5.100) to manage. This is a good setup. Where you might run into trouble is if you excluded a range of IPs that covered the specific IP we listed (say excluding 192.168.5.10 to 192.168.5.150), since the CC-NOC will exclude that range before it includes the specific address you want to manage.

Edit SNMP Ranges

This page allows you to modify your initial configuration settings (see Raritan's *CommandCenter NOC Deployment Guide*) allowing you to change the mapping of the SNMP community string to the nodes, that is, specific addresses or address ranges for which it should be used.

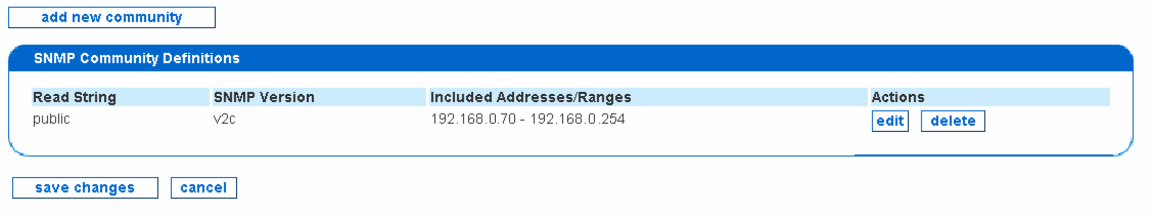
The CC-NOC uses the SNMP protocol to collect performance information from devices that support this protocol, and provides an easy way to view performance graphs of particular devices on the network.

SNMP implements a security mechanism it calls *Community Strings*, which are similar to passwords. The CC-NOC requires the *Get Community String,* often called the *Read-only Community*, to access the SNMP performance metrics. As community strings are configurable on a per device basis, the number of community strings you may need to enter will vary with the environment. Many organizations use one community string enterprise-wide, and others maintain them on a per-device or group of devices basis.

The community strings for any device from which you wish to collect performance information is required. Review your community definitions below and add, edit or remove community definitions as needed.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Network Management Configuration**.

3. Click **Edit the SNMP Ranges**.

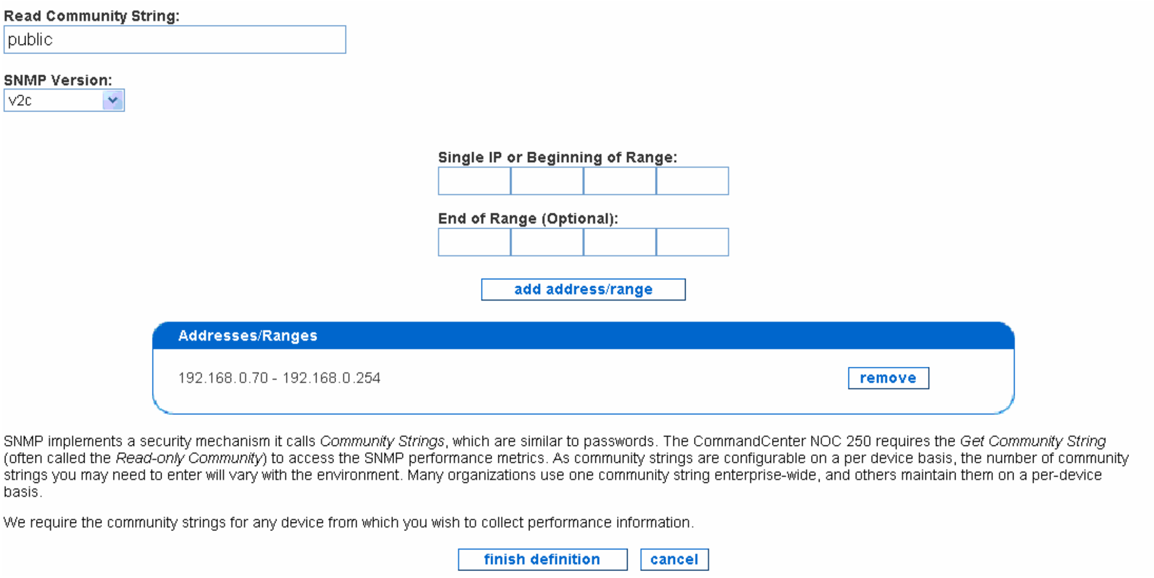


SNMP Community Definitions

Read String	SNMP Version	Included Addresses/Ranges	Actions
public	v2c	192.168.0.70 - 192.168.0.254	edit delete

Figure 8 Edit SNMP Ranges

4. Click **add new community** or **edit** next to the already defined SNMP range.



Read Community String: public

SNMP Version: v2c

Single IP or Beginning of Range:

End of Range (Optional):

Addresses/Ranges

192.168.0.70 - 192.168.0.254

SNMP implements a security mechanism it calls *Community Strings*, which are similar to passwords. The CommandCenter NOC 250 requires the *Get Community String* (often called the *Read-only Community*) to access the SNMP performance metrics. As community strings are configurable on a per device basis, the number of community strings you may need to enter will vary with the environment. Many organizations use one community string enterprise-wide, and others maintain them on a per-device basis.

We require the community strings for any device from which you wish to collect performance information.

Figure 9 Defining SNMP Ranges

5. Edit the community string or add a new one.
6. Specify the SNMP version by selecting **v1**, **v2c**, or **Not Specified** from the **SNMP version** drop-down list box.
7. Add ranges or addresses to the community, one at a time. To enter a range, fill in both the **Single IP or Beginning of Range** and **End of Range** fields, and click **add address/range.** To enter a single address, simply leave off the **End of Range** address. Note that you *must* provide an IP address or range for each string; if you wish to provide an SNMP string for all devices that the CC-NOC is managing, just specify the range as 0.0.0.0 - 255.255.255.255. Click **remove** if you wish to remove the defined addresses.
8. Click **finish definition**.

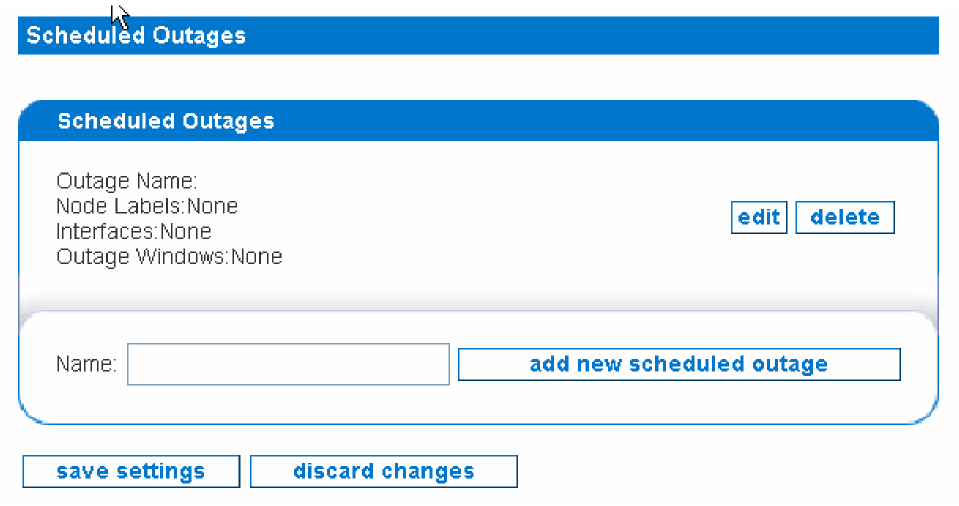
Note: *Community Strings are required for any device from which you wish to collect SNMP performance information. The default SNMP community string is* ***public****.*

Configure Scheduled Outages

This page allows you to create reoccurring windows where services will not be polled on a particular node. You can schedule planned outages for managed devices on your network. The downtime experienced by a device during a scheduled outage will not count negatively against the uptime statistics measured for the device.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Network Management Configuration**.

3. Click **Configure Schedule Outages**.



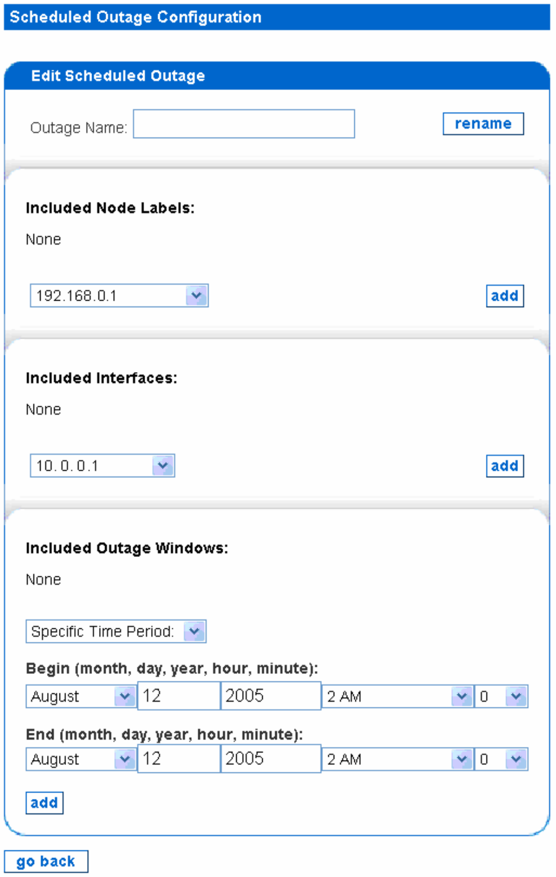
Scheduled Outages

Scheduled Outages

Outage Name:
Node Labels: None
Interfaces: None
Outage Windows: None

Figure 10 Configuring Scheduled Outages

4. Type a name for the scheduled outage and click **add new scheduled outage**.



Scheduled Outage Configuration

Edit Scheduled Outage

Outage Name:

Included Node Labels:

None

192.168.0.1

Included Interfaces:

None

10.0.0.1

Included Outage Windows:

None

Specific Time Period:

Begin (month, day, year, hour, minute):

August 12 2005 2 AM 0

End (month, day, year, hour, minute):

August 12 2005 2 AM 0

Figure 11 Edit Scheduled Outages

5. Type a name for the scheduled outage.
6. Select a **node label**, that is, a DNS hostname or IP address, from the **Included Node Label** drop-down list and click **add**. Adding a node label is optional and can be removed once added.
7. Select an **interface**, that is, an IP address, from the **Included Interfaces** drop-down list and click **add**. Adding an interface is optional and can be removed once added.

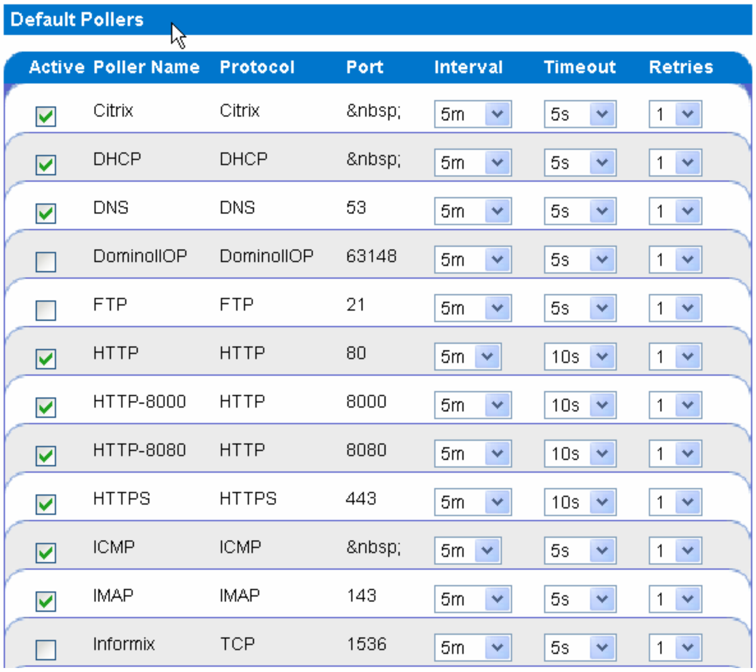
8. Specify an **outage window**. For outage windows that are set to *Recurring Weekly*, you cannot specify outages that start on one day of the week and end on a different day. In these cases where the outage spans 12:00 AM (Midnight), you should create two outages, one that ends at 11:59 PM and another that begins at 12:00 AM on the following day. Even though there appears to be a one minute gap between these outage spans, that is not the case. The outage will be processed seamlessly.
9. Click **add**.

Configure Pollers

This page allows you to determine which of the default pollers, that is, the monitors that exercise your web servers, email servers, etc. and create service down messages should be running on your system. Also configurable is their behavior, for example, poll attempt timeouts, retry attempts, etc. Additionally, you can create your own pollers for custom or niche applications you may be running in your environment.

Note: *The SNMP poller is disabled by default because in most cases, the availability of SNMP data is not integral to the core business of a company, thus it is excluded from availability calculations. Even if this poller is disabled, SNMP performance collection will still take place and the SNMP graphs for statistics like network traffic and disk usage will be updated. If the SNMP service experiences an outage, it may cause gaps in these graphs when data is unavailable but the outage will not affect your availability statistics.*

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Network Management Configuration**.
3. Click **Configure Pollers**.



Default Pollers

Active	Poller Name	Protocol	Port	Interval	Timeout	Retries
☑	Citrix	Citrix		5m	5s	1
☑	DHCP	DHCP		5m	5s	1
☑	DNS	DNS	53	5m	5s	1
□	DominoIIOP	DominoIIOP	63148	5m	5s	1
□	FTP	FTP	21	5m	5s	1
☑	HTTP	HTTP	80	5m	10s	1
☑	HTTP-8000	HTTP	8000	5m	10s	1
☑	HTTP-8080	HTTP	8080	5m	10s	1
☑	HTTPS	HTTPS	443	5m	10s	1
☑	ICMP	ICMP		5m	5s	1
☑	IMAP	IMAP	143	5m	5s	1
□	Informix	TCP	1536	5m	5s	1

Figure 12 Configure Pollers

- The **Active** column shows the current status of the poller. If the active field is checked, the poller will be scanned in the next poller rescan.
- The **Poller Name** column shows the name of each service in the poller configuration.
- The **Protocol** column shows the communications protocol used for polling each service.
- The **Port** column shows the ports at which the service will be polled.
- This panel also allows the admin user to **configure polling intervals, the timeout period between retries, and number of retries before an outage is declared.** Adjusting polling

intervals (they were initially set at 5 minutes for a reason), timeouts and/or retries without proper planning or forethought runs the risk of:

- Having the pollers get behind
- Adding unreasonable amounts of network traffic in the environment
- Misdiagnosis of outages, in the case of low retries

Note: *Raritan strongly recommends that these parameters be adjusted only if change is absolutely necessary.*

4. Enable or disable polling of these services through the check boxes on the left of each row.
5. If you make a change to any of the polling attributes, after you make those changes click **apply changes** to commit the changes. This will cause the CC-NOC to restart and set the new configuration.
6. Clicking **add custom poller** loads a page that gives you the ability to add named poller services.

- The **Poller Name:** column is the name of the new service to be added.
- The **Protocol**: is the communications protocol used for polling the service. If you simply want to check to see if the target port is open, then choose "TCP" as the protocol.
- The **Port:** lists the ports at which the service will be polled. If there is more than one port where the service can be located, it's recommended to create multiple distinct pollers, each with unique names, following the model *name-####,* where the *name* is the Poller Name and the # characters are replaced by the port number you intend to poll. After you add the custom poller, click a**pply changes** on the **Configure Pollers** page to apply the settings.
- When specifying ports, if there is more than one port where the service can be located, it is recommended to create multiple distinct pollers, each with unique names, following the model *name-####,* where the *name* is the Poller Name and the # characters are replaced by the port number you intend to poll.
- If the **Make Active** field is checked, the poller will be turned on and will scan the network during the next poller rescan.

7. Click **add**.
8. After you add the custom poller, click **apply changes** on the **Configure Pollers** page to apply the settings.

Warning: *When an administrator adds a new service, the capabilities scanning configuration is also updated to reflect the new service added and the scan status will be set to "on."*

Manage, Unmanage, Rescan, or Delete Devices

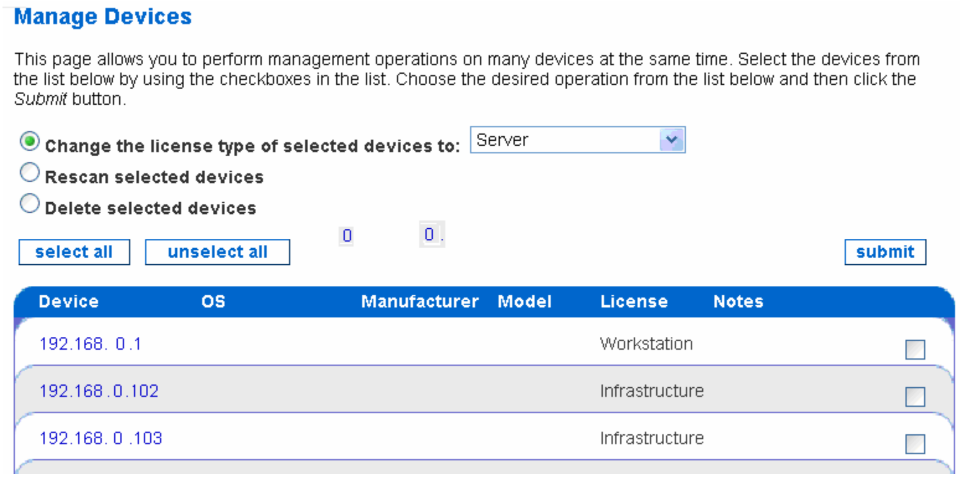
After discovery, the CC-NOC categorized each device as either a Server, Infrastructure device, or Workstation. This page allows you to change this categorization or remove a device from being managed by the CC-NOC. For example, you may want to use this page to "promote" a workstation so that additional metrics, for example, service and performance are collected for it, similar to a server.

Note: *Devices managed to collect WMI information are also displayed in this page – please see **Chapter 4: Configuring Windows Management** for additional information.*

You can choose to manage or unmanage several devices at once. You can also perform rescans of several devices at the same time from this page.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Network Management Configuration**.

3. Click **Manage, Unmanage, Rescan, or Delete Devices**.



Manage Devices

This page allows you to perform management operations on many devices at the same time. Select the devices from the list below by using the checkboxes in the list. Choose the desired operation from the list below and then click the *Submit* button.

● Change the license type of selected devices to: Server

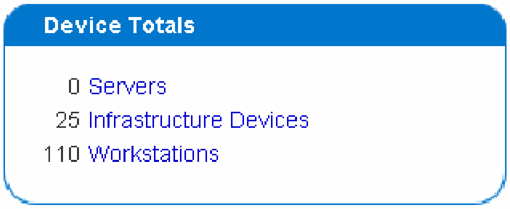
○ Rescan selected devices

○ Delete selected devices

Device	OS	Manufacturer	Model	License	Notes	
192.168. 0.1				Workstation		□
192.168.0.102				Infrastructure		□
192.168. 0 .103				Infrastructure		□

Figure 13 Manage, Unmanage, Rescan, or Delete Devices

4. Select the devices from the list by clicking in the check boxes.
5. You can change the license type of the selected devices to: **Server**, **Infrastructure**, **Workstation**, **Promoted Workstation**, or **Unmanaged**. Selecting **Unmanaged** will not remove it from the list, but will remove its licence, stop sending events to CC-SG if configured, and decrease network resources since it won't be polled any longer. Changing it to **Promoted Workstation** from Workstation will instruct the CC-NOC to collect performance and service statistics, similar to that of a server. This requires that it is under Windows management – please see **Chapter 4: Configuring Windows Management** for additional information. You can have up to five promoted workstations.
6. If you delete one or more device, it is removed from the list but not deleted from the database.
7. You can filter the list by clicking on either **Servers**, **Infrastructure Devices**, or **Workstations** under Device Totals.



Device Totals

0 Servers

25 Infrastructure Devices

110 Workstations

Figure 14 Device Totals

8. You can also produce a report by choosing a format, for example, HTML or XML and click **generate report**.
9. Click **submit**.

Note: *If an Infrastructure device, for example, Cisco router is listed as Unknown, it means that the default sysName value of "Unknown" has not been changed to something more meaningful. This can be corrected by either clicking the 'Change Device Label' link on the device page or the administrator of the "Unknown" device can assign a meaningful name to the sysName value.*

Configure Performance Thresholds

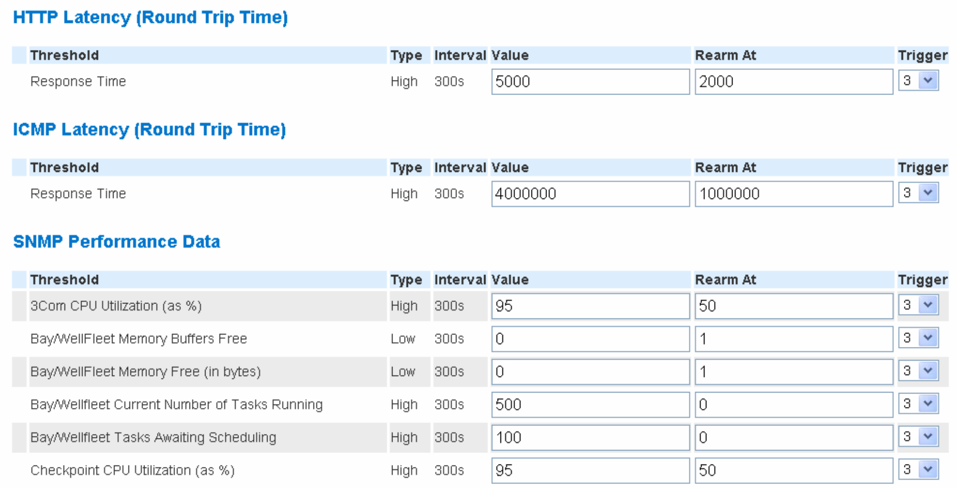
This page displays the current values at which SNMP performance metrics are considered problematic and events are generated. You have complete control over these thresholds, including their value, their re-arm values, and the number of consecutive data samples, for example, "triggers" which must be exceeded before an event is generated.

***Note**: Performance thresholds are configured for devices with Infrastructure, Server, or Promoted Workstation licenses.*

By configuring performance thresholds, administrators can adjust the high/low thresholds of certain SNMP performance metrics. This function puts considerable configuration power into the hands of the administrator – but one that should be used only in the event of clear evidence of need, for example, environments that have servers that run under a heavy load constantly might want to increase the high threshold – but only after receiving alarms that do not indicate a problem. Setting thresholds too low or too high can result in either too many notifications or a lack of notifications for problems respectively. Thresholds can also be configured on a per-device basis – see **Edit Performance Thresholds (Per Device)** later in this chapter. Per-device thresholds override values that are configured here.

*Please see **Appendix C: Performance Monitoring** for additional information.*

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Network Management Configuration**.
3. Click **Configure Performance Thresholds**.



HTTP Latency (Round Trip Time)

Threshold	Type	Interval	Value	Rearm At	Trigger
Response Time	High	300s	5000	2000	3

ICMP Latency (Round Trip Time)

Threshold	Type	Interval	Value	Rearm At	Trigger
Response Time	High	300s	4000000	1000000	3

SNMP Performance Data

Threshold	Type	Interval	Value	Rearm At	Trigger
3Com CPU Utilization (as %)	High	300s	95	50	3
Bay/WellFleet Memory Buffers Free	Low	300s	0	1	3
Bay/WellFleet Memory Free (in bytes)	Low	300s	0	1	3
Bay/Wellfleet Current Number of Tasks Running	High	300s	500	0	3
Bay/Wellfleet Tasks Awaiting Scheduling	High	300s	100	0	3
Checkpoint CPU Utilization (as %)	High	300s	95	50	3

Figure 15 Configure Performance Thresholds

The **Value** column indicates the threshold, which varies by metric, at which an alarm condition of either “high” or “low” exists, depending upon the metrics of that performance indicator. The **Rearm At** column is an indicator of the value at which the threshold alarm will reset, after it has detected an alarm condition. The **Trigger** column details how many polling cycles the value must be above or below the Value level to trigger an alarm. Example: CPU Utilization set at 95.0 Value, 50.0 Rearm, and Trigger at 3 would issue a “High Threshold” alarm if the node had 95% or higher CPU usage over 15 minutes (3 5-minute intervals). If the Value dropped below 50% either during or after the initial Trigger, then the alarm would reset and a new alarm would be issued if the same conditions reappeared.

***Note:** If the threshold is of type **High**, the value must be greater than or equal to the **Rearm At** value. If the threshold is of type **Low,** the value must be less than or equal to the **Rearm At** value.*

4. Each time you adjust the performance thresholds, click **save thresholds** to commit the changes.
5. You can also click **reset** to restore the threshold values to their pre-set condition.

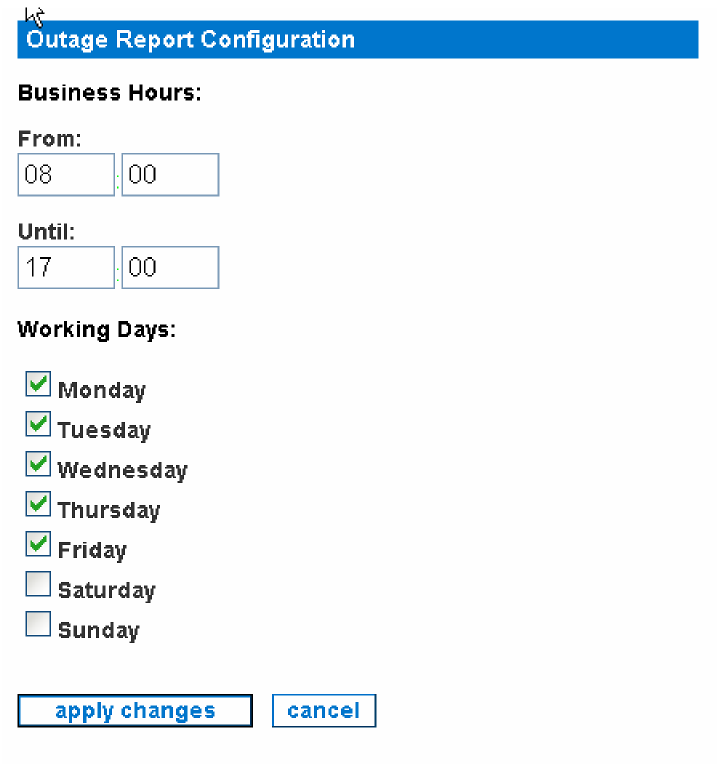
Configure Outage Report

This page allows you to view and modify the working business hours and days for the Outage Report. The Outage Report generates two availability percentages:

- One for total availability during the entire week
- Another for availability during business hours

You can edit the time period that is used to calculate the business hours availability by changing the data in the fields in this page.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Network Management Configuration**.
3. Click **Configure Outage Report**.



Outage Report Configuration

Business Hours:

From:
08 : 00

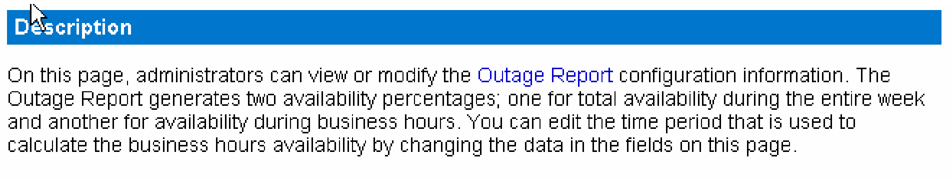
Until:
17 : 00

Working Days:

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☐ Saturday
☐ Sunday

Figure 16 Configure Outage Report

4. Type business hours in 24-hour (military) format.
5. Using the check boxes, select the working days you wish to include in the report.
6. Click **apply changes**.
7. Click **Outage Report** in the right-hand side of the page to generate a report.



Description

On this page, administrators can view or modify the Outage Report configuration information. The Outage Report generates two availability percentages; one for total availability during the entire week and another for availability during business hours. You can edit the time period that is used to calculate the business hours availability by changing the data in the fields on this page.

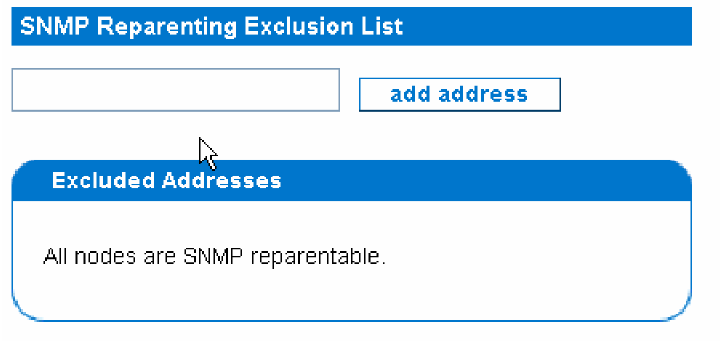
Figure 17 Navigating to Outage Report

SNMP Reparenting Exclusion List

This page allows you to specify addresses that should be excluded from SNMP reparenting. This feature is useful if you have multi-interface SNMP devices that have identical IP addresses to other multi-interface devices.

The most common example of this is if you are managing several routers that each act as gateways to separate private networks. In this case, all of the routers may have a "192.168.0.1" interface that acts as a gateway for the private network. Normally, the SNMP reparenting logic would detect that multiple nodes are sharing an IP address and would collect all of the interfaces for all of the routers under a single node. By entering "192.168.0.1" in the exclusion list on this page, you can prevent this from happening and keep all of these nodes separate.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Network Management Configuration**.
3. Click **SNMP Reparenting Exclusion List**.



SNMP Reparenting Exclusion List

Excluded Addresses

All nodes are SNMP reparentable.

Figure 18 SNMP Reparenting Exclusion List

4. Type an IP address you want to exclude from SNMP reparenting.
5. Click **add address**.

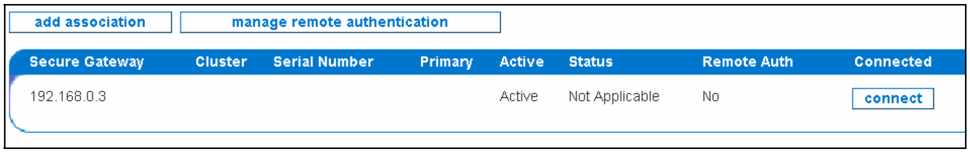
Associate CommandCenter Secure Gateway (CC-SG)

Associating a CC-SG with this appliance allows your users more flexibility when solving issues by giving them direct out-of-band KVM (Keyboard, Video, Mouse) using RRC, MPC, or RC and in-band access using SSH Client, VNC Client, or RemoteDesktop Viewer to problem devices. When a CC-SG is associated with your CC-NOC, your users will have many convenient ways of accessing managed devices.

***Note:** Although you may have several CC-SG's connected to this CC-NOC via a secure connection, only one can be the remote authentication and authorization source.*

Configure a CC-SG

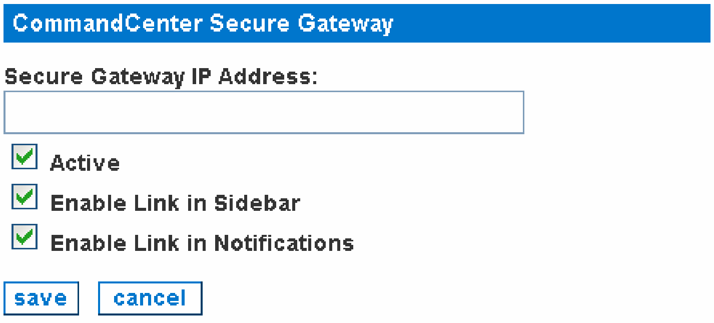
1. Click on the **Admin** tab in the top navigation bar.
2. Click **CommandCenter Secure Gateway Configuration**.



Secure Gateway	Cluster	Serial Number	Primary	Active	Status	Remote Auth	Connected
192.168.0.3				Active	Not Applicable	No	connect

Figure 19 Associate a CommandCenter Secure Gateway

3. Click **add association**.



CommandCenter Secure Gateway

Secure Gateway IP Address:

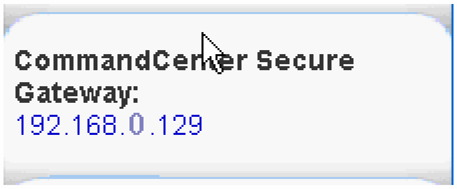
☑ Active

☑ Enable Link in Sidebar

☑ Enable Link in Notifications

Figure 20 Configure a CommandCenter Secure Gateway

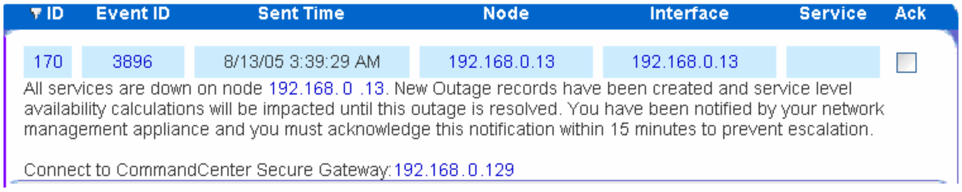
4. Type an **IP address** or hostname for the CC-SG. This is a required field. If entering a hostname, it can only contain letters, numbers, periods, or hyphens, and it must begin with either a letter or a number.
5. Clicking **Active** will turn on all links to the CC-SG. When **Active** is not checked, the CC-SG will be marked as inactive, which will turn off all links to that appliance without removing the configuration entirely.
6. If you click **Enable Link in Sidebar**, all normal and administrator users will have a link in the left-hand sidebar that will take them directly to your CC-SG appliance's user interface. Note that Executive users do not have access to the CC-SG.



CommandCenter Secure Gateway:
192.168.0.129

Figure 21 CommandCenter Secure Gateway in Sidebar

7. If you click **Enable Link in Notifications**, all outgoing notifications will have a convenient link added that will take your users to your CC-SG appliance's user interface or to the CC-SG target itself if remote authentication has been configured. This link will also be present in the Notification Browser and while viewing individual notices.



▼ID	Event ID	Sent Time	Node	Interface	Service	Ack
170	3896	8/13/05 3:39:29 AM	192.168.0.13	192.168.0.13		□

All services are down on node 192.168. 0 .13. New Outage records have been created and service level availability calculations will be impacted until this outage is resolved. You have been notified by your network management appliance and you must acknowledge this notification within 15 minutes to prevent escalation.

Connect to CommandCenter Secure Gateway: 192.168.0.129

Figure 22 CommandCenter Secure Gateway in Notification Browser

8. Click **save**.

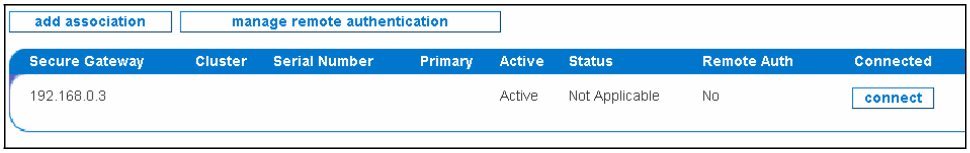
Create a CC-SG Peer via a Secure Channel

After configuring the CC-SG with CC-NOC information, for example, specifying its IP address, and configuring CC-NOC with CC-SG information, you can create a secure channel between CC-SG and CC-NOC. Configuring CC-SG with CC-NOC information is documented in the *CommandCenter Secure Gateway Administrator Guide*.

***Note**: To create a valid connection, the time settings on both the CC-NOC and CC-SG should be synchronized. The best method of achieving this synchronization, it to use a common NTP (Network Time Protocol) server. For this reason, the CC-NOC and CC-SG are required to be configured to use an NTP server.*

You will either copy and paste the CC-SG passcodes or the CC-SG administrator will submit two passcodes to you, which you will enter here. Once the certificate exchange process is complete, a secure channel is established between CC-NOC and CC-SG. The secure channel created here is available for one year.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **CommandCenter Secure Gateway Configuration**.



Secure Gateway	Cluster	Serial Number	Primary	Active	Status	Remote Auth	Connected
192.168.0.3				Active	Not Applicable	No	connect

Figure 23 Associate a CommandCenter Secure Gateway

3. Click **connect** next to the CC-SG you want to create a secure channel.

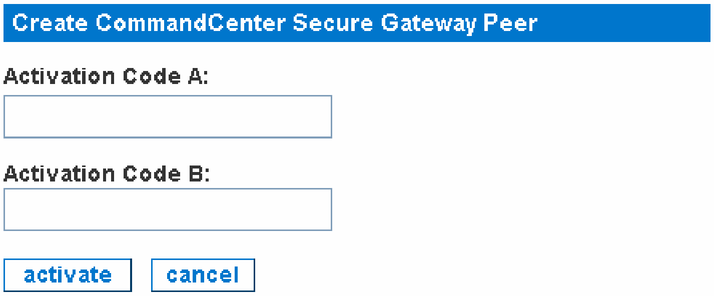


Figure 24 Create a CC-SG Peer

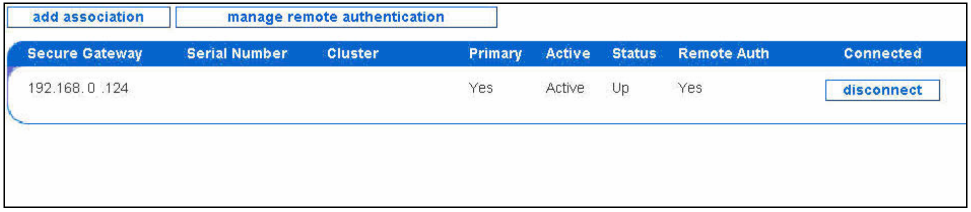
4. Either copy and paste the first passcode from CC-SG or type the passcode as supplied by the CC-SG administrator in **Activation Code A**.
5. Either copy and paste the second passcode from CC-SG or type the passcode supplied by the CC-SG administrator in **Activation Code B**.
6. Click **activate**. This will start a handshake conversation between the CC-SG and the CC-NOC. They each will generate and share keys that will uniquely and securely identify each to the other. Once that handshake is complete, the two appliances will start sharing information.

Important! To successfully connect, you must enter the passcodes in CC-NOC within five minutes after they are generated on CC-SG. This will minimize the window of opportunity for intruders to breach the system with a brute-force attack. Avoid transmitting the passcodes over email or other electronic means to avoid a possible interception by automated systems. A phone call or exchange of written codes between trusted parties is better protection against automated interception.

Disconnect a CC-SG

Disconnecting a CC-SG will close the secure channel between CC-NOC and CC-SG. You will not be able to access CC-SG from CC-NOC.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **CommandCenter Secure Gateway Configuration**.



Secure Gateway	Serial Number	Cluster	Primary	Active	Status	Remote Auth	Connected
192.168. 0 .124			Yes	Active	Up	Yes	disconnect

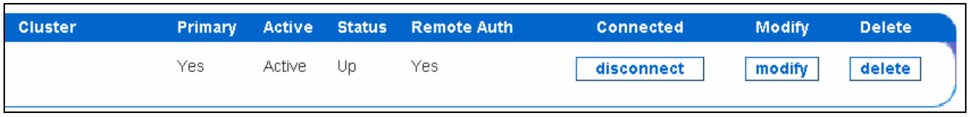
Figure 25 Disconnect a CommandCenter Secure Gateway

3. Click **disconnect**.

Delete a CC-SG

Deleting a CC-SG will remove all configuration of the CC-SG. Also, if CC-NOC is currently connected to CC-SG and a secure channel exists, deleting the CC-SG will tear down the secure channel. You will not be able to access this CC-SG from CC-NOC.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **CommandCenter Secure Gateway Configuration**.



Cluster	Primary	Active	Status	Remote Auth	Connected	Modify	Delete
	Yes	Active	Up	Yes	disconnect	modify	delete

Figure 26 Delete a CommandCenter Secure Gateway

3. Click **delete**.

Map CC-SG User Groups to Local User Roles

If you are using remote authentication via an associated CC-SG, this option allows you to view all user groups on the remote CC-SG and map them to CC-NOC user roles (Administrator, User, Executive User).

***Note**: This assumes that a CC-SG has already been associated with this CC-NOC and that a secure channel to CC-SG has been established – see section **Associate CommandCenter Secure Gateway (CC-SG)** in this chapter for details.*

Therefore, when a user remotely accesses CC-SG or a CC-SG target through CC-NOC, their remote user groups will be checked against this mapping list. For example, you might want to map a CC-SG "**Guest**" user group to a CC-NOC "**Executive User**" role, giving users only access to the read-only sections of the user interface. Only groups with known mappings will be allowed access to the CC-NOC.

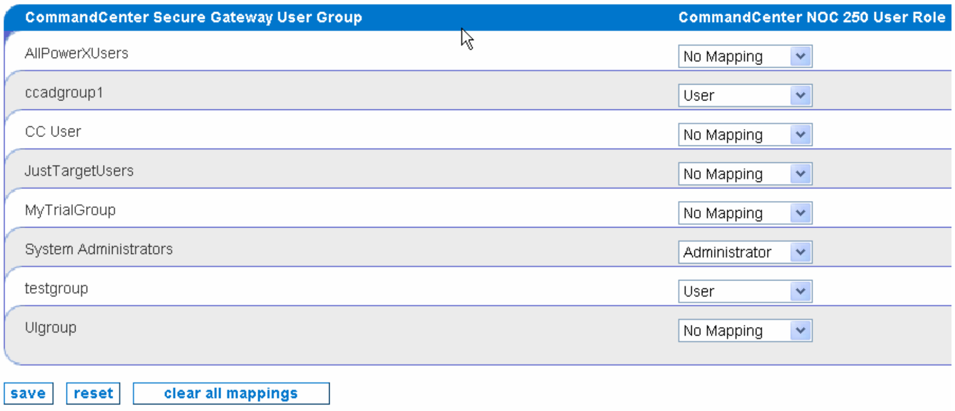
Important! Configuring these mappings is required in order for remote authentication to work. Although you may have several CC-SG's connected to this CC-NOC via a secure connection, only one can be the remote authentication and authorization source.

If a user is mapped to a CC-NOC user role but they do not have appropriate permissions to view a channel on CC-SG as defined in the CC-SG's user group's policy, they will not be able to access the CC-SG target. Therefore, it is important to understand the permissions of the policy that is applied to a user group on CC-SG. Refer to Raritan's *CommandCenter Secure Gateway Administrator Guide* for details.

If a CC-SG user belongs to multiple user groups, they will be given the highest privileges possible from all of the groups they belong to. For example, if they belong to a normal "User" group and an "Administrator" group, they will be given "Administrator" rights.

To map CC-SG user groups to CC-NOC user roles:

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Map Secure Gateway User Groups to Local User Roles**. Alternatively, you can click **manage remote authentication** from the CC-SG Association window.



CommandCenter Secure Gateway User Group	CommandCenter NOC 250 User Role
AllPowerXUsers	No Mapping
ccadgroup1	User
CC User	No Mapping
JustTargetUsers	No Mapping
MyTrialGroup	No Mapping
System Administrators	Administrator
testgroup	User
Ulgroup	No Mapping

Figure 27 Map CC-SG User Groups to Local User Roles

3. For each CC-SG user group, select a CC-NOC user role (**Administrator**, **User**, **Executive User**) or specify **No Mapping**.
4. Click save to retain all mappings.
5. To remove all mappings, click **clear all mappings** and then press **save**.
6. To reset to initial values, click **reset**.

Note: *The special* ***admin*** *user account is always considered a "local user" and is never checked remotely.*

Multi-Site Management

Multi-Site configuration allows you to configure how to use your Raritan appliances together over multiple sites. You can forward native Raritan events to other Raritan CC-NOC appliances or third-party systems. You can also relay all incoming SNMP traps to a third-party system.

Within multi-site management, you can:

- Configure Event Forwarding
- Configure Trap Relaying

Configure Event Forwarding

This page allows you to configure the events, for example, SNMP traps you want forwarded to external systems. It also allows you to configure the external systems to forward the events to.

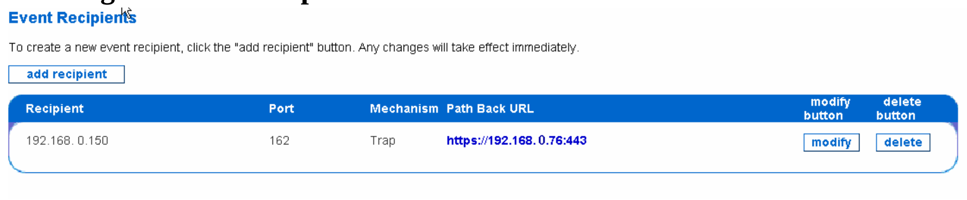
Within event forwarding, you can:

- Configure Event Recipients
- Configure Event Severities to Forward

Configure Event Recipients

To instruct your CC-NOC to forward copies of its events as SNMP traps to other management platforms or Raritan appliances, use **Configure Event Recipients** to specify where your events should be forwarded.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Multi-site Management**.
3. Click **Configure Event Forwarding**.
4. Click **Configure Event Recipients**.



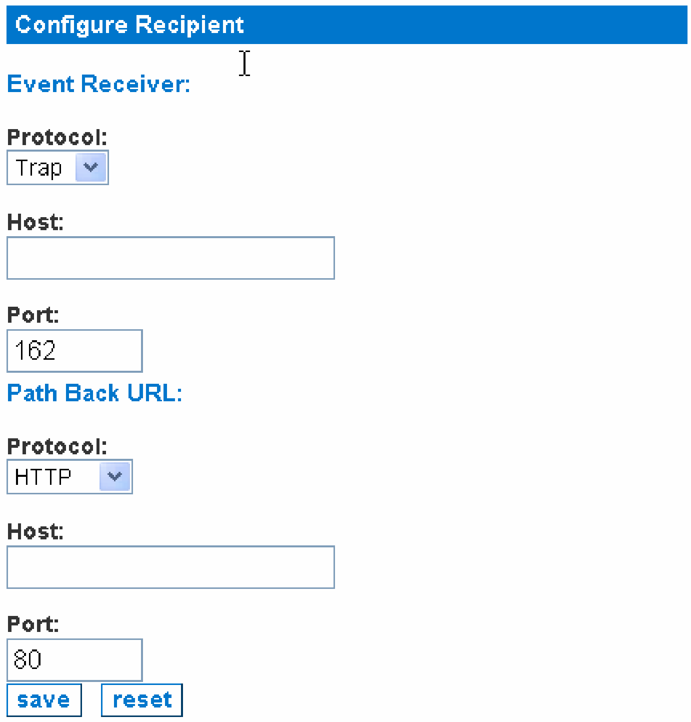
Event Recipients

To create a new event recipient, click the "add recipient" button. Any changes will take effect immediately.

Recipient	Port	Mechanism	Path Back URL	modify button	delete button
192.168. 0.150	162	Trap	https://192.168.0.76:443	modify	delete

Figure 28 Configure Event Recipients

5. Click **add recipient**.



Configure Recipient

Event Receiver:

Protocol: Trap

Host:

Port: 162

Path Back URL:

Protocol: HTTP

Host:

Port: 80

Figure 29 Adding Event Recipients

6. Click **add recipient**.
7. Type protocol, host, and port for the **Event Receiver** which is the destination address of the management platform or Raritan appliance you are sending the trap to. On this platform or appliance resides an SNMP agent that listens for the traps. This Host can be either an IP

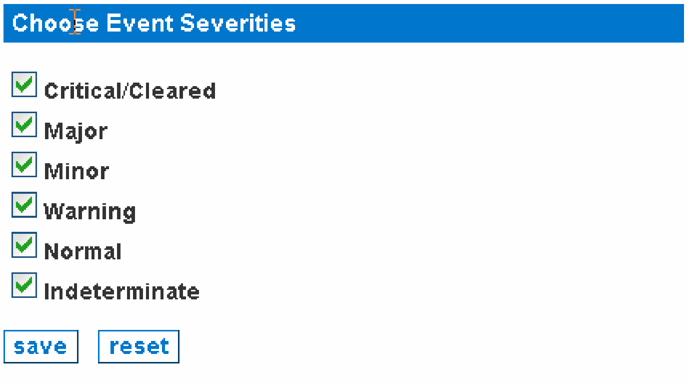
address or a hostname that this appliance can resolve. Example: Protocol=Trap, Host= 192.168.51.150, Port=162.

8. Type protocol, host, and port for the **Path Back URL** which is the IP address or hostname of this CC-NOC. The Host entered is the web address that a user of the external event recipient can use to connect back to this appliance via a web browser. The external event recipient might be on the other side of a firewall, however, and so the URL that a user would use to access this appliance's web user interface is a required parameter when creating an event recipient. Currently both **HTTP** and **HTTPS** are supported. Example: Protocol=HTTPS, Host= 192.168.53.176, Port=443.
9. Click **save**.

Configure Event Severities to Forward

To instruct your CC-NOC to forward copies of its events as SNMP traps to other management platforms or Raritan appliances, use **Configure Event Severities to Forward** to specify which events should be forwarded.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Multi-site Management**.
3. Click **Configure Event Forwarding**.
4. Click **Configure Event Severities to Forward**.



Choose Event Severities

☑ Critical/Cleared
☑ Major
☑ Minor
☑ Warning
☑ Normal
☑ Indeterminate

Figure 30 Configure Event Severities to Forward

5. Click the check boxes before the **Event Severities** you want to forward. All events matching these severities will be forwarded to all recipients specified in **Event Forwarding Recipient** – see section **Configure Event Recipients** earlier in this chapter. These changes will take effect immediately.
6. Click **save**.

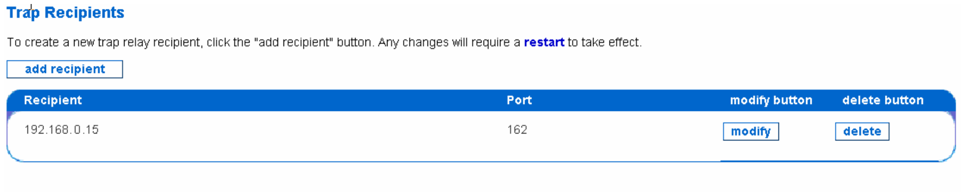
Note: *For the purposes of event forwarding, the Critical and Cleared severities are equivalent. A Cleared event occurs when a Critical situation, for example, a network outage has ended.*

Configure Trap Relaying

This page allows you to configure where any incoming SNMP traps should be relayed. You can relay incoming traps to a management platform or Raritan appliance. On this platform or appliance resides an SNMP agent that listens for the traps.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Multi-site Management**.

3. Click **Configure Trap Relaying**.



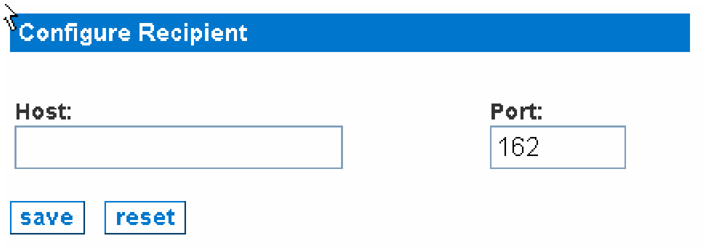
Trap Recipients

To create a new trap relay recipient, click the "add recipient" button. Any changes will require a **restart** to take effect.

Recipient	Port	modify button	delete button
192.168.0.15	162	modify	delete

Figure 31 Configure Trap Relaying

4. Click **add recipient**.



Configure Recipient

Host:

Port: 162

Figure 32 Specifying Trap Recipient

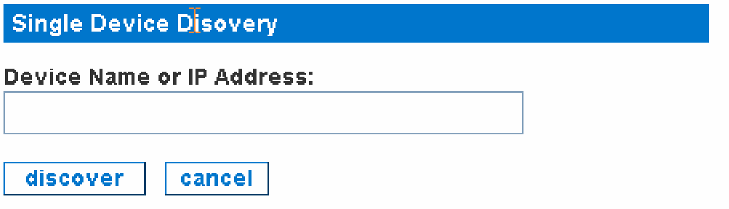
5. Specify a hostname that is resolvable from this appliance or an IP address in the **Host** field. This can be the same platform or appliance that was specified when configuring event recipients – see section **Configure Event Recipients** earlier in this chapter for additional information.
6. Type a port, for example, 162 on that host that is listening for incoming SNMP traps.
7. Click **save**.

Discover a Single Device

This features allows you to enter a single device for immediate entry into the discovery queue. For example, if a new server has been added to your environment and you want to monitor it immediately, it can be added here. The discovery process will then determine the characteristics of this device and map it to an available license type: Infrastructure, Server, Workstation, or Promoted Workstation. Depending on system load, a single device can usually be discovered within at least five minutes.

Note*: If a device is already discovered, adding the device again will not discover it twice. Only newly discovered devices are added to the currently managed set of devices.*

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Discover a Single Device** under Tools.



Single Device Disovery

Device Name or IP Address:

Figure 33 Discover a Single Device

3. Enter either a NetBIOS name, a hostname, or an IP address.
4. Click **discover**.

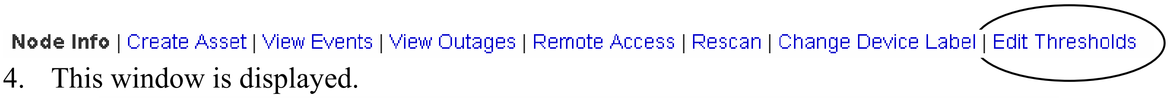
Note*: If two devices have the same NetBIOS name, only one will be discovered.*

Edit Performance Thresholds (Per Device)

In addition to configuring performance values per category–see section **Configure Performance Thresholds** earlier in this chapter, you can also configure performance thresholds on a per-device basis. Per-device thresholds will override those set per category.

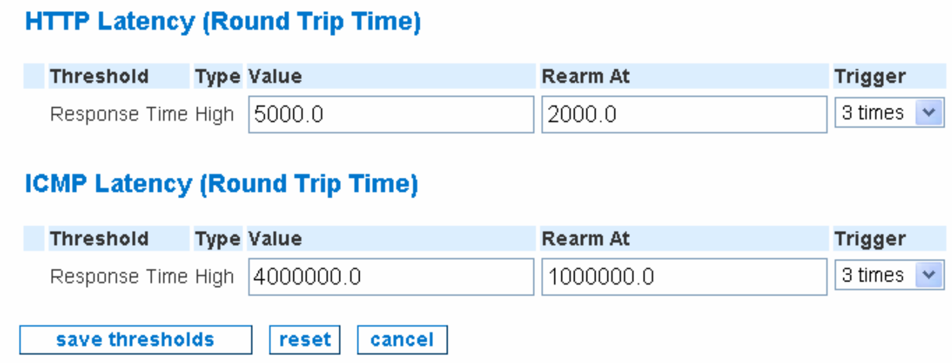
Note*: Performance thresholds can be configured on a per-device basis only for devices with Infrastructure, Server, or Promoted Workstation licenses.*

1. Click **Search** under **Device Search** in the left-hand corner of the Home page.
2. Click on the IP address of a device with an Infrastructure or Server license.
3. At the top of the window, click **Edit Thresholds**.



Node Info | Create Asset | View Events | View Outages | Remote Access | Rescan | Change Device Label | Edit Thresholds

4. This window is displayed.



HTTP Latency (Round Trip Time)

Threshold	Type	Value	Rearm At	Trigger
Response Time High		5000.0	2000.0	3 times

ICMP Latency (Round Trip Time)

Threshold	Type	Value	Rearm At	Trigger
Response Time High		4000000.0	1000000.0	3 times

Figure 34 Configure Performance Thresholds (Per-Device)

The current values at which SNMP, ICMP, HTTP, and/or Windows (WMI) performance metrics are considered problematic and events are generated for this particular device are listed in the window. You have complete control over these thresholds, including their value, their re-arm values, and the number of consecutive data samples (e.g., "triggers") which must be exceeded before an event is generated.

5. Enter values for **Value**, **Rearm At**, and **Trigger**.

- The **Value** column indicates the threshold, which varies by metric, at which an alarm condition of either “high” or “low” exists, depending upon the metrics of that performance indicator.
- The **Rearm At** column is an indicator of the value at which the threshold alarm will reset, after it has detected an alarm condition.
- The **Trigger** column details how many polling cycles the value must be above or below the Value level to trigger an alarm.

Example: CPU Utilization set at 95.0 Value, 50.0 Rearm, and Trigger at 3 would issue a “High Threshold” alarm if the node had 95% or higher CPU usage over 15 minutes (3 5-minute intervals). If the Value dropped below 50% either during or after the initial Trigger, then the alarm would reset and a new alarm would be issued if the same conditions reappeared.

Note: *If the threshold is of type* ***High****, the value must be greater than or equal to the* ***Rearm At*** *value. If the threshold is of type* ***Low,*** *the value must be less than or equal to the* ***Rearm At*** *value.*

6. Each time you adjust the performance thresholds, click **save thresholds** to commit the changes.
7. You can also click **reset** to restore the threshold values to their pre-set condition.

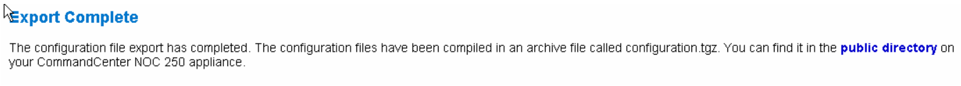
Administrator Tools

Administrator tools help you diagnose and fix problems with the CC-NOC. These tools allow you to backup configuration files, download logs, check the disk usage of your CC-NOC, and establish connections to Technical Support. Access administrator tools either from the **Tools** tab or from the **Admin** tab.

Export and Download Configuration Files

This page allows you to export the current configuration of the CC-NOC appliance. The configuration file will be archived in a file called **configuration.tgz**. This will most commonly be used at the request of Technical Support. You can then download this file by accessing **http://<CommandCenter_NOC_IP_Address>/public**.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Administrator Tools**.
3. Click **Export & Download Configuration Files**



Export Complete

The configuration file export has completed. The configuration files have been compiled in an archive file called configuration.tgz. You can find it in the **public directory** on your CommandCenter NOC 250 appliance.

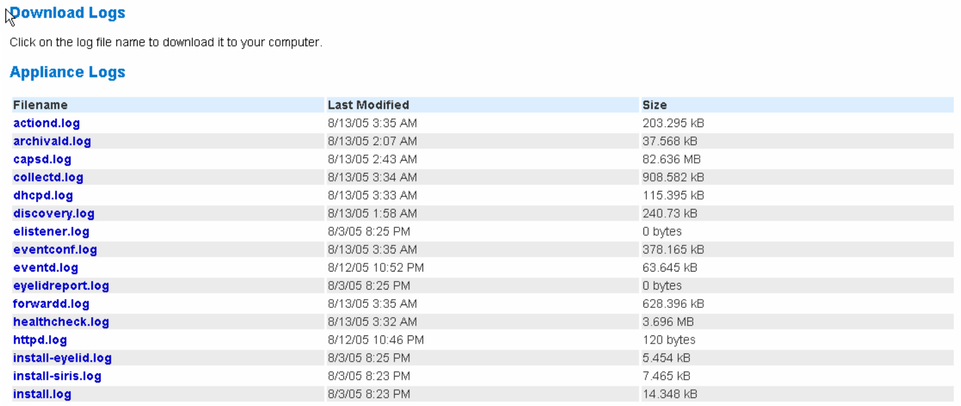
Figure 35 Export & Download Configuration Files

4. Access **http://<CommandCenter_NOC_IP_Address>/public** to view the file.

Download Log Files

This page allows you to download system log files, most commonly used at the request of Technical Support.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Administrator Tools**.
3. Click **Download Log Files**.



Download Logs

Click on the log file name to download it to your computer.

Appliance Logs

Filename	Last Modified	Size
actiond.log	8/13/05 3:35 AM	203.295 kB
archivald.log	8/13/05 2:07 AM	37.568 kB
capsd.log	8/13/05 2:43 AM	82.636 MB
collectd.log	8/13/05 3:34 AM	908.582 kB
dhcpd.log	8/13/05 3:33 AM	115.395 kB
discovery.log	8/13/05 1:58 AM	240.73 kB
elistener.log	8/3/05 8:25 PM	0 bytes
eventconf.log	8/13/05 3:35 AM	378.165 kB
eventd.log	8/12/05 10:52 PM	63.645 kB
eyelidreport.log	8/3/05 8:25 PM	0 bytes
forwardd.log	8/13/05 3:35 AM	628.396 kB
healthcheck.log	8/13/05 3:32 AM	3.696 MB
httpd.log	8/12/05 10:46 PM	120 bytes
install-eyelid.log	8/3/05 8:25 PM	5.454 kB
install-siris.log	8/3/05 8:23 PM	7.465 kB
install.log	8/3/05 8:23 PM	14.348 kB

Figure 36 Download Log Files

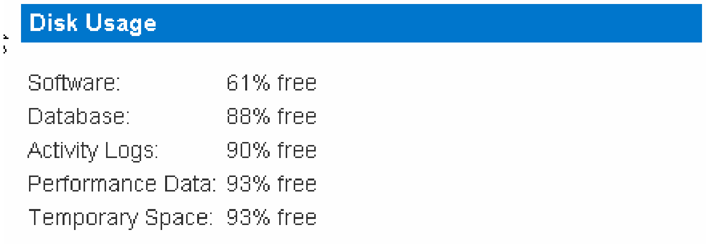
4. Open a log file to display its contents by clicking on it.

Check Disk Utilization on Appliance

This page allows you to see how much of the internal storage the appliance has used while collecting information about your network. The storage inside the appliance is sufficient to handle almost any monitoring tasks but if you are experiencing problems with the device, you may want to check to make sure that storage space is available.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Administrator Tools**.

3. Click **Check Disk Utilization on Appliance**.



Disk Usage

Software:	61% free
Database:	88% free
Activity Logs:	90% free
Performance Data:	93% free
Temporary Space:	93% free

Figure 37 Check Disk Utilization on Appliance

The **Disk Usage** section lists the current free space percentages for different areas of the storage within the CC-NOC appliance. The disk storage inside this CC-NOC appliance is used to store logs of system activity, performance information for the devices that you are monitoring, and a database of collected management information that includes event and notification records.

It is possible to exhaust the storage space on this CC-NOC if you are monitoring a number of devices that exceeds the specifications of the CC-NOC. To clean up the storage space, you can delete unused data periodically – see section **Prune Unused Performance Data** later in this chapter for additional information.

Send Incident Report

If you experience a problem with the CC-NOC, submit an Incident Report.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Administrator Tools**.
3. Click **Send Incident Report**.

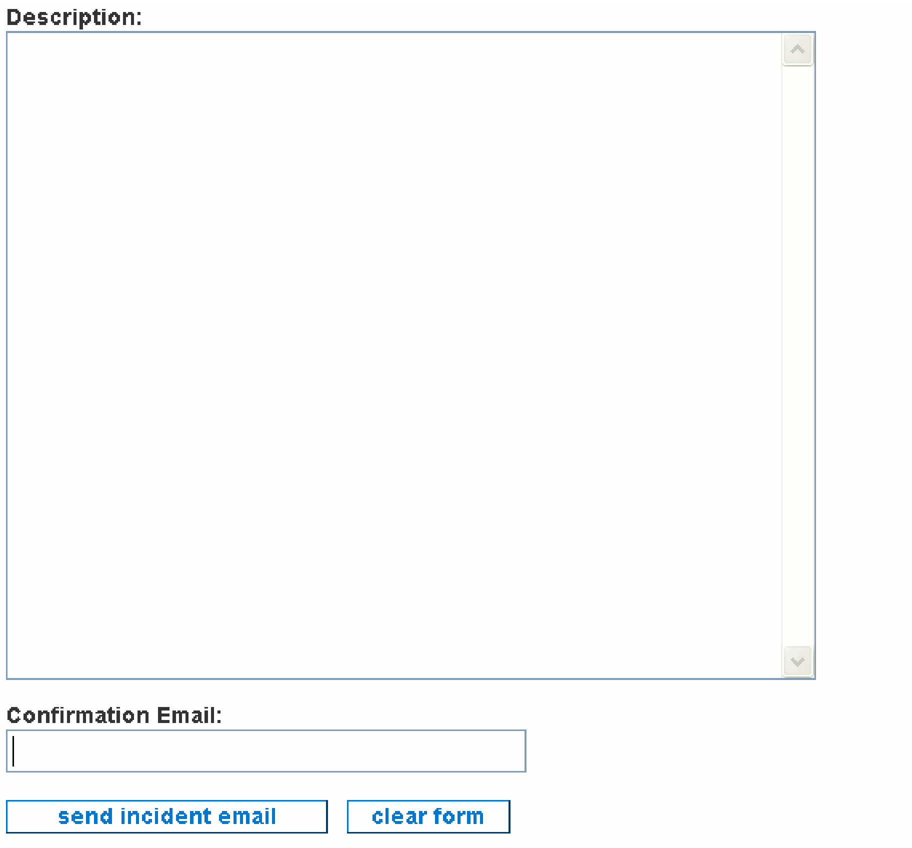


Figure 38 Send Incident Report

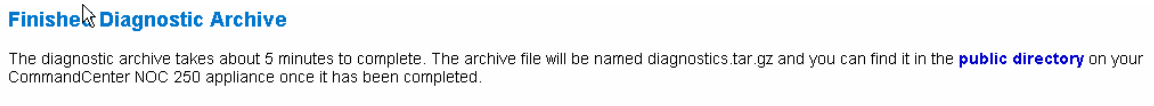
4. Type a description of the problem you are experiencing in the text box.
5. Type an email address in **Confirmation Email:** so that when the incident report email is received, you will get a confirmation message.
6. Click **send incident email**.

Generate Diagnostics File

If your CC-NOC does not have email access (an SMTP server has not configured – see section **Outgoing Email Communication**), use this option to create an archive that can be downloaded from the CC-NOC to a computer that does have email access.

The diagnostics file will be archived in a file called **diagnostics.tar.gz**. You can then download this file by accessing **http://<CommandCenter_NOC_IP_Address>/public**.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Administrator Tools**.
3. Click **Generate Diagnostics File**.



Finished Diagnostic Archive

The diagnostic archive takes about 5 minutes to complete. The archive file will be named diagnostics.tar.gz and you can find it in the **public directory** on your CommandCenter NOC 250 appliance once it has been completed.

Figure 39 Generate Diagnostics File

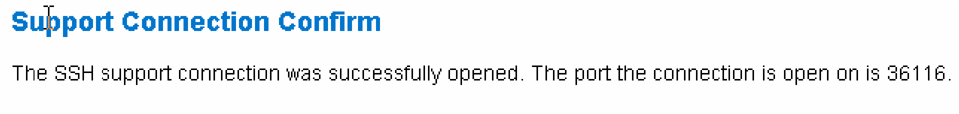
4. Access **http://<CommandCenter_NOC_IP_Address>/public** to view the file.

Establish Support Connection

If you have contacted Technical Support and they have requested SSH access to your appliance, you can open a Secure Shell (SSH) connection by clicking **establish support connection**.

Opening the connection may take between 10 to 30 seconds. Your firewall must allow out-going connections from the CC-NOC on both port 22 (SSH) and port 443 (HTTPS).

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Administrator Tools**.
3. Click **establish support connection**.



Support Connection Confirm

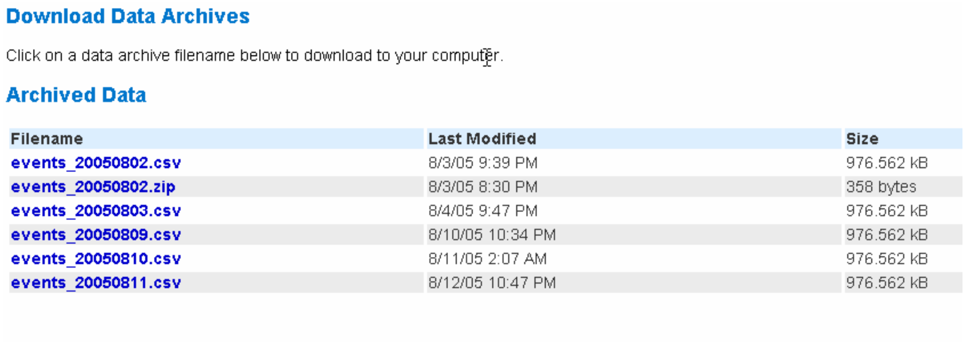
The SSH support connection was successfully opened. The port the connection is open on is 36116.

Figure 40 Establish Support Connection via SSH

Download Data Archives

Every 24 hours, the previous day's events are placed into an event archival file and made accessible. Download this archival file or unzip it to access a comma-separated value (CSV) file, which can be opened with any spreadsheet application to view the events for that day.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Administrator Tools**.
3. Click **Download Archived Data**.



Download Data Archives

Click on a data archive filename below to download to your computer.

Archived Data

Filename	Last Modified	Size
events_20050802.csv	8/3/05 9:39 PM	976.562 kB
events_20050802.zip	8/3/05 8:30 PM	358 bytes
events_20050803.csv	8/4/05 9:47 PM	976.562 kB
events_20050809.csv	8/10/05 10:34 PM	976.562 kB
events_20050810.csv	8/11/05 2:07 AM	976.562 kB
events_20050811.csv	8/12/05 10:47 PM	976.562 kB

Figure 41 Download Data Archives

4. Click one of the files to download.
5. Open and view the file with the appropriate application, for example, Excel.

Advanced Administration

This page presents more uncommon administrative tasks, as well as support tools which may be useful when troubleshooting specific problems, such as when applying system patches/upgrades, or as directed by support personnel.

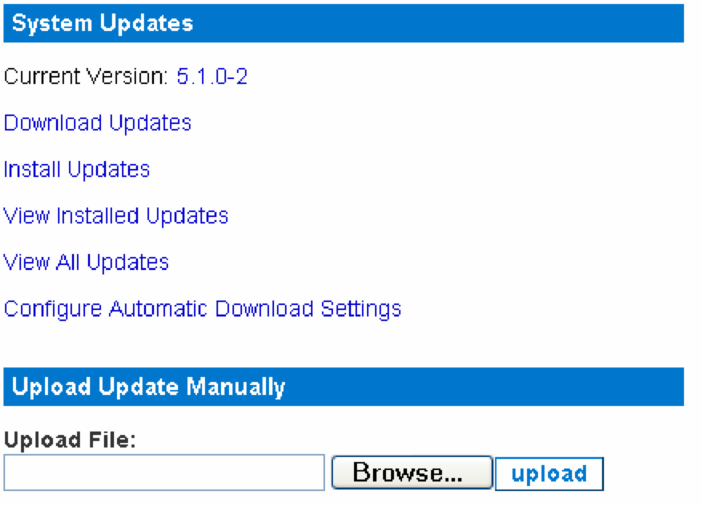
Options in this page allow you to perform several types of advanced maintenance on the CC-NOC itself, such as clearing out collected data and patching the software that the appliance is running. Please read all of the options thoroughly before using these features to make sure that you do not erase valuable data inadvertently.

***Note:** You may wish to download a copy of a recent system backup before using any of these options.*

System Software & Signature Updates

This feature allows you to query the Raritan servers for new updates and if available, to optionally enable auto-update detection, download, and installation. The CC-NOC is enabled to do the "leg work" of system patch application and system upgrades with limited administrator involvement.

All CC-NOC patches and updates are made available on a web server which can be automatically checked by your CC-NOC appliance. If new patches/updates are available, they can also be automatically downloaded, and optionally, automatically applied. The degree to which this process is performed is in your control, using the options available in this page.



System Updates

Current Version: 5.1.0-2

Download Updates

Install Updates

View Installed Updates

View All Updates

Configure Automatic Download Settings

Upload Update Manually

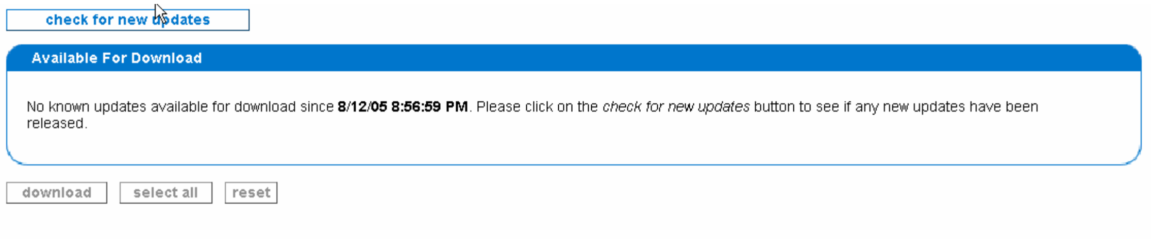
Upload File:

Figure 42 System Updates

Download Updates

This option displays a page that enables you to quickly and easily see what, if any, updates are available for your CC-NOC.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Advanced Administration**.
3. Click **System Software & Signature Updates**.
4. Click **Download Updates**.



Available For Download

No known updates available for download since **8/12/05 8:56:59 PM**. Please click on the *check for new updates* button to see if any new updates have been released.

Figure 43 Download Updates

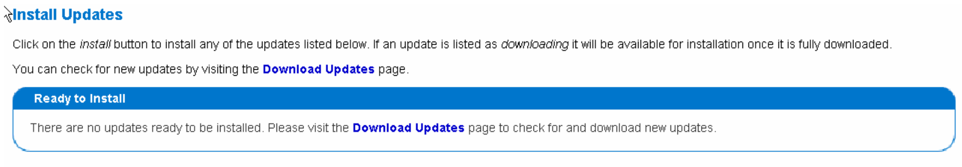
5. The list is all of the updates that the CC-NOC does know about. If no updates are displayed, click **check for new updates**.
6. To download updates, click the corresponding check box and click **download**. You will be taken to an install page where you can choose to install any updates that have finished downloading. Please note it may take several minutes for the updates to finish downloading depending on how large each update file is and how many you have chosen to download in tandem.

Install Updates

This option allows you to select which updates you want to install. The updates should have already been downloaded.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Advanced Administration**.
3. Click **System Software & Signature Updates**.

4. Click **Install Updates**.



Install Updates

Click on the *install* button to install any of the updates listed below. If an update is listed as *downloading* it will be available for installation once it is fully downloaded.

You can check for new updates by visiting the Download Updates page.

Ready to Install

There are no updates ready to be installed. Please visit the Download Updates page to check for and download new updates.

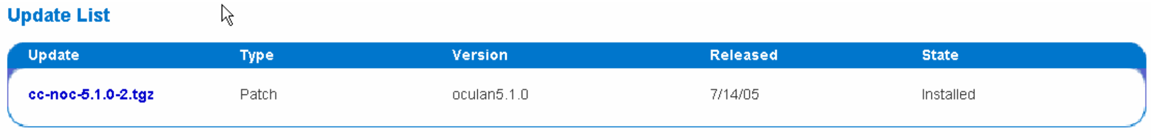
Figure 44 Install Updates

5. Click **install** to install any of the updates that are listed. If an update is listed as downloading, it will be available for installation once it is fully downloaded. Check for new updates by accessing the Download Updates page – see section **Download Updates** earlier in this chapter for additional information.

View Installed Updates

The **View Installed Updates** page provides a listing of all updates which have been applied, while the **View All Updates** page provides an overall view of updates which have been downloaded and not applied, as well as those that have been installed.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Advanced Administration**.
3. Click **System Software & Signature Updates**.
4. Click **View Installed Updates**.



Update List

Update	Type	Version	Released	State
cc-noc-5.1.0-2.tgz	Patch	oculan5.1.0	7/14/05	Installed

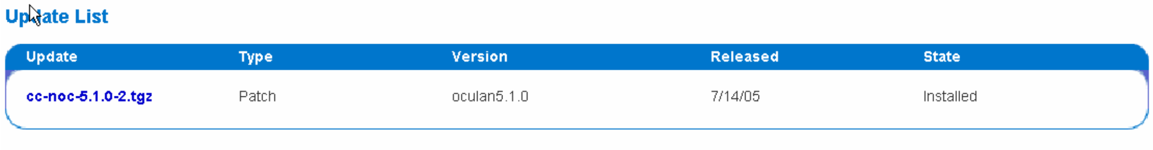
Figure 45 View Installed Updates

5. If desired, click the file to view details.

View All Updates

The **View All Updates** page provides an overall view of updates which have been downloaded and not applied, as well as those that have been installed, while the **View Installed Updates** page provides a listing of all updates which have been applied.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Advanced Administration**.
3. Click **System Software & Signature Updates**.
4. Click **View All Updates**.



Update List

Update	Type	Version	Released	State
cc-noc-5.1.0-2.tgz	Patch	oculan5.1.0	7/14/05	Installed

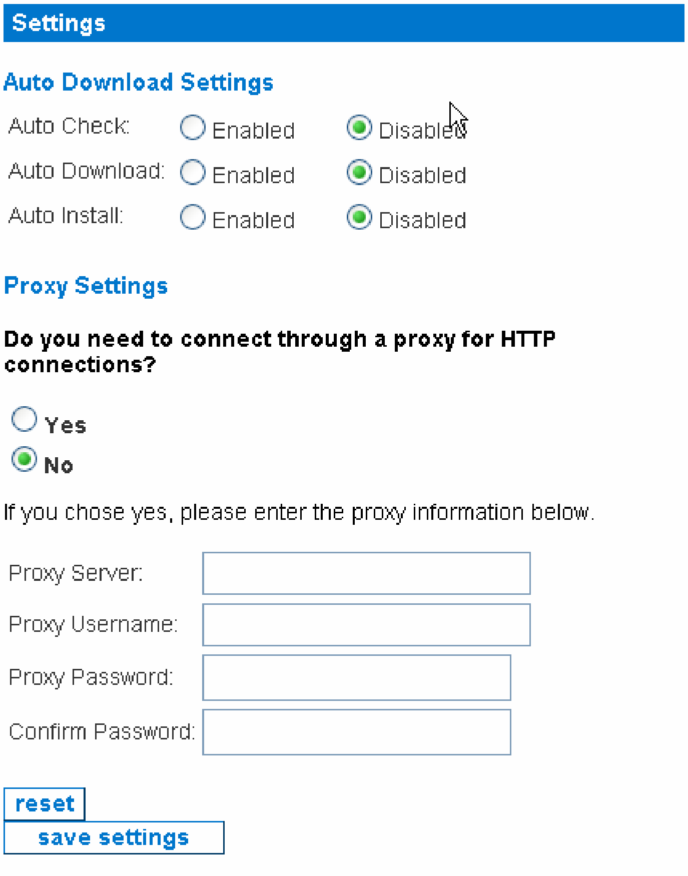
Figure 46 View All Updates

5. If desired, click the file to view details.

Configure Automatic Download Settings

This page allows you to specify if the system should be allowed to regularly check for updates and if available, download them to the CC-NOC. Additionally, available updates can be automatically installed as well. Using these options, you can control these behaviors independently, so if you want to automatically check for updates and download them if they are available, yet do not want them automatically installed, set **Auto Download** to **enable**, but leave **Auto Install** configured as **disabled**.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Advanced Administration**.
3. Click **System Software & Signature Updates**.
4. Click **Configure Automatic Download Settings**.



Settings

Auto Download Settings

Auto Check: ○ Enabled ● Disabled

Auto Download: ○ Enabled ● Disabled

Auto Install: ○ Enabled ● Disabled

Proxy Settings

Do you need to connect through a proxy for HTTP connections?

○ Yes

● No

If you chose yes, please enter the proxy information below.

Proxy Server:

Proxy Username:

Proxy Password:

Confirm Password:

Figure 47 View All Updates

5. Click **Enabled or Disabled** for Auto Check, Auto Download, and Auto Install.
6. If you are using a proxy server for HTTP requests you may need to enter the proxy settings in order for manual or auto-downloads to work. If you are using a proxy, click **Yes** to the question and enter in the proxy information in the provided fields. If you are not using a proxy click **No**.
7. Click **save settings**.

Upload Update Manually

For those who do not have Internet access or choose not to use the web-based update functionality, files can be manually downloaded to any location using the username and password provided and subsequently uploaded to the CC-NOC.

The **Upload File:** dialog box was created to facilitate that upload. Note that only valid Raritan patch files can be uploaded to this appliance. The upload of other files may cause problems with the appliance and may void your warranty.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Advanced Administration**.
3. Click **Browse:**
4. Select the file to upload and click **Open**.
5. Click **upload**.

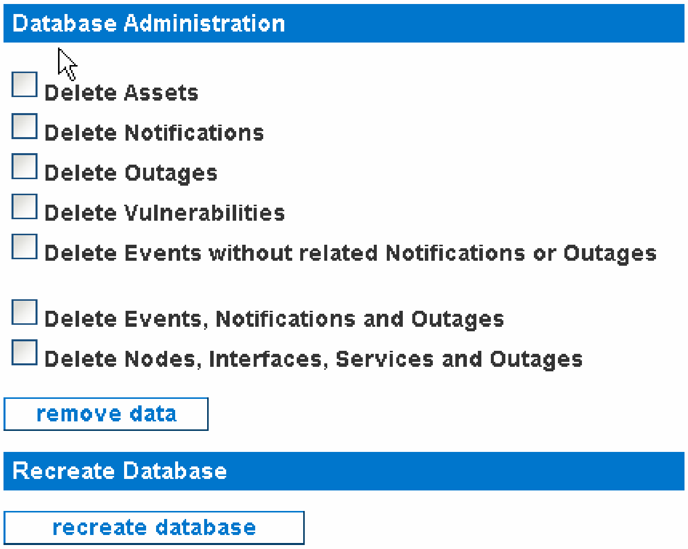
Appliance Database Administration

This page allows you to clean out unnecessary or unused information stored in the database, including node information, events, outages, etc. These operations are necessary if you would like to purge some of the data and start over with a clean database.

You will not lose any management information if you recreate your database but the CC-NOC will need to stop its management services and web user interface while the database is unavailable.

Note: *Before using this option, you should download a recent backup file – please see section* ***Data Backup and Restore*** *for additional information.*

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Advanced Administration**.
3. Click **Appliance Database Administration.**



Database Administration

□ Delete Assets
□ Delete Notifications
□ Delete Outages
□ Delete Vulnerabilities
□ Delete Events without related Notifications or Outages

□ Delete Events, Notifications and Outages
□ Delete Nodes, Interfaces, Services and Outages

Recreate Database

Figure 48 Appliance Database Administration

4. Using the check boxes, select the type of data you wish to purge.
5. Click **remove data** and confirm your choices.
6. Clicking **recreate database** causes the database structure to be purged and re-built. This is necessary if your database has become corrupted. You will likely only need to use this option if advised by Technical Support. If you suspect an issue related to database corruption, please contact Technical Support.

Data Backup and Restore

This page allows you to manipulate the backup files automatically generated by the CC-NOC in addition to providing the ability to upload backup files for restoration purposes. Backup files are created every 24-hours for compliance and auditing purposes.

This feature allows you to:

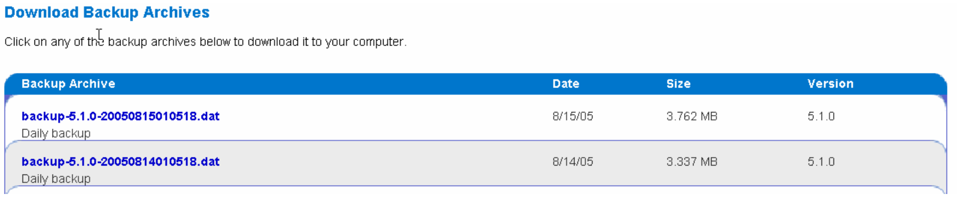
- Download backup files from the CC-NOC appliance to another computer.
- Upload a backup file from another computer to the CC-NOC.
- Install a backup file.

If you upload a backup file to the CC-NOC, you will be taken to the install page where you can choose to apply the backup to the CC-NOC.

Download a Backup File

It is recommended to download a backup file on a periodic or regular basis.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Advanced Administration**.
3. Click **Data Backup and Restore.**
4. Click **Download Backup Files.**



Download Backup Archives

Click on any of the backup archives below to download it to your computer.

Backup Archive	Date	Size	Version
backup-5.1.0-20050815010518.dat Daily backup	8/15/05	3.762 MB	5.1.0
backup-5.1.0-20050814010518.dat Daily backup	8/14/05	3.337 MB	5.1.0

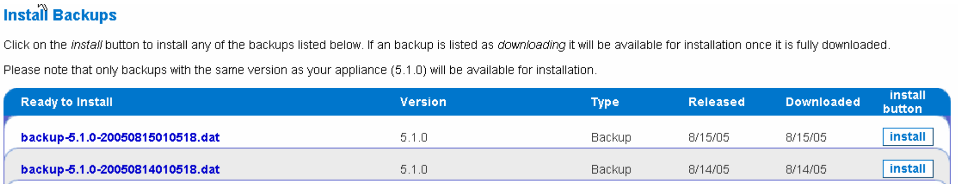
Figure 49 Download Backup Files

5. Click a file to begin the download.

Install a Backup File

If restoring a backup file to a new piece of hardware, contact Raritan Support for assistance in migrating the data.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Advanced Administration**.
3. Click **Data Backup and Restore.**
4. Click **Install Backup.**



Install Backups

Click on the *install* button to install any of the backups listed below. If an backup is listed as *downloading* it will be available for installation once it is fully downloaded.

Please note that only backups with the same version as your appliance (5.1.0) will be available for installation.

Ready to Install	Version	Type	Released	Downloaded	install button
backup-5.1.0-20050815010518.dat	5.1.0	Backup	8/15/05	8/15/05	install
backup-5.1.0-20050814010518.dat	5.1.0	Backup	8/14/05	8/14/05	install

Figure 50 Install Backup Files

5. Click **install** next to a backup file to install the file. Only backups with the same version as the appliance will be available for installation.
6. You can click the backup file name to view details of the file.

Manually Upload a Backup File

For those who do not have Internet access or choose not to use the web-based upload functionality, backup files can be manually uploaded to the CC-NOC.

The **Upload File:** dialog box was created to facilitate that upload. Note that only valid Raritan backup files can be uploaded to this appliance. The upload of other files may cause problems with the appliance and may void your warranty.

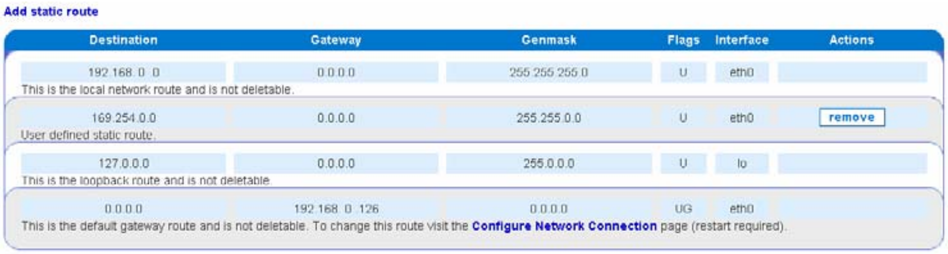
1. Click on the **Admin** tab in the top navigation bar.
2. Click **Advanced Administration**.
3. Click **Data Backup and Restore.**
4. Click **Browse:**
5. Select the backup file to upload and click **Open**.
6. Click **upload**.
7. Install the backup file as described in the previous section – see section **Install a Backup File** earlier in this chapter.

Manage Routes

This page allows you to add and remove static routes to networks and/or hosts in your environment. This may be critical if you have multiple routers on the local segment which lead to distinct, different parts of your network. The local network and loopback routes are not deletable.

1. Click on the **Admin** tab in the top navigation bar.

2. Click **Advanced Administration**.
3. Click **Manage Routes.**



Add static route

Destination	Gateway	Genmask	Flags	Interface	Actions
192.168.0.0	0.0.0.0	255.255.255.0	U	eth0	
This is the local network route and is not deletable.					
169.254.0.0	0.0.0.0	255.255.0.0	U	eth0	remove
User defined static route.					
127.0.0.0	0.0.0.0	255.0.0.0	U	lo	
This is the loopback route and is not deletable.					
0.0.0.0	192.168.0.126	0.0.0.0	UG	eth0	
This is the default gateway route and is not deletable. To change this route visit the **Configure Network Connection** page (restart required).					

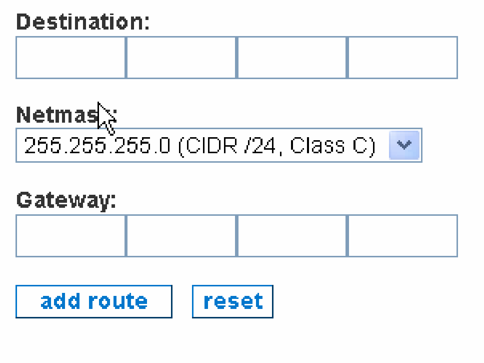
Figure 51 Manage Routes

4. To delete a user-defined static route, click **remove** in the row of the unwanted route**.**
5. To change the default gateway route, revisit the **Configure Network Connection** page – see **Configure Network Connection** earlier in this chapter for additional information. A restart is required.

Add a New Network Route

To add a new network route:

1. Above the route table, click **Add static route**.



Destination:

Netmask:
255.255.255.0 (CIDR /24, Class C)

Gateway:

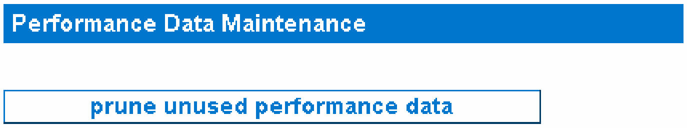
Figure 52 Add a New Network Route

2. Type the destination address, netmask, and gateway for the new network route. The gateway is optional.
3. Click **add route**.

Prune Unused Performance Data

This page will search for performance data that remains from deleted nodes, Windows computers, and satellite appliances. If you have made drastic changes to your network recently, running this might help you reclaim some disk space on this appliance.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Advanced Administration**.
3. Click **Prune Unused Performance Data.**



Performance Data Maintenance

Figure 53 Prune Unused Performance Data

4. Click **OK** when asked to confirm.

Delete Management Settings and Data

This page gives you a way to completely reset the appliance to nearly a "factory default" state, deleting all collected information and configuration settings.

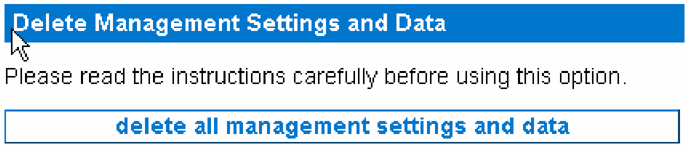
Warning! *This action is irreversible. If you download a backup of your data, you can restore it to the appliance later if necessary, but if you do not download a backup, all of your data will be lost permanently.*

However, unlike resetting the appliance to a factory default that you can do while connected to a serial connection – see Raritan's *CommandCenter NOC Deployment Guide*, this option keeps the current version of software, the license file, and the network settings of this appliance, for example, IP address. Once deleted, the appliance will restart at the Configuration Wizard and let you set the appliance up from scratch.

Windows Management appliances communicate directly with the management data on the CC-NOC. If the management data is deleted on the CC-NOC while a Windows Management appliance is connected, the Windows Management appliance may continue to send events and performance data with incorrect information.

Note: *In a distributed environment, please shut down all Windows Management appliances, that is, a CC-NOC 2500M that may be connected to the CC-NOC 2500N.*

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Advanced Administration**.
3. Click **Delete Management Settings and Data.**



Delete Management Settings and Data

Please read the instructions carefully before using this option.

Figure 54 Delete Management Settings and Data

4. Click **delete all management settings and data**.
5. Confirm your choice on whether to proceed or not.

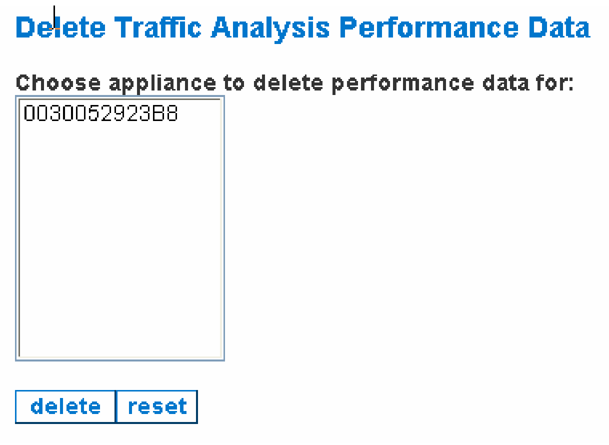
Delete Traffic Analysis Performance Information

This page will search for traffic analysis performance data and remove it. If you have made drastic changes to your network recently, running this might help you reclaim some disk space on this appliance.

Note: *Traffic analysis performance data is stored in backup files.*

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Advanced Administration**.

3. Click **Delete Traffic Analysis Performance Information.**



Delete Traffic Analysis Performance Data

Choose appliance to delete performance data for:

0030052923B8

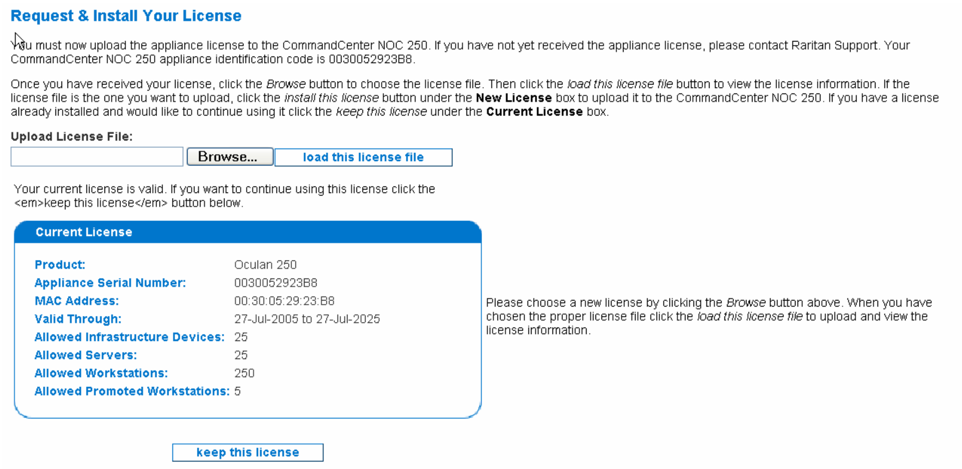
Figure 55 Delete Traffic Analysis Performance Data

4. Choose the appliance on which to delete the performance data**.**
5. Click **delete**.

Install CC-NOC License

This page allows you to upload a new license file to the CC-NOC. You were asked to do this during installation of the CC-NOC or when configuring the network – see Raritan's *CommandCenter NOC Deployment Guide*). If you have not yet received the appliance license, please contact Technical Support.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Install CommandCenter NOC License.**



Request & Install Your License

You must now upload the appliance license to the CommandCenter NOC 250. If you have not yet received the appliance license, please contact Raritan Support. Your CommandCenter NOC 250 appliance identification code is 0030052923B8.

Once you have received your license, click the *Browse* button to choose the license file. Then click the *load this license file* button to view the license information. If the license file is the one you want to upload, click the *install this license* button under the **New License** box to upload it to the CommandCenter NOC 250. If you have a license already installed and would like to continue using it click the *keep this license* under the **Current License** box.

Upload License File:

Your current license is valid. If you want to continue using this license click the <em>keep this license</em> button below.

Current License

Product:	Oculan 250
Appliance Serial Number:	0030052923B8
MAC Address:	00:30:05:29:23:B8
Valid Through:	27-Jul-2005 to 27-Jul-2025
Allowed Infrastructure Devices:	25
Allowed Servers:	25
Allowed Workstations:	250
Allowed Promoted Workstations:	5

Please choose a new license by clicking the *Browse* button above. When you have chosen the proper license file click the *load this license file* to upload and view the license information.

Figure 56 Install a new License File

3. Click **Install CommandCenter NOC License.**
4. Click **Browse** to choose the license file.
5. Click **load this license file** to view the license information.
6. If the license file is the one you want to upload, click **install this license** under the **New License** box to upload it to the CC-NOC.
7. If you have a license already installed and would like to continue using it, click the **keep this license** under the **Current License** box.

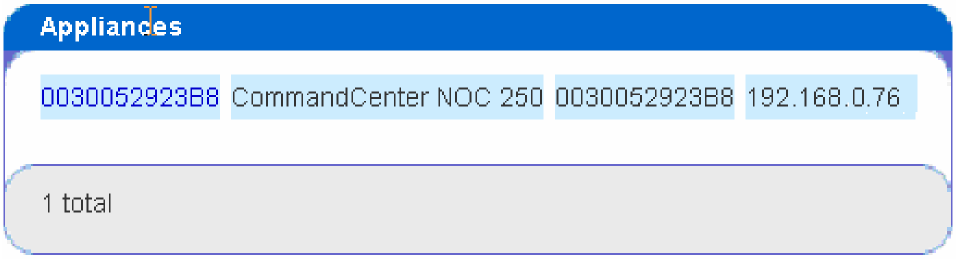
Note: *In a distributed environment, to install a license for a CC-NOC 2500M or CC-NOC 2500S, from the CC-NOC 2500N click on the* ***Admin*** *tab, click* ***Upload Appliance Licenses****, and click* ***load new appliance license****.*

Installed Appliances List

Use this page to change the name or description of a CC-NOC and disable specific functionality on the appliance.

The Raritan suite of services includes a series of hardware-based and software-based solutions to address the entire complement of network, systems, and security management for your organization.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Installed Appliances List.**



Appliances

0030052923B8	CommandCenter NOC 250	0030052923B8	192.168.0.76

1 total

Figure 57 Installed Appliances List

The table above reflects all of the appliances that have been configured to report information back to this Web Console. This listing of appliances also includes a free-form note with each entry, allowing you to change the name that the appliance uses when it reports to the Web Console, as well as to provide additional information about that appliance, such as where it is installed, whom to contact if there are problems in that environment, or a specific problem you may be using the appliance to troubleshoot.

Note: *In a distributed environment, you need to shutdown all CC-NOC appliances that may be connected to the CC-NOC 2500N before changing the name.*

3. To change the name or note associated with any given appliance, click the current name of the appliance to be redirected to a page where this change is possible. Note that this functionality is only available to the **admin** user.

Chapter 3: Configuring Intrusion Detection

This chapter describes procedures to configure a CC-NOC so it can monitor and analyze system events for attempts to access system resources in an unauthorized manner. In the event of an attack, real-time alerts can be sent to specified individuals.

Intrusion detection can be configured to run on a CC-NOC 100, CC-NOC 250, or on a CC-NOC 2500S in a distributed environment. Typically, you would place a CC-NOC on the "inside interface" of your firewall. To configure a CC-NOC 2500S with intrusion detection, use the web user interface of a CC-NOC 2500N.

***Note**: Please see **Appendix E: Managing and Responding to Intrusion Detection Events** for more details.*

Configure a Spanned or Mirrored Port

Devices must be able to see packets passing on a network in order for intrusion detection and network performance to function properly. To accomplish this, configure a "mirrored" or "spanned" port on your network. We recommend the following resources to help you configure the port:

- For Cisco Catalyst switches: http://www.cisco.com/warp/public/473/41.html
- For HP Procurve switches, download the Management and Configuration Guide for your switch: http://www.hp.com/rnd/support/manuals/index.htm
- For 3Com switches, see the appropriate manuals for configuration of the "Roving Analysis Port".

To ensure that the CC-NOC is passing packets correctly, you can view your network traffic – please see Raritan's *CommandCenter NOC User Guide* for additional information on viewing network traffic.

Ethernet TAP

Instead of using a spanned or mirrored port, an Ethernet tap could be used that may be considered a more secure method in which to listen to network traffic than a spanned port.

An Ethernet TAP passes data between two network ports. Additionally, it outputs data from the two network ports to either two half-duplex monitoring ports or to a single aggregated full-duplex monitoring port. The CC-NOC monitoring port connects to a full-duplex Ethernet TAP monitoring port.

Benefits

An Ethernet TAP operates at the electrical level instead of the network level so it mirrors the traffic on the wire precisely, without altering it in any way. Also, the TAP monitoring port is unidirectional. Therefore, using an Ethernet TAP has several advantages over a hub or spanned port:

- The traffic is always precisely mirrored without alteration.
- The traffic flows one direction out of the Ethernet TAP so there is no chance that an intruder (or any user of the network) could detect the fact that the CC-NOC is monitoring the traffic.
- Since there are no output wires connecting the monitoring port of the CC-NOC to the network, there is no chance that the CC-NOC could accidentally send traffic out of the port.

Deployment

Place the Ethernet TAP on the Ethernet cable in the same location where an Ethernet hub would be used. The Ethernet tap has the exact same function as the hub, except that one of the ports is uni-directional and outputs data that is passing over the wire. This is the port that is connected to CC-NOC's monitoring interface.

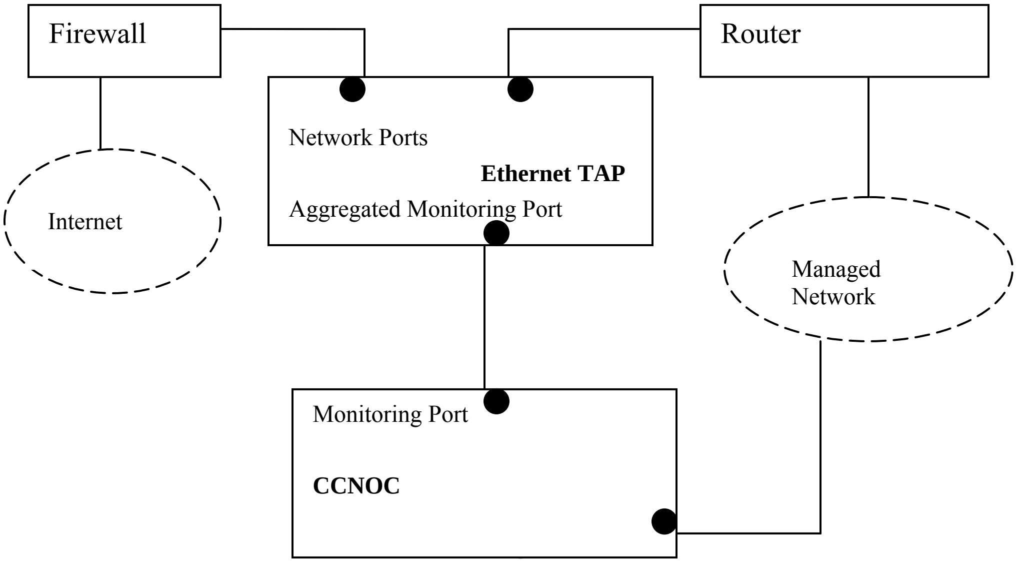


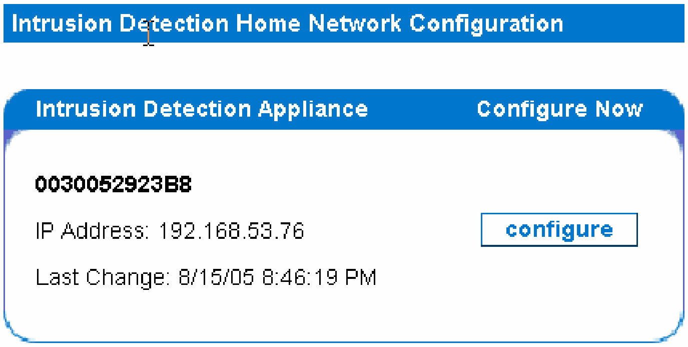
Figure 58 Ethernet TAP Deployment

Configure Appliance Home Networks

The CC-NOC that has been selected to handle intrusion detection will detect some signatures differently depending on whether or not they are incoming or outgoing from the home network. For this reason, it is important to set up the home network for the device to ensure that the intrusion detection is as accurate as possible and that the number of false positive alerts is minimized.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Intrusion Detection Configuration**.
3. Click **Configure Home Appliance Networks**.

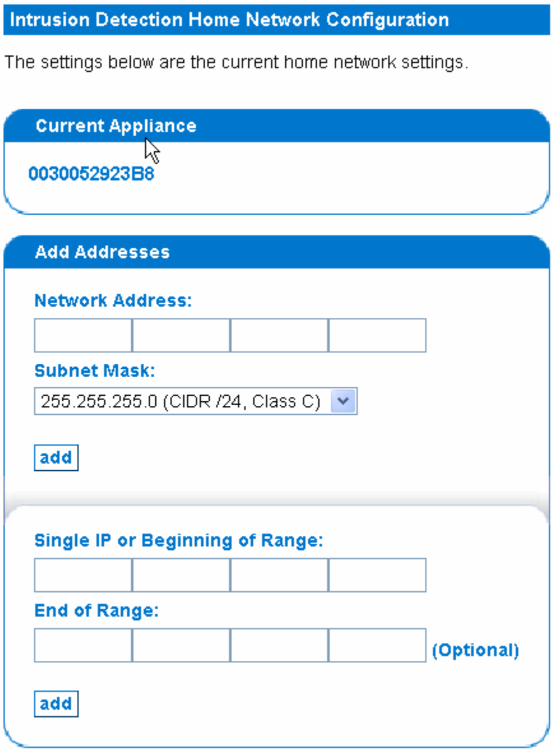
All of the Intrusion Detection appliances that can communicate with this system are listed in the box. The **Last Change** field indicates the last time that the home network for the appliance was changed.


Intrusion Detection Home Network Configuration

Intrusion Detection Appliance	Configure Now
0030052923B8 IP Address: 192.168.53.76 Last Change: 8/15/05 8:46:19 PM	configure

Figure 59 Selecting an Intrusion Detection Appliance for Home Network Configuration

4. Choose the appliance that you wish to configure by clicking **Configure** next to it.



Intrusion Detection Home Network Configuration

The settings below are the current home network settings.

Current Appliance

0030052923B8

Add Addresses

Network Address:

Subnet Mask: 255.255.255.0 (CIDR /24, Class C)

Single IP or Beginning of Range:

End of Range: (Optional)

Figure 60 Configuring Home Network for Intrusion Detection Appliance

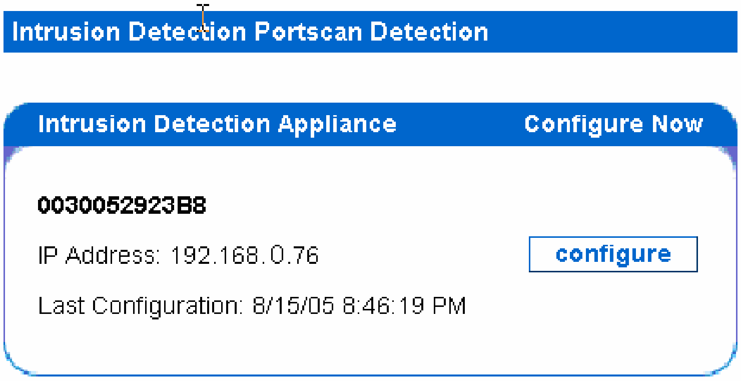
5. To include an entire subnet in your home network, use the **Add Addresses** box. Type in the network address and select the subnet mask from the list that is provided.
6. To include single hosts or ranges of host IP addresses, use the input boxes in the bottom half of the panel. Please note that you can only add a maximum of 50 "stray" IP addresses that are not a part of a subnet. This includes individual addresses and all addresses within your ranges**.**
7. Click **finish configuration.**

Configure Port Scan Detection

Intrusion Detection appliances can perform stateful inspection of packets to detect port scanning activity, that is, the probing for openings and availabilities in a network on your network. However, some legitimate services that open multiple connections to hosts, like DNS, NFS, and SMB, may produce false-positive port scan events. Use this page to exclude servers that generate false-positive port scan events from port scan detection.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Intrusion Detection Configuration**.
3. Click **Configure Portscan Detection**.

All of the Intrusion Detection appliances that can communicate with this system are listed in the box. The **Last Change** field indicates the last time that the home network for the appliance was changed.



Intrusion Detection Portscan Detection

Intrusion Detection Appliance — Configure Now

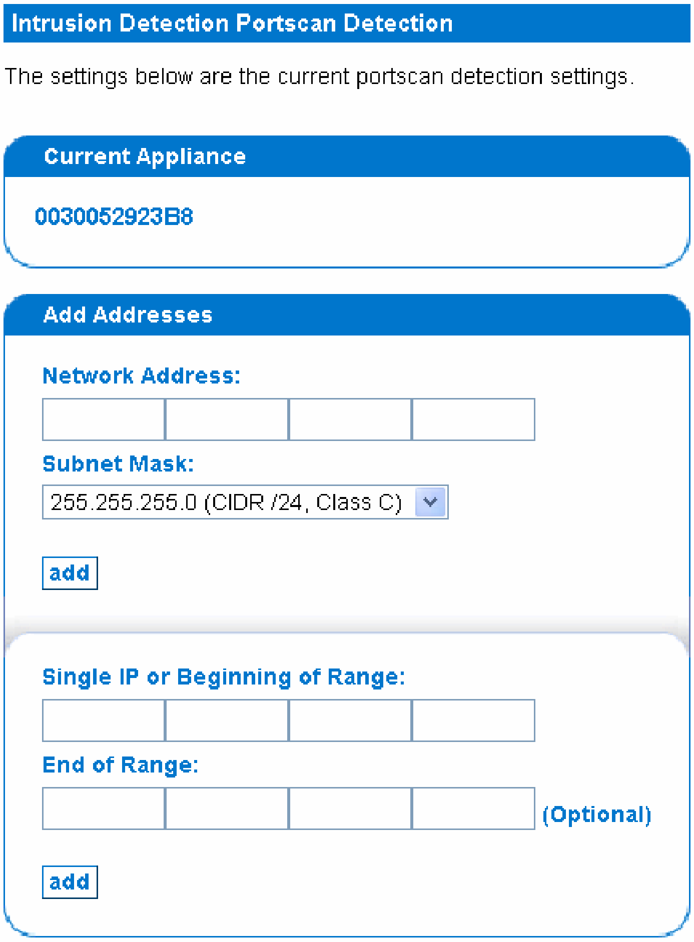
0030052923B8

IP Address: 192.168.0.76

Last Configuration: 8/15/05 8:46:19 PM

Figure 61 Selecting an Intrusion Detection Appliance for Portscan Detection

4. Choose the appliance that you wish to configure by clicking **Configure** next to it.



Intrusion Detection Portscan Detection

The settings below are the current portscan detection settings.

Current Appliance

0030052923B8

Add Addresses

Network Address:

Subnet Mask: 255.255.255.0 (CIDR /24, Class C)

Single IP or Beginning of Range:

End of Range: (Optional)

Figure 62 Configuring Portscan Detection for an Intrusion Detection Appliance

Determining which ports are open on a target machine is often the first step towards a successful attack on a network system. Attackers generally use port scanning utilities to probe a target system and make a list of all open ports on the device. After they have this list, they will send specific attacks to the open ports with the hope of exploiting a vulnerability on the target. The port scanning process is often detectable by monitoring traffic to the target machine. However, the normal activity of some services such as DNS and NFS often resembles the activity of an attacker executing a portscan against a target system.

5. To exclude an entire subnet from portscan analysis, use the **Add Addresses** box. Type in the network address and select the subnet mask from the list that is provided.
6. To include single hosts or ranges of host IP addresses, use the input boxes in the bottom half of the panel. Please note that you can only add a maximum of 50 "stray" IP addresses that are not a part of subnet. This includes individual addresses and all addresses within your ranges**.**
7. To prevent detection of portscans originating from the home network of the appliance, check the **Exclude all traffic originating from your home network...** check box. This can prevent some types of false-positives, such as the traffic generated by a host on your network that is simultaneously accessing several services on a remote host.
8. To exclude all DNS and SMB traffic on your network from portscan analysis, use the check boxes in the bottom exclusion pane.
9. Click **finish configuration**.

Enable/Disable Signature Types via Signature Profiler

With the **Intrusion Detection Signature Profiler**, it is possible to enable and disable types of intrusion detection on the CC-NOC. A properly configured CC-NOC will detect patterns in network traffic that identify a potential threat. By tuning the set of signature rules that the CC-NOC reacts to, the intrusion detection can be configured to detect attacks affecting the specific devices and services on your network.

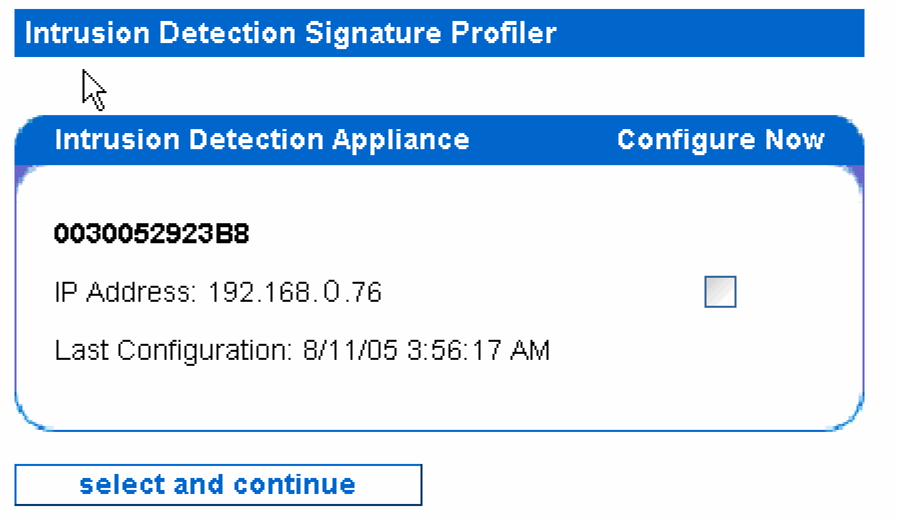
Once you’ve created the signature rules, the CC-NOC will then use these rules to dynamically select which signatures apply to your environment, relieving you of the burden of ongoing signature administration.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Intrusion Detection Configuration**.
3. Click **Intrusion Detection Signature Profiler**.

Select Intrusion Detection Appliance(s)

All of the Intrusion Detection appliances that can communicate with the system hosting this Web Console are listed in the Intrusion Detection Appliance box. The **Last Configuration** field indicates the last time that the detection scheme for the Intrusion Detection was changed or the last time that a security patch was used to update the signatures on the Intrusion Detection. Enabling automatic updates provides up-to-date signatures – see **System Software & Signature Updates** in **Chapter 2: General and Advanced Administration** for additional information.

If an Intrusion Detection appliance is listed as **Not Configured**, you must use the Signature Profiler to configure its signatures so that it can begin relaying events.



Intrusion Detection Signature Profiler

Intrusion Detection Appliance	Configure Now
0030052923B8 IP Address: 192.168.0.76 Last Configuration: 8/11/05 3:56:17 AM	□

Figure 63 Selecting Intrusion Detection Appliances for Signature Profiler

4. To configure one or more Intrusion Detection appliances with identical configurations, check the boxes under the **Configure Now** heading.

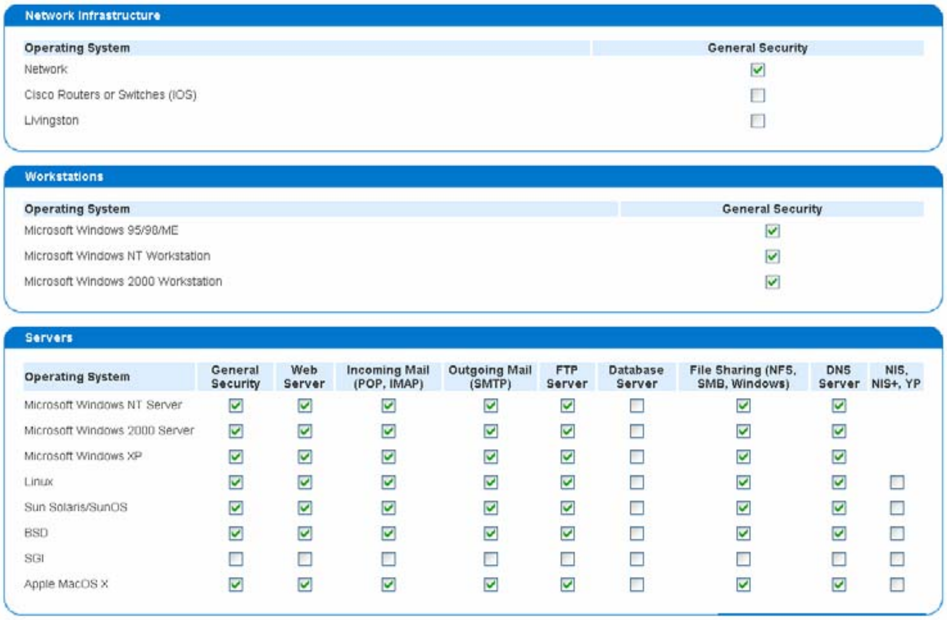
Note: *The CC-NOC 100 and CC-NOC 250 only supports a single network segment connected to the traffic sniffing port. To monitor additional network segments, configuring a CC-NOC 2500N with multiple CC-NOC 2500S appliances is necessary.*

5. Click **Select and continue** when you have made your selection.
6. Choose the appliance that you wish to configure by clicking **Configure** next to it.

Select Types of Signatures to Monitor

When in doubt, enable detection. There is no disadvantage to enabling extra detection, except that you may receive extraneous events from your Intrusion Detection appliances. You should usually never disable detection of **General Security** on the **Network**. This category includes a variety of attacks that can affect any network, regardless of the devices and services on it. Some signatures that affect multiple operating systems are always enabled, regardless of the signatures that you select below.

If your network does not contain any devices or services of a type listed below, you may wish to disable detection of signatures that only affect that device or service. For instance, if you have Linux servers but none of them are running an FTP service, you may wish to disable detection of signatures that only affect FTP services on Linux. Or, if you do not have any Windows 95/98/ME workstations, you may want to disable **General Security** for those machines to reduce the number of false-positive events that may be generated.



Network Infrastructure

Operating System	General Security
Network	☑
Cisco Routers or Switches (IOS)	□
Livingston	□

Workstations

Operating System	General Security
Microsoft Windows 95/98/ME	☑
Microsoft Windows NT Workstation	☑
Microsoft Windows 2000 Workstation	☑

Servers

Operating System	General Security	Web Server	Incoming Mail (POP, IMAP)	Outgoing Mail (SMTP)	FTP Server	Database Server	File Sharing (NFS, SMB, Windows)	DNS Server	NIS, NIS+, YP
Microsoft Windows NT Server	☑	☑	☑	☑	☑	□	☑	☑	
Microsoft Windows 2000 Server	☑	☑	☑	☑	☑	□	☑	☑	
Microsoft Windows XP	☑	☑	☑	☑	☑	□	☑	☑	
Linux	☑	☑	☑	☑	☑	□	☑	☑	□
Sun Solaris/SunOS	☑	☑	☑	☑	☑	□	☑	☑	□
BSD	☑	☑	☑	☑	☑	□	☑	☑	□
SGI	□	□	□	□	□	□	□	□	□
Apple MacOS X	☑	☑	☑	☑	☑	□	☑	☑	□

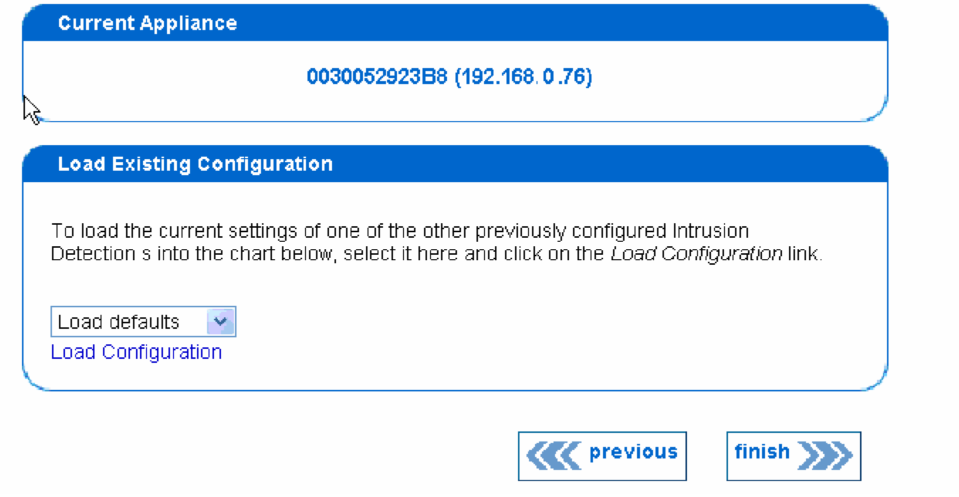
Figure 64 Selecting Signature Types

7. To enable detection of a type of signature, check the check box for the type of signature.
8. To disable detection, uncheck the check box.
9. When you have changed the settings to reflect the devices and services on your network, click **Finish**.

Load Default Signatures or Settings from Another Appliance

Alternatively, you can quickly configure your Intrusion Detection appliance by selecting a set of pre-selected signatures appropriate for most networks or by selecting a previously saved appliance's signature settings.

10. To load the defaults, select **Load defaults** from the drop-down selection list and click **Load Configuration**.
11. To load a previously saved signature setting from a particular appliance, select the **appliance** from the drop-down selection list and click **Load Configuration.**



Current Appliance

0030052923B8 (192.168.0.76)

Load Existing Configuration

To load the current settings of one of the other previously configured Intrusion Detection s into the chart below, select it here and click on the *Load Configuration* link.

Load defaults

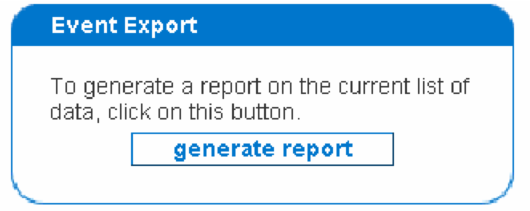
Figure 65 Load Intrusion Detection Settings

12. When you have changed the settings to reflect the devices and services on your network, click **Finish**.

Delete Intrusion Detection Performance Data

Use this option to delete and reset the intrusion detection performance data for one or more intrusion detection appliances.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Intrusion Detection Configuration**.
3. Click **Delete Performance Information**.



Event Export

To generate a report on the current list of data, click on this button.

Figure 66 Deleting Intrusion Detection Performance Data

4. From the list or appliances, highlight the CC-NOC from the selection box and click **delete.** The intrusion detection performance data will be deleted and reset.

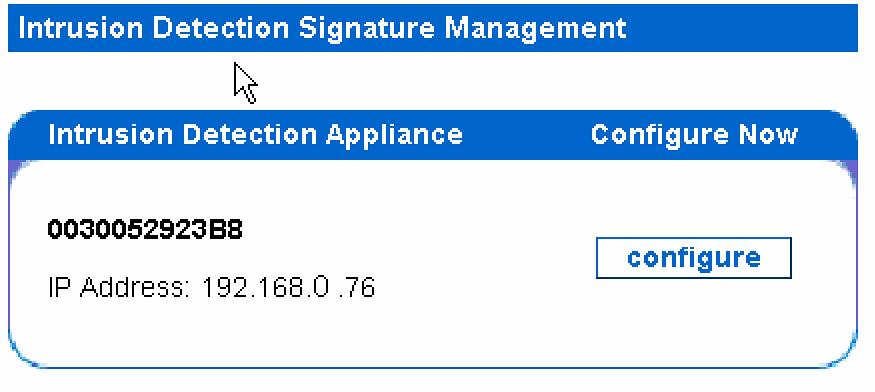
Advanced Intrusion Detection Administration

Advanced administration assists in fine tuning the set of signatures that an intrusion detection application will use to detect intrusion traffic on the network.

Manage Signatures

The **Manage Signatures** page allows you to disable specific signatures on a per-appliance basis. This allows you to disable signatures that may produce false-positive alerts because of conditions on your network. These settings will take precedence over the broader categories that may be selected in the Signature Profiler.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Intrusion Detection Configuration**.
3. Click **Advanced Security Administration**.
4. Click **Manage Signatures**.

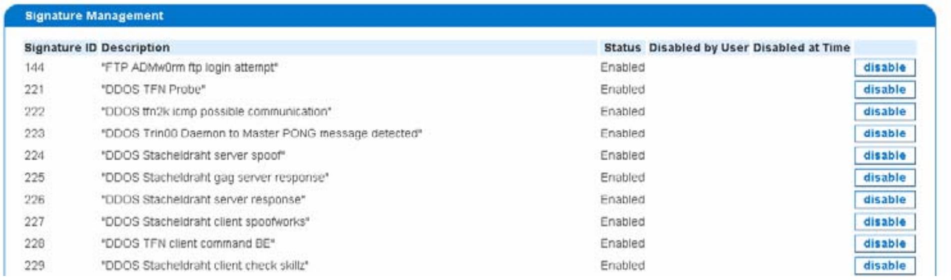


Intrusion Detection Signature Management

Intrusion Detection Appliance	Configure Now
0030052923B8 IP Address: 192.168.0 .76	configure

Figure 67 Selecting an Intrusion Detection Appliance for Changing Signature Set

5. Select the appliance you wish to enable/disable signatures for by clicking **configure** next to it.



Signature Management

Signature ID	Description	Status	Disabled by User	Disabled at Time	
144	"FTP ADMw0rm ftp login attempt"	Enabled			disable
221	"DDOS TFN Probe"	Enabled			disable
222	"DDOS tfn2k icmp possible communication"	Enabled			disable
223	"DDOS Trin00 Daemon to Master PONG message detected"	Enabled			disable
224	"DDOS Stacheldraht server spoof"	Enabled			disable
225	"DDOS Stacheldraht gag server response"	Enabled			disable
226	"DDOS Stacheldraht server response"	Enabled			disable
227	"DDOS Stacheldraht client spoofworks"	Enabled			disable
228	"DDOS TFN client command BE"	Enabled			disable
229	"DDOS Stacheldraht client check skillz"	Enabled			disable

Figure 68 Generating New Signature Set

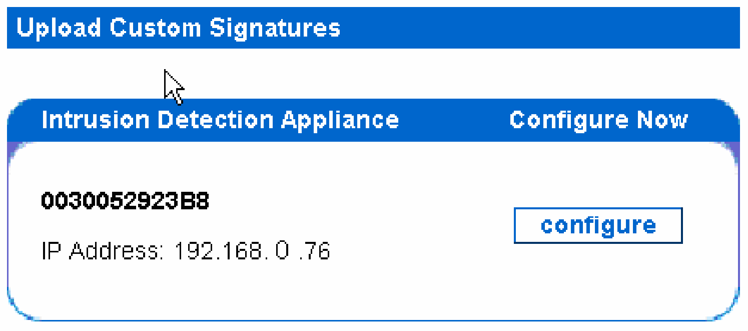
6. After you have finished making any changes to the signature set, you will need to manually generate a new signature set so that the appliance will get the latest settings. Click **generate new signature set** at the bottom of the screen to generate the signature set.

Within several minutes, the signatures will be generated and the CC-NOC will load the new settings and continue to monitor for security events.

Upload Custom Signatures Tool

The **Upload Custom Signatures** page allows you to upload a specific set of rules that will be sent to a specified Intrusion Detection appliance. This feature can be used to augment the set of signatures that Raritan provides as part of the ongoing software updates for the appliance.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Intrusion Detection Configuration**.
3. Click **Advanced Security Administration**.
4. Click **Upload Custom Signatures**.

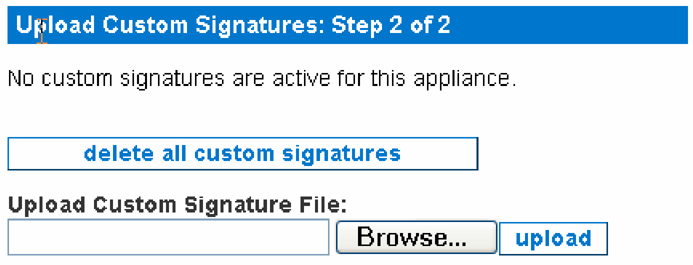


Upload Custom Signatures

Intrusion Detection Appliance	Configure Now
0030052923B8 IP Address: 192.168. 0 .76	configure

Figure 69 Selecting an Intrusion Detection Appliance for Changing Signature Set

5. Click **configure** next to the appliance you wish to upload a specific set of signatures.



Upload Custom Signatures: Step 2 of 2

No custom signatures are active for this appliance.

Figure 70 Selecting an Intrusion Detection Appliance for Changing Signature Set

6. Click **Browse** to open a custom signature file. The custom signature file that is uploaded must adhere to these rules:

- Custom signatures must be in a file with one signature entry per line.
- Comment lines must begin with the "#" character.
- The signatures must be in Snort-compatible format, with no blank lines in the file.
- Click **upload**.

Hints and Tips:

- Custom signatures will take precedence over all stock signatures that are produced by the Signature Profiler.
- The signatures will apply to incoming packets in the order that they appear in the file.
- You may upload multiple files containing signatures. The signatures will apply to incoming packets in the order that the files were uploaded.
- To delete the current set of custom signatures for this appliance, click **Delete All Custom Signatures**.
- Keep a backup of the signature files that you have uploaded; the only way to change custom signature settings is to delete the existing custom signatures and upload a new set.

After you have uploaded new custom rules, it will take several minutes for the rules to be activated by the Intrusion Detection service.

Chapter 4: Configuring Windows Management

This chapter describes procedures to configure a CC-NOC so it can use Microsoft's WMI (Windows Management Instrumentation) to monitor and manage Windows servers and workstations in your network. WMI information is collected from the Windows systems and is used to extract and report on inventory and event information. With Windows Management configured, you can also remotely start and stop services on managed Windows systems that are licensed with a server license.

Note: *If you are using a CC-NOC 100/250, windows management is configured on the appliance itself. If you have a distributed environment, windows management is relegated to a CC-NOC 2500M and configuration is performed via the web user interface of a CC-NOC 2500N.*

Windows Management Instrumentation (WMI)

This feature assists in the labor-intensive task of managing Windows servers and workstations. Leveraging Microsoft's Windows Management Instrumentation (WMI), a version of WBEM with support for Windows-specific management metrics and operations, keeps you abreast of the status of Windows platforms in your network. For example, with Windows Management, you can:

- Check that all MS Office applications are legally licensed.
- Obtain a list of workstations that have just installed new software.
- Pinpoint machines that are running Spyware, which should be uninstalled.

For Windows servers, for example, Windows 2000 Server and Windows 2003 Server and for Windows workstations, for example, Windows 2000, Windows 2003, Windows XP Professional, WMI provides this information:

	Windows Servers	Windows Workstations
Hardware Inventory	√	√
Software Inventory	√	√
Service Status and Management	√	
Event Logs	√	
Performance Metrics	√	

Note: *By default, WMI is supported on Windows 2000, Windows XP Professional, or Windows 2003 systems. It is not supported on Windows 95/98/NT systems. However, you can download software from Microsoft to enable WMI support – please see* ***Appendix D: Setting up WMI on Target Machines*** *for additional information.*

The Windows Management system provides hardware, software, and configuration inventory data, allowing you to make informed decisions when responding to user calls for help, even if the system is currently unavailable.

Configure an External Windows Proxy

To collect WMI data from managed Windows systems, an external proxy needs to be configured which will forward WMI requests from the CC-NOC to the managed Windows systems. If you are using a CC-NOC 2500M for Windows Management, it can use its own internal proxy or you can use the steps below to configure an external proxy.

External Proxy Host Requirements

For best results, it is recommended to use Windows XP Professional, Service Pack 2 (or later) with auto updates enabled to facilitate communications between CC-NOC and the managed systems.

The external proxy needs to meet these requirements:

- 1000 MHz CPU or higher
- 512 MB of RAM or higher
- Windows XP Professional with Service Pack 2 or higher
- Non-mission-critical role on your network

Overview

To configure a CC-NOC so it collects WMI data, you need to:

1. Configure an external system within the environment to act as a Proxy for gathering WMI data, unless you are using a CC-NOC 2500M's internal proxy, by downloading and running a provided configuration tool.
2. Configure the CC-NOC with the proper permissions, for example, domain or individual system permissions, to interact with both the Proxy and the target systems.

Note: *It is recommended to configure one proxy per subnet unless you have configured a WINS server in your environment. You can also specify LMHOST file entries on a CC-NOC 2500M for name resolution – see* ***Configure WINS*** *later in this chapter for details.*

The next few sections explain how to perform the above tasks. Please follow the steps below to ensure optimal performance on your Windows external proxies as they collect management information.

Download and Run `ProxyInstaller`

Configuring a system as a proxy is accomplished in two steps. The first step is to remove the legacy proxy settings on the external system if you are using a 5.0 version or earlier and download the newest proxy configuration program. The second step is to run ProxyInstaller. ProxyInstaller only edits registry settings; additional software is not installed.

Note*: If you have a CC-NOC 5.0 or earlier and are experiencing problems with your current external proxy, it is recommended to upgrade to CC-NOC 5.4 proxy.*

You must repeat these steps on all Windows machines that are acting as an external proxy for CC-NOC 100, 250, or 2500M. CC-NOC 2500M acts on its own as a Windows management proxy; no action is required to migrate it to a new configuration and all updates to CC-NOC 2500 are automatic.

To configure an external proxy:

1. Ensure you have Administrator privileges on the external proxy.
2. If you have a CC-NOC 5.0 or earlier:
   a) Download the installed legacy program (`cfgproxy.exe`) on CC-NOC 100, CC-NOC 250, or CC-NOC 2500N from the following URL:
   `http://<Your_CommandCenter_NOC_IP>/public/cfgproxy.exe`
   b) Remove legacy proxy settings, run the `cfgproxy.exe` program with the "uninstall" option:
   ```
   c:\> cfgproxy.exe -u
   ```
3. Download the newest proxy configuration program, `ProxyInstaller`, from this location: `http://<address_of_noc>/public/ProxyInstaller.zip`

4. Unzip the `ProxyInstaller` archive on your Windows machine and move the directory to a location where you would like to keep the program. For example, a good location could be: `C:\Program Files\Raritan\ProxyInstaller`
5. Double-click on `ProxyInstaller.exe` to run the program.
6. Type in either the Remote Appliance (CC-NOC 2500M) IP address or the Manager Server (CC-NOC 100 or 250) IP address depending on the type of series you are installing.
7. Press the **Install** button to reconfigure your external Windows machine with the latest proxy settings.

Open Ports on External Proxy Host

In order for a CC-NOC appliance to query Windows performance data from devices on your network, the firewall on any target Windows devices may require modification. The following ports on any target Windows device must accept traffic from the IP address of a CC-NOC 2500M or any system configured as an external Windows proxy:

- 137 udp
- 139 tcp
- 445 tcp

To open these ports on any Windows XP (SP2) machine running a Windows firewall, use the following procedure:

1. Open a **cmd** prompt and enter the following command:

```
netsh firewall set service type = fileandprint mode = enable scope =
custom address = <address of external proxy or 2500M>
```

For example, if the IP address of your external proxy or CC-NOC 2500M is 192.168.1.45, then you would enter:

```
netsh firewall set service type = fileandprint mode = enable scope =
custom address = 192.168.1.45
```

2. Enter the following command:

```
netsh firewall set service type = remoteadmin mode = enable scope =
custom address = <address of external proxy or 2500M>
```

For example, if the IP address of your external proxy or CC-NOC 2500M is 192.168.1.45, then you would enter:

```
netsh firewall set service type = remoteadmin mode = enable scope =
custom address = 192.168.1.45
```

By default, Windows XP (SP2) enables the “Force Guest” option in the registry. A CC-NOC appliance cannot authenticate a Windows system that has the “Force Guest” option enabled. To disable the “Force Guest” option, you must modify the registry by using the following procedure:

1. Backup the registry.
2. From the **Run** prompt, enter the following command:

```
Regedit
```

3. Navigate to this registry key:

```
Hkey_Local_Machine\System\CurrentControlSet\Control\LSA\Forceguest
```

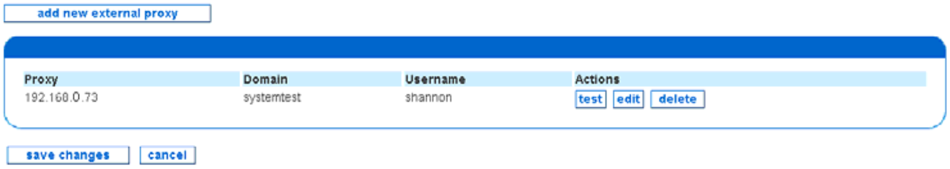
4. Change the value of the “**Forceguest**” key from **1** (enabled) to **0** (disabled).

Configuring the CC-NOC to communicate with the Proxy

To configure the CC-NOC to communicate with the Proxy system in the environment is accomplished by using the Windows Management Configuration Wizard.

The Windows Management Configuration Wizard is an interface to specify and configure *proxy hosts*, which facilitate connectivity between the CC-NOC and your managed Windows servers and workstations. This configuration wizard walks you step-by-step through the creation of proxies, association of authentication information with specific domains, and the ability to associate authentication information with specific hosts as well.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Windows Management Configuration**.
3. Click **Windows Management Configuration Wizard**.
4. Click **start configuration** to launch the wizard.



Proxy	Domain	Username	Actions
192.168.0.73	systemtest	shannon	test edit delete

Figure 71 Configure an External Proxy for Windows Management

5. Click **add new external proxy**.

Note: *To access the Windows Management Configuration Wizard in a distributed environment, that is, from a CommandCenter 2500N, in the navigation tab bar at the top click on the* ***Admin*** *tab, then* ***CC-NOC 2500M Configuration****. Click* ***CommandCenter NOC 2500M Configuration Wizard*** *or click* ***configure*** *next to the appliance you are currently configuring.*

Identifying Local Proxy

The local proxy host specified here will be central to communications with some subset (or all) of your managed Windows platforms, allowing the CC-NOC to request information from a particular server or workstation, which this proxy will then translate into a Microsoft proprietary protocol and pass on to the end system.

Note: *This step is required only if using an external proxy. If you are using a CC-NOC 2500M, you can use its own internal proxy.*

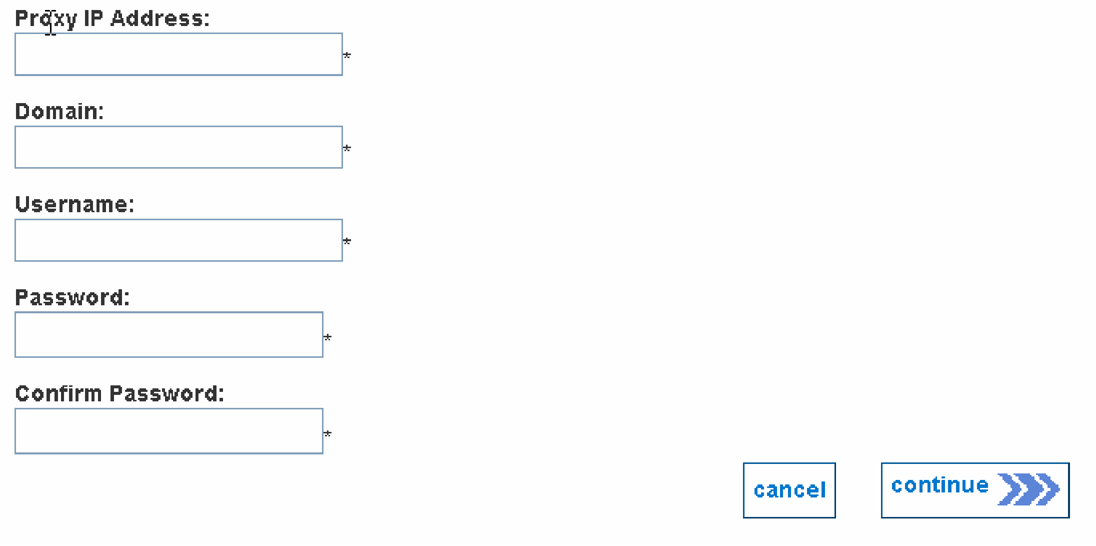


Figure 72 Specifying proxy host information

6. Type the **IP address** for the proxy host. This should be the same host that the configuration tool was run – see section **Download and Run** earlier in this chapter for additional information.

***Note:** Hostname values in this field must be resolvable via DNS or must be a numeric IP address.*

7. Type values for **domain**, **username**, **password**, and confirm the password. Note that the username must be a local user on that system, which is a member of the Local Administrators group.
8. Click **continue** to proceed.

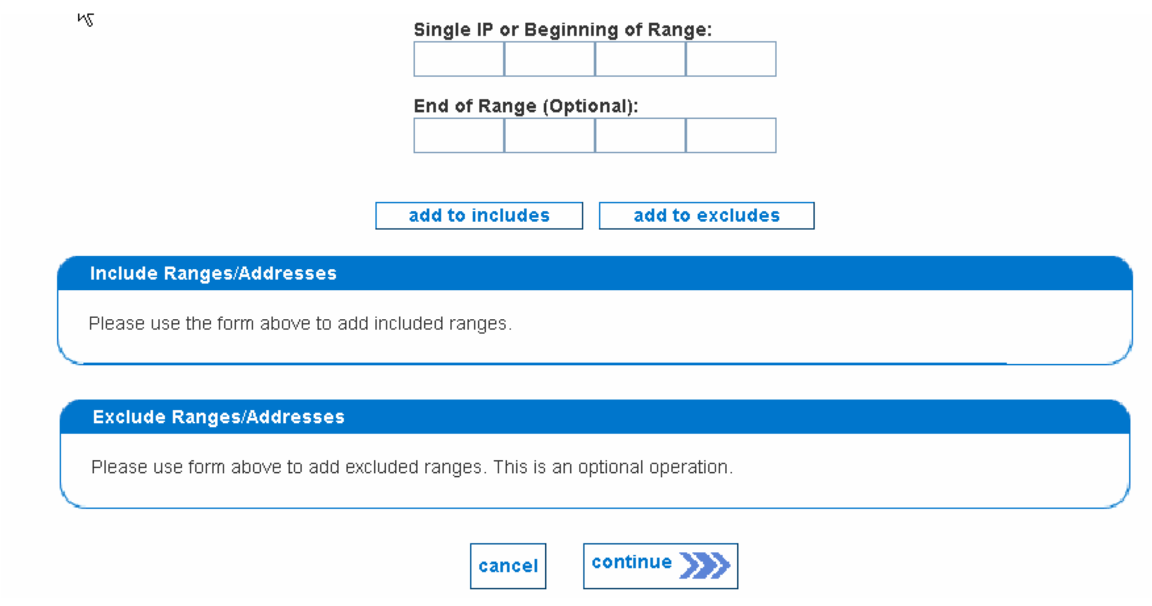
Specifying Windows Management Ranges

In this step, you will identify TCP/IP address ranges that can communicate with both the CC-NOC as well as the defined *proxy host*.

***Note:** If using the default internal proxy of a CC-NOC 2500M, click **edit** under **Default Proxy** to specify the address ranges.*

This range will be scanned for systems that can be managed using Microsoft's Windows Management Instrumentation (WMI). Once discovered, each system is categorized as either a Server, Infrastructure Device, or Workstation device and the appropriate license is assigned if available.

***Note:** It is recommended not to include DHCP devices in the discovery range. However, limited DHCP support is provided for managed devices, that is, those that are assigned as an Infrastructure Device or Server. For workstations, duplicates that result from DHCP address changes must be removed manually.*



Please use the form above to add included ranges.

Please use form above to add excluded ranges. This is an optional operation.

Figure 73 Specifying proxy host information

9. Type **IP addresses** or **ranges** and click either **add to includes** or **add to excludes** to add them to the list. You can only add one at a time. The TCP/IP address ranges and/or specific addresses you enter are the ones you would like to manage. You must specify at least one Include range or address to complete this part of the configuration. If there are any ranges or addresses you would like to exclude, for example, printers, you can also specify them. The Exclude panel keeps devices from being discovered, while the Includes panel identifies those addresses that should be discovered and managed. If you would like to later remove one from the list, click **remove** to the right of its listing.

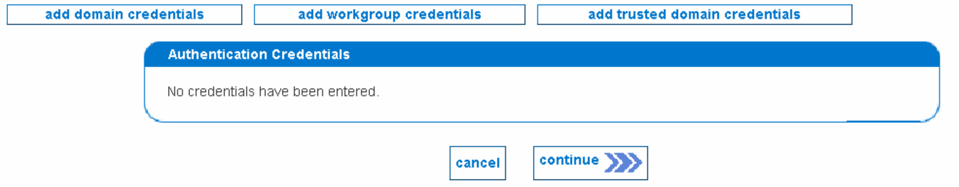
Note: *After windows discovery process is complete, you may notice an overlap in devices that were specified in the Discovery Range – please see* ***Edit Discovery Ranges*** *in* ***Chapter 2: General and Advanced Administration*** *for additional information. Therefore, it may be necessary to change the licenses of some devices, especially if you want to collect additional data. For example, you may want to change a workstation license to a server license if a license is available – please see* ***Manage, Unmanage, Rescan, or Delete Devices*** *in* ***Chapter 2: General and Advanced Administration*** *for additional information.*

Management naming resolution

The CC-NOC uses the TCP/IP ranges initially to find devices. However, to be able to gather WMI data from a target host, its WINDOWS NAME must be resolvable from the PROXY SYSTEM. Ensure that the system you choose as a Proxy has the ability to resolve Windows Names in the range you specify via either NetBIOS, or services like WINS or `lmhosts` file - see section **Configure WINS** for details. If the Proxy cannot resolve the Windows Name, even if it can ping the IP address, you will not be able to communicate with that host to gather WMI data.

Proxy Identification and Credentials

Once you have identified *proxies* and *ranges*, the CC-NOC will begin the discovery process in search of targets for management via WMI. Now you need to configure authentication information for your target servers and workstations, for example, desktops, laptops, etc.


add domain credentials
add workgroup credentials
add trusted domain credentials
Authentication Credentials

No credentials have been entered.

Figure 74 Specifying proxy authentication credentials

For every domain, workgroup, or trusted domain that is associated with hosts you wish to manage, you will need to provide authentication information, for example, username and password, which will be used to log into the systems and pull performance, event log, and/or system inventory information. If you wish, you may provide this information on the device-level once the device has been discovered. Note that this is arguably more secure, but considerably more administration intensive.

The CC-NOC supports authentication via any of these three common mechanisms for authentication:

- Domain-based authentication
- Workgroup-based authentication
- Trusted Domain-based authentication

Domain-based authentication is the most commonly used form of authentication in Windows environments. For every domain that is associated with hosts you wish to manage, you will need to provide authentication information, for example, username and password, which will be used to log into the systems and pull performance, event log, and/or system inventory information. The Username and Password will be passed to a server within the domain for authentication. The target machine must be a member of this domain and the Username must be configured as a user within that domain.

Workgroup-based authentication means that the machine has been identified as part of a Workgroup and that the Username is an existing local user on that particular end system. If you wish to use local authentication to your target servers/workstations and those machines are not part of a common workgroup, you will be allowed to enter those local credentials on a subsequent page. As a part of its systems discovery, the CC-NOC identifies target machines as members of a Workgroup, if applicable. For those machines, you may specify a local user on those machines to use for authentication purposes.

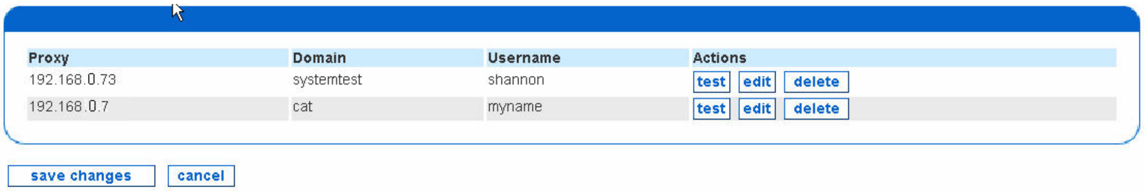
***Note:** Any local user defined must be a member of the Local Administrators group to authenticate and allow data collection to occur.*

Trusted Domain-based authentication is used when the target machines are part of a domain other than the domain to be used for authentication, yet there exists a trust relationship between the two domains. This feature can be difficult to troubleshoot and should be used only by advanced Windows administrators.

10. Select one of the credentials to add authentication. Supply the following information for each type:

Domain-Based	Workgroup-Based	Trusted Domain-Based
unique **domain** name	**workgroup** name	unique **domain** name of which the target system is a member
a **username** that must be a member of the Local Administrators group on the target systems. In most cases the Domain administrator will be a member of this group.	a **username** that must be a member of the Local Administrators group on the target systems	a unique **trusted domain** name is the domain which will be used for authentication
a **password**	a **password**	A username that must be a member of the Local Administrators group on the target systems. In most cases the Domain administrator will be a member of this group.
confirm password	confirm password	a **password**
		confirm password

11. After entering the information, click **add credential**.
12. To complete the wizard**,** click **continue**.



Proxy	Domain	Username	Actions
192.168.0.73	systemtest	shannon	test edit delete
192.168.0.7	cat	myname	test edit delete

Figure 75 List of Windows Management Proxies

13. If you are satisfied with the list of proxies, click **save changes**.

***Note:** You need administrative privileges to add credentials for all three types of authentication.*

Configuring a WINS Server or LMHOSTS File

If you need to collect WMI data from Windows servers that exist in another network and you need to resolve Windows NetBIOS names to IP addresses, on the external proxy you can either:

- Configure the WINS server.
- Edit the `lmhosts` file.

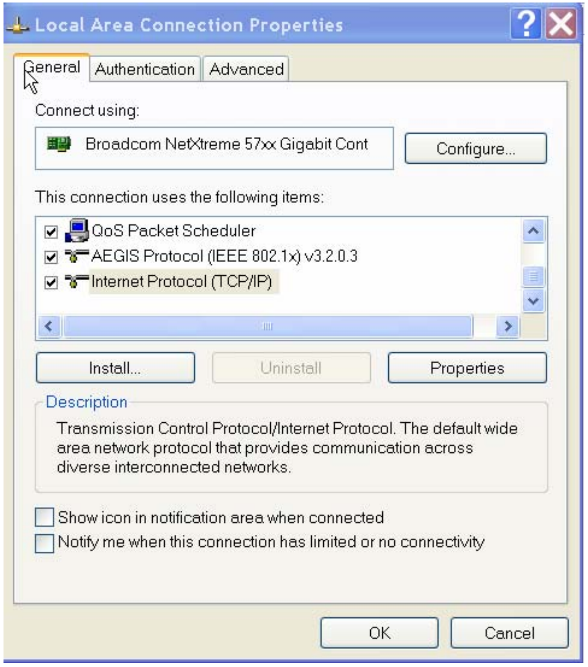
Configure a WINS Server on External Proxy

Since NetBIOS names are not routed between networks, you can configure the external proxy to use a WINS server so NetBIOS names are resolved to IP addresses. If using the internal proxy of a CC-NOC 2500M, you can configure it as explained in section **Configure WINS** later in this chapter.

To ensure successful name resolution, a route for the remote network must exist on the default router and an entry is needed in the WINS server. The WINS server entry can be configured from the **Properties** dialog box or from typing the **netsh** command on the command line interface.

Properties Dialog Box

1. On the network interface used by the proxy, select **Control Panel**.
2. Click **Network Connections**.
3. Click on the network interface that is connected to the external proxy, for example, Local Area Connection.
4. Click the **Properties** button.
5. Scroll down and select **Internet Protocol (TCP/IP)**.



Connect using:

Broadcom NetXtreme 57xx Gigabit Cont

This connection uses the following items:

☑ QoS Packet Scheduler
☑ AEGIS Protocol (IEEE 802.1x) v3.2.0.3
☑ Internet Protocol (TCP/IP)

Description

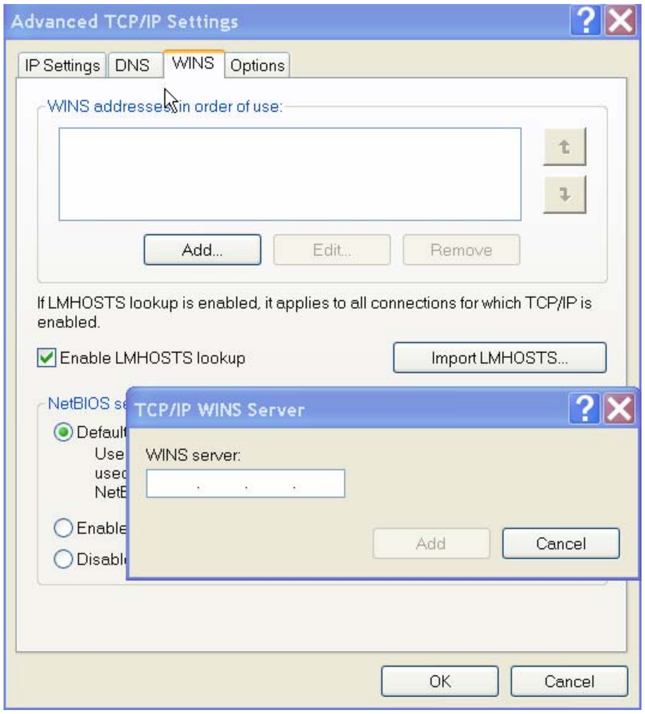
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected
□ Notify me when this connection has limited or no connectivity

Figure 76Selecting Internet Protocol (TCP/IP) for WINS Settings

6. Click the **Properties** button.
7. Click the **Advanced** button.

8. Click on the **WINS** tab.



If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

Figure 77Selecting WINS Tab

9. Click the **Add…** button and specify the address of the WINS server for the remote appliance to use for Windows computer name resolution and click **add**.

Command Line Interface

Alternatively, you can issue this command on the command line interface:

```
netsh interface ip set WINS <nic name> static <wins server IP address>
```

Where:

<*nic name*> is the interface that is connected to the external proxy

<*wins server IP address*> is the IP address of the WINS server.

Edit LMHOSTS File on External Proxy

If a WINS server is not available but you need to resolve NetBIOS names to IP addresses for Windows servers that exist in another network, you can also edit the `lmhosts` file on the external proxy.

1. On the external proxy, start a text editor like **Notepad**.
2. Locate the `lmhosts` file in this path:

   <*Windows home drive*>\<*windows home directory*>\system32\drivers\etc

   For example, `C:\WINDOWS\system32\drivers\etc`
3. Add an entry to the `lmhosts` file in the following format:

   ```
   <IP Address> <ComputerName (NetBIOS Name)>
   ```

   Where:

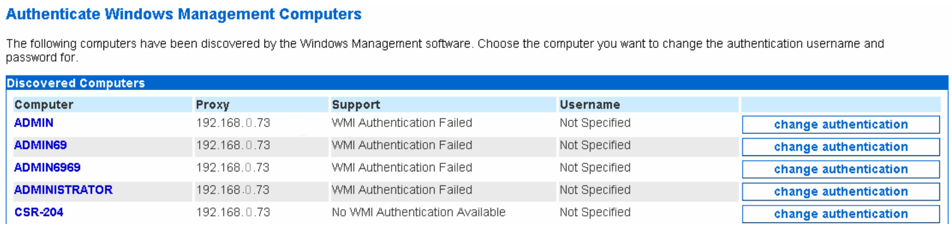
   <*IP Address*> is the IP address of each remote Windows server from which you wish to collect WMI data.

   <*ComputerName (NetBIOS Name)*> is the NetBIOS name you wish to resolve.
4. Save the file.

Authenticate Windows Computers

This option allows you to change the authentication usernames and passwords for discovered servers and workstations.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Windows Management Configuration**.
3. Click **Authenticate Windows Computers**.



Authenticate Windows Management Computers

The following computers have been discovered by the Windows Management software. Choose the computer you want to change the authentication username and password for.

Discovered Computers

Computer	Proxy	Support	Username	
ADMIN	192.168.0.73	WMI Authentication Failed	Not Specified	change authentication
ADMIN69	192.168.0.73	WMI Authentication Failed	Not Specified	change authentication
ADMIN6969	192.168.0.73	WMI Authentication Failed	Not Specified	change authentication
ADMINISTRATOR	192.168.0.73	WMI Authentication Failed	Not Specified	change authentication
CSR-204	192.168.0.73	No WMI Authentication Available	Not Specified	change authentication

Figure 78 Change Authentication Usernames and Passwords for Discovered Targets

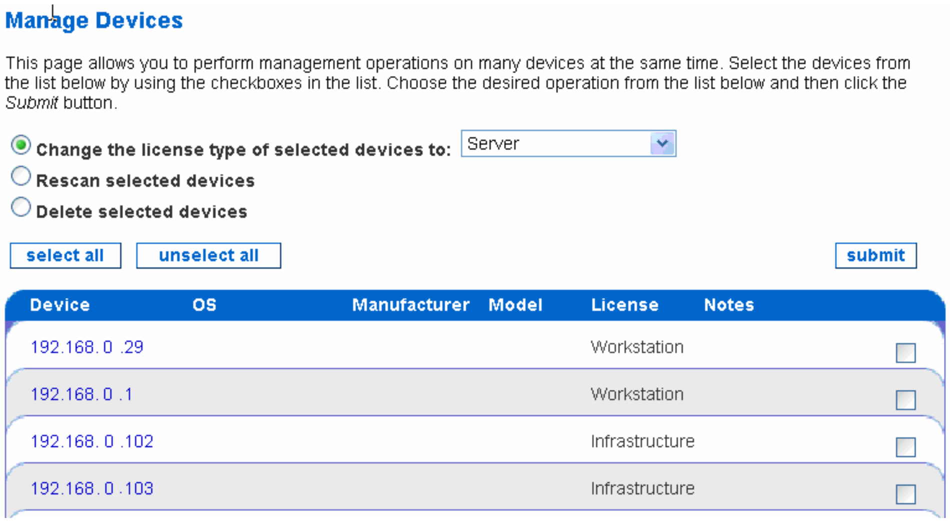
4. Click **change authentication** next to the managed device for which to want to change the usernames or password.
5. Type a username, password, confirm the password, and click **authenticate**. The first login that is successful will be used to gather WMI data. If all login attempts are unsuccessful, then it is not possible to collect WMI data from the computer with the given username and password and it will be displayed with status "**Auth Failed**" in the device list. Click **cancel** to end the authentication test and return to the list of discovered computers.

Manage, Unmanage, or Rescan Devices

This option allows you to directly choose which devices that you want managed as either Servers, Infrastructure, or Workstations. If licenses are available, you can "promote" a workstation or assign it a server license so performance and service metrics are also collected.

You can choose to manage or unmanage several devices at once. You can also perform rescans of several devices at the same time.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Windows Management Configuration**.
3. Click **Manage, Unmanage, or Rescan Devices**.



Manage Devices

This page allows you to perform management operations on many devices at the same time. Select the devices from the list below by using the checkboxes in the list. Choose the desired operation from the list below and then click the *Submit* button.

● **Change the license type of selected devices to:** Server

○ **Rescan selected devices**

○ **Delete selected devices**

Device	OS	Manufacturer	Model	License	Notes	
192.168. 0 .29				Workstation		□
192.168. 0 .1				Workstation		□
192.168. 0 .102				Infrastructure		□
192.168. 0 .103				Infrastructure		□

Figure 79 Manage Devices

4. Using the check boxes, select the devices in the list that you want to perform management operations on.

5. Choose the desired operation, for example, change license type to **Promoted Workstation**.
6. Click **submit**.

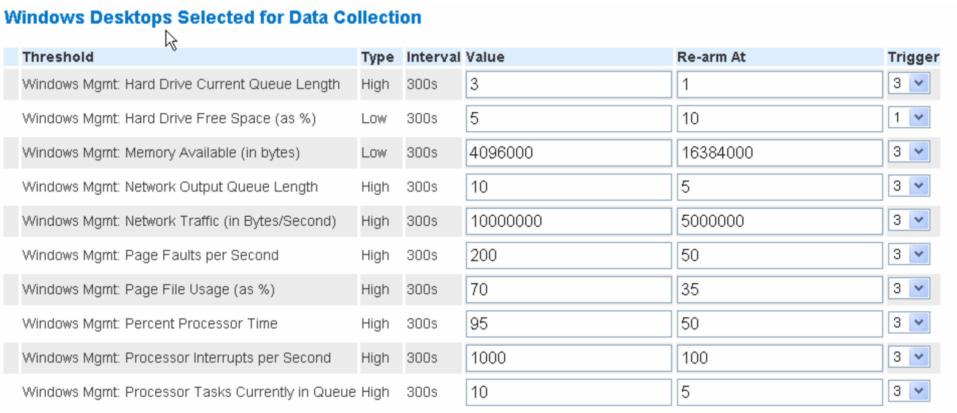
To generate an inventory report of the current list of devices, select an output format, for example, HTML or XML, and click **generate report**. XML can be used in Crystal Reports.

Note: *If an Infrastructure device, for example, Cisco router, is listed as Unknown, it means that the default sysName value of "Unknown" has not been changed to something more meaningful. This can be corrected by either clicking the 'Change Device Label' link on the device page or the administrator of the "Unknown" device can assign a meaningful name to the sysName value.*

Configure Windows Performance Thresholds

This option allows you to configure the performance thresholds associated with Windows performance metrics for workstations and servers. All currently thresholded metrics are reflected and values, re-arm values, and triggers are exposed for customization in your environment.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Windows Management Configuration**.
3. Click **Configure Windows Performance Thresholds**.



Windows Desktops Selected for Data Collection

Threshold	Type	Interval	Value	Re-arm At	Trigger
Windows Mgmt: Hard Drive Current Queue Length	High	300s	3	1	3
Windows Mgmt: Hard Drive Free Space (as %)	Low	300s	5	10	1
Windows Mgmt: Memory Available (in bytes)	Low	300s	4096000	16384000	3
Windows Mgmt: Network Output Queue Length	High	300s	10	5	3
Windows Mgmt: Network Traffic (in Bytes/Second)	High	300s	10000000	5000000	3
Windows Mgmt: Page Faults per Second	High	300s	200	50	3
Windows Mgmt: Page File Usage (as %)	High	300s	70	35	3
Windows Mgmt: Percent Processor Time	High	300s	95	50	3
Windows Mgmt: Processor Interrupts per Second	High	300s	1000	100	3
Windows Mgmt: Processor Tasks Currently in Queue	High	300s	10	5	3

Figure 80 Configuring Windows Performance Thresholds

Listed above are the current values at which Windows performance metrics are considered problematic which generates events. You have complete control over these thresholds, including their value, their re-arm values, and the number of consecutive data samples, for example, "triggers", which must be exceeded before an event is generated.

If the threshold is of type **High**, the Value must be greater than or equal to the Re-arm. If the threshold is of type **Low**, the Value must be less than or equal to the Re-arm.

Click **save thresholds** at the bottom of the page when you are finished editing the thresholds. Changing any of the thresholds will require a restart of the CC-NOC. Clicking **reset** will set the thresholds back to their values since the last edit.

Configure WINS Server or LMHOSTS File on 2500M

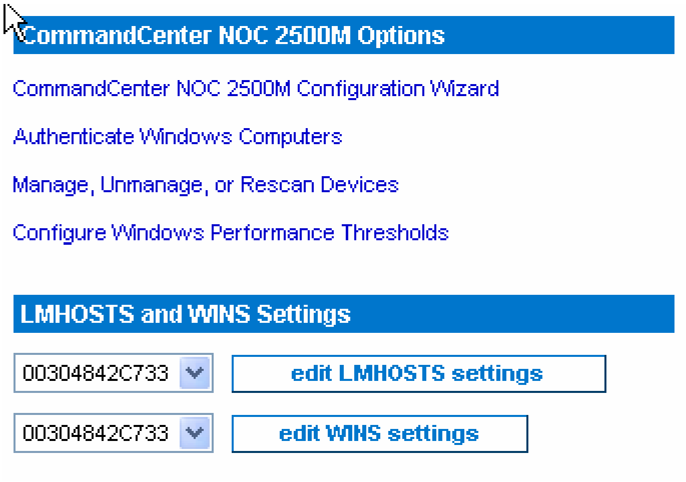
In a distributed environment, you can edit the `lmhosts` file or WINS settings for the CC-NOC 2500M appliance.

Edit WINS Settings

You can also specify a WINS server for the selected appliance if you are using the internal proxy on the CC-NOC 2500M appliance and you need to collect WMI data off a few Windows servers that exist in another network. A WINS server is used to resolve Windows NetBIOS names to IP address.

To edit WINS settings:

1. Click on the **Admin** tab in the top navigation bar.
2. Click **CommandCenter NOC 2500M Configuration**.

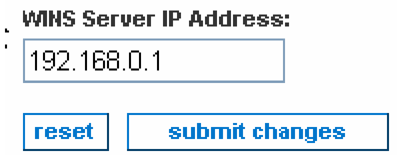

CommandCenter NOC 2500M Options
CommandCenter NOC 2500M Configuration Wizard
Authenticate Windows Computers
Manage, Unmanage, or Rescan Devices
Configure Windows Performance Thresholds
LMHOSTS and WINS Settings
edit LMHOSTS settings
edit WINS settings

00304842C733

00304842C733

Figure 81 Edit WINS Settings

3. Select the CC-NOC 2500M appliance from the pull-down menu next to **edit WINS settings**.
4. Click **edit WINS settings**.



WINS Server IP Address:

192.168.0.1

Figure 82 WINS Server IP Address

5. Specify a WINS server for the remote appliance to use for Windows computer name resolution and click **submit changes**. If you do not wish to specify a WINS server, then leave the WINS server field blank and click s**ubmit changes**.

Edit LMHOSTS File

To resolve Windows NetBIOS names to IP addresses, you can edit the `lmhosts` file if you are using the internal proxy on the CC-NOC 2500M appliance and a WINS server is not available.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **CommandCenter NOC 2500M Configuration**.

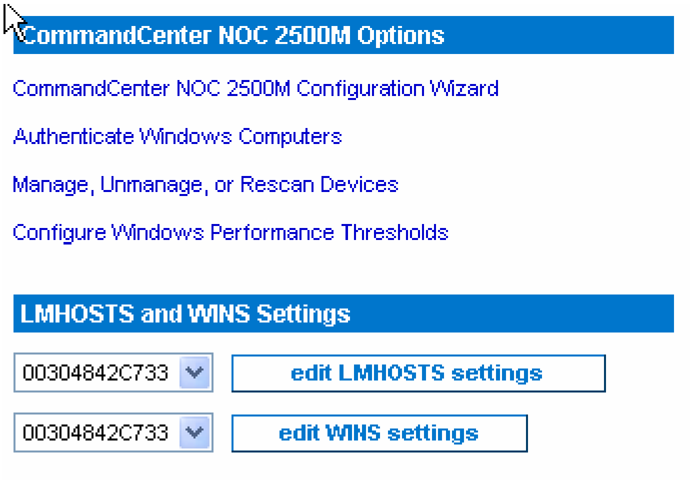
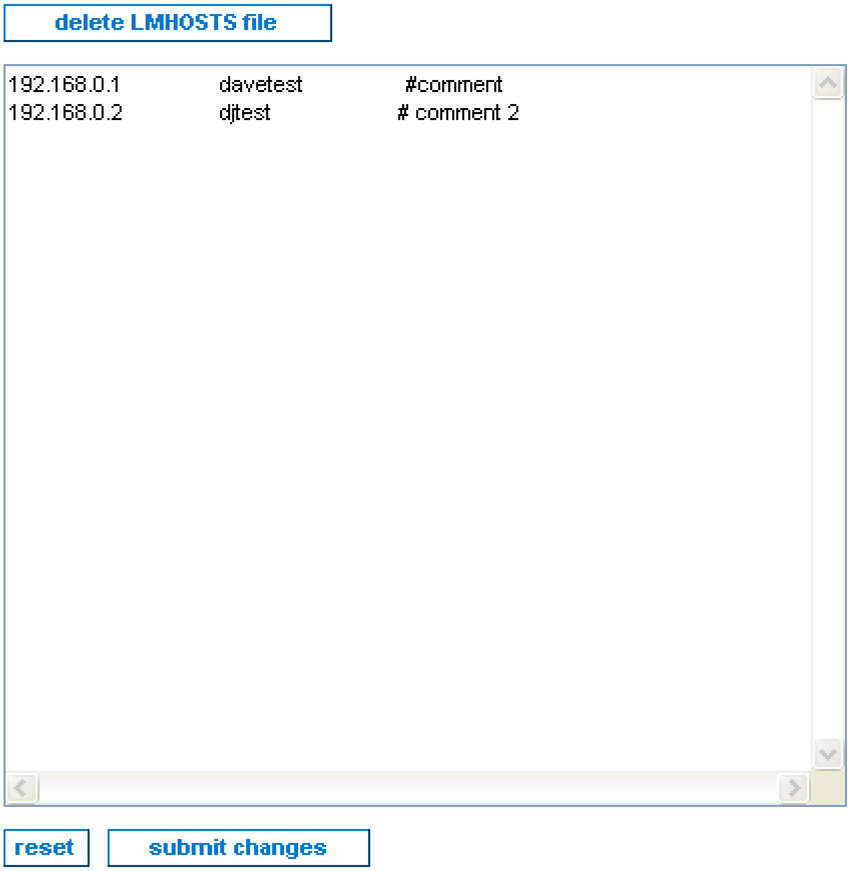

CommandCenter NOC 2500M Options
CommandCenter NOC 2500M Configuration Wizard
Authenticate Windows Computers
Manage, Unmanage, or Rescan Devices
Configure Windows Performance Thresholds
LMHOSTS and WINS Settings
00304842C733
edit LMHOSTS settings
00304842C733
edit WINS settings

Figure 83 CommandCenter NOC 2500M Options

3. Select the CC-NOC 2500M appliance from the pull-down menu next to **edit LMHOSTS settings**.
4. Click **edit LMHOSTS settings**.



```
192.168.0.1          davetest          #comment
192.168.0.2          djtest           # comment 2
```

Figure 84 Edit LMHOSTS File

5. Specify the IP address of each remote Windows server from which you wish to collect WMI data.
6. You can also delete all of the `lmhosts` settings for the appliance by clicking **delete LMHOSTS file**.
7. Click **submit changes**.

Chapter 5: Configuring Vulnerability Scanning

This chapter describes procedures to configure a CC-NOC so it can scan for vulnerabilities, for example, exploits and thresholds against devices within your network. Scanning for vulnerabilities assists administrators in resolving security concerns.

Vulnerability scanning finds *system vulnerabilities,* for example, unpatched systems, older known vulnerable server daemons, etc., that can be exploited by harmful network traffic. This harmful traffic can be generated by intruders to gain access to restricted information, alter the flow of data through your network, or even disable important services on your network.

Vulnerability scanning provides the following information about your network devices:

- Detection and diagnosis of vulnerabilities
- Deep detection of all open ports and services
- Logging of all available information that may benefit intruders
- Detection of passwords that are set to default or easy-to-guess values

With this information, you can take steps to make your network more secure from network-based intrusion such as:

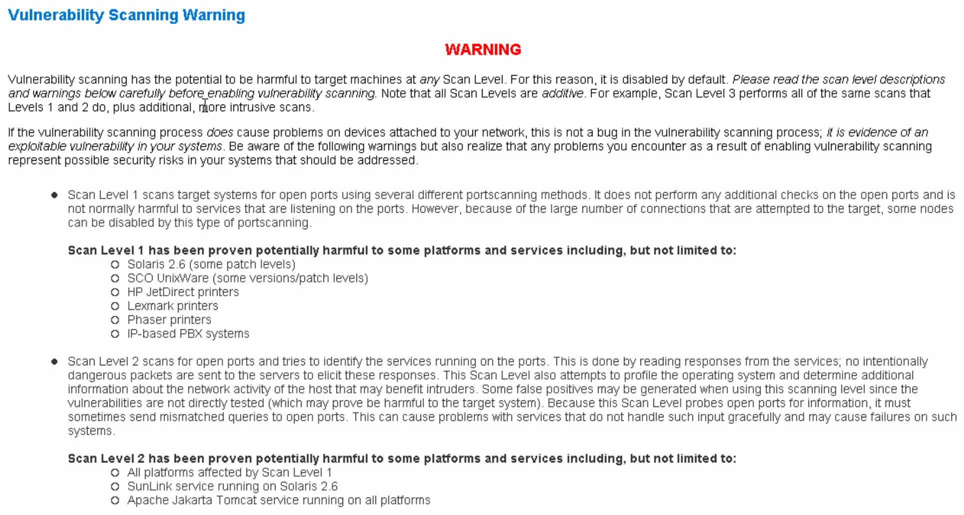
- Apply patches and software updates to fix known security holes
- Shut down unwanted or unnecessary services
- Remove access to sensitive information on your network
- Change security settings and passwords to make them more difficult to crack

The vulnerability scanning process can be performed at Scan Levels 1 through 4. The higher the scan level, the more invasive the scan will be to the target IP address. Use caution when performing scans with Scan Level 3 and 4; although the information they provide may be more accurate and comprehensive, they can also expose the target machines to dangerous exploits that may cause data loss or denial of services. Scan levels can only be assigned by an administrator.

Accessing Vulnerability Scanning

Vulnerability scanning is a feature that lets you determine whether or not the systems that you are managing are vulnerable to different types of known intrusions. When vulnerabilities are detected on your systems, you will be provided a list of the vulnerabilities for the interface and, if available, possible solutions or links to more information about the vulnerabilities, including **Common Vulnerabilities and Exposures (CVE)** entries. For more information, go to http://www.cve.mitre.org/.

1. Click on the **Vulnerabilities** tab in the top navigation bar.
2. Click **Configure Vulnerability Scanning**.



Vulnerability Scanning Warning

WARNING

Vulnerability scanning has the potential to be harmful to target machines at *any* Scan Level. For this reason, it is disabled by default. *Please read the scan level descriptions and warnings below carefully before enabling vulnerability scanning.* Note that all Scan Levels are *additive*. For example, Scan Level 3 performs all of the same scans that Levels 1 and 2 do, plus additional, more intrusive scans.

If the vulnerability scanning process *does* cause problems on devices attached to your network, this is not a bug in the vulnerability scanning process; *it is evidence of an exploitable vulnerability in your systems*. Be aware of the following warnings but also realize that any problems you encounter as a result of enabling vulnerability scanning represent possible security risks in your systems that should be addressed.

- Scan Level 1 scans target systems for open ports using several different portscanning methods. It does not perform any additional checks on the open ports and is not normally harmful to services that are listening on the ports. However, because of the large number of connections that are attempted to the target, some nodes can be disabled by this type of portscanning.

  Scan Level 1 has been proven potentially harmful to some platforms and services including, but not limited to:
  - Solaris 2.6 (some patch levels)
  - SCO UnixWare (some versions/patch levels)
  - HP JetDirect printers
  - Lexmark printers
  - Phaser printers
  - IP-based PBX systems

- Scan Level 2 scans for open ports and tries to identify the services running on the ports. This is done by reading responses from the services; no intentionally dangerous packets are sent to the servers to elicit these responses. This Scan Level also attempts to profile the operating system and determine additional information about the network activity of the host that may benefit intruders. Some false positives may be generated when using this scanning level since the vulnerabilities are not directly tested (which may prove be harmful to the target system). Because this Scan Level probes open ports for information, it must sometimes send mismatched queries to open ports. This can cause problems with services that do not handle such input gracefully and may cause failures on such systems.

  Scan Level 2 has been proven potentially harmful to some platforms and services including, but not limited to:
  - All platforms affected by Scan Level 1
  - SunLink service running on Solaris 2.6
  - Apache Jakarta Tomcat service running on all platforms

Figure 85 Vulnerability Scanning Warning

3. Read the warning and at the bottom of the page, click **I Agree.**

By clicking on **I Agree** and proceeding to the configuration page, you acknowledge these risks and take responsibility for all potential damages and outages. Otherwise, click **I Do Not Agree** and you will be returned to the **Admin** page. Contact your reseller or product support for more information about the benefits and risks involved in vulnerability scanning.

Vulnerability Scan Levels

Vulnerability scanning has the potential to be harmful to target machines at *any* Scan Level. For this reason, it is disabled by default. Read the scan level descriptions and warnings below carefully before enabling vulnerability scanning.

Note: *All Scan Levels are additive. For example, Scan Level 3 performs all of the same scans that Levels 1 and 2 do, plus additional, more intrusive scans.*

If the vulnerability scanning process *does* cause problems on devices attached to your network, this is not a bug in the vulnerability scanning process; *it is evidence of an exploitable vulnerability in your systems*. Be aware of the following warnings but also realize that any problems you encounter as a result of enabling vulnerability scanning represent possible security risks in your systems that should be addressed.

Scan Level 1

Scan Level 1 scans target systems for open ports using several different port scanning methods. It does not perform any additional checks on the open ports and is not normally harmful to services that are listening on the ports. However, because of the large number of connections that are attempted to the target, some nodes can be disabled by this type of port scanning.

Scan Level 1 has been proven potentially harmful to some platforms and services including, but not limited to:

- Solaris 2.6 (some patch levels)
- SCO UnixWare (some versions/patch levels)
- HP JetDirect printers
- Lexmark printers
- Phaser printers
- IP-based PBX systems

Scan Level 2

Scan Level 2 scans for open ports and tries to identify the services running on the ports. This is done by reading responses from the services; no intentionally dangerous packets are sent to the servers to elicit these responses. This Scan Level also attempts to profile the operating system and determine additional information about the network activity of the host that may benefit intruders. Some false positives may be generated when using this scanning level since the vulnerabilities are not directly tested, which may prove be harmful to the target system. Because this Scan Level probes open ports for information, it must sometimes send mismatched queries to open ports. This can cause problems with services that do not handle such input gracefully and may cause failures on such systems.

Scan Level 2 has been proven potentially harmful to some platforms and services including, but not limited to:

- All platforms affected by Scan Level 1
- SunLink service running on Solaris 2.6
- Apache Jakarta Tomcat service running on all platforms

Scan Level 3

Scan Level 3 performs all of the checks of Levels 1 and 2. Additionally, it will craft packets and attempt minor intrusions against the target interface to directly test for vulnerabilities. This process can harm the target machine if the vulnerabilities are successfully exploited by the scanning process. It is not advisable to use this scan against mission-critical targets, regardless of OS or services that are running.

Scan Level 4

Scan Level 4 performs all checks of previous levels and also attempts exploits that are known to be directly harmful to target systems. These include vulnerabilities that can alter data on the target or bring down services or the operating system by using denial-of-service techniques. It is absolutely not advisable to use this scan against mission-critical targets, regardless of OS or services that are running.

At each Scan Level, there is the potential for damage including data loss, network communication loss, hardware damage, loss of network integrity, or exposure of information to unauthorized parties.

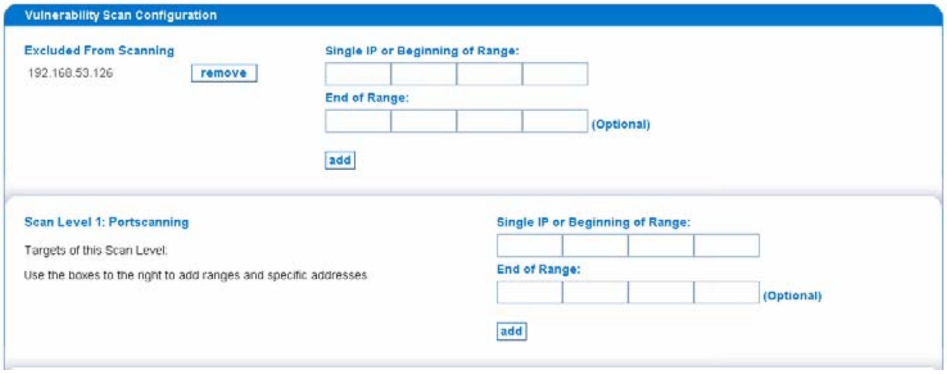
Warning: *Vulnerability scanning at any level has the potential to be harmful to target machines. Scan Levels 3 and 4 carry out real intrusion attempts against targets and can have negative effects on the target machines to the point of data loss and denial of services. Use these scan levels with extreme caution. You may want to schedule these scans to run off-hours.*

Specify IP Addresses and Schedule the Scan

After agreeing to the Warning, you now need to identify the targets of the scan. Only the admin user can configure vulnerability scanning.

To build a scan:

1. After clicking **I Agree** to the warning, click **edit settings** at the bottom of the page.


Vulnerability Scan Configuration
Excluded From Scanning
remove
Single IP or Beginning of Range:
End of Range:
(Optional)
add
Scan Level 1: Portscanning
Single IP or Beginning of Range:
End of Range:
(Optional)
add

192.168.53.126

Targets of this Scan Level:

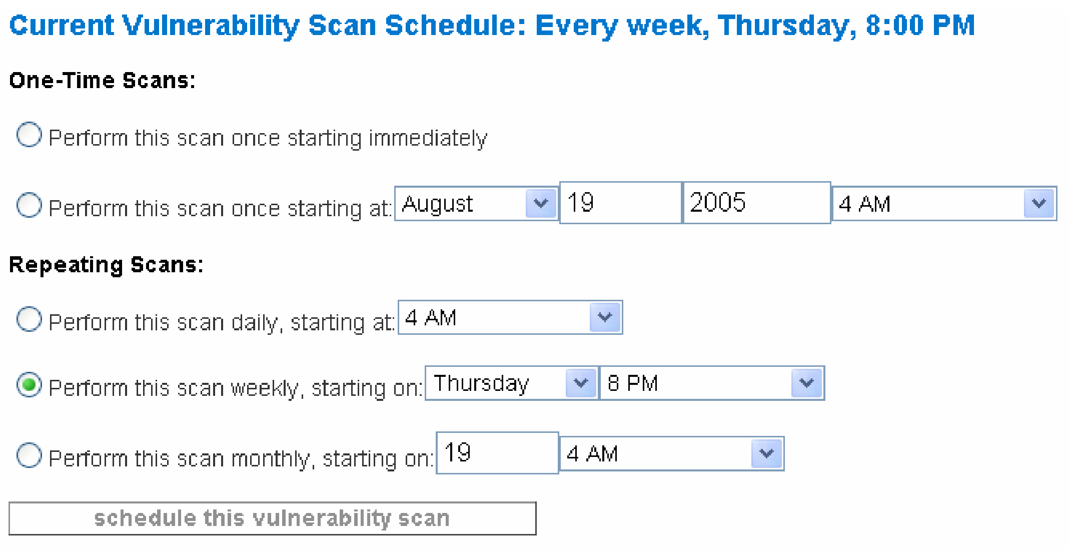
Use the boxes to the right to add ranges and specific addresses

Figure 86 Type IP Addresses for Vulnerability Scanning

2. Add the appropriate IP addresses to the levels you want to scan. You can add either specific IP addresses, by filling in the **Single IP or Beginning of Range** field, or a range of IP addresses, by filling in the **End of Range** field.

Note: *The Excluded from Scanning box lets you exclude IP addresses from any type of scanning. The IP ranges specified in this box override all other scanning settings.*

3. Click **add** to have the targets added, or excluded, from the scan.
4. Click **save settings** to save all addresses entered and return to the previous page.
5. Scroll to the bottom of the page and create a scanning schedule. Vulnerability scanning can be scheduled to occur when it won't adversely impact your network. This will allow you to perform the more intensive vulnerability scanning without impacting your network availability. Recurring scans can also be configured, allowing you to maintain your network security.



Current Vulnerability Scan Schedule: Every week, Thursday, 8:00 PM

One-Time Scans:

○ Perform this scan once starting immediately

○ Perform this scan once starting at: August 19 2005 4 AM

Repeating Scans:

○ Perform this scan daily, starting at: 4 AM

● Perform this scan weekly, starting on: Thursday 8 PM

○ Perform this scan monthly, starting on: 19 4 AM

Figure 87 Create a Vulnerability Scanning Schedule

6. Select one of the options to perform a one-time scan of the devices that were specified or set up a scan that repeats according to the frequency you specify.
7. Click **schedule this vulnerability scan**.

Chapter 6: Configuring Notifications

This chapter describes procedures to configure a CC-NOC so it can send and escalate notices through email, pagers, etc. if and when specific CC-NOC events occur.

When important events are detected, users may receive a notice that is a descriptive message sent automatically to a pager, an email address, or both. To receive notices, a user must have their notification information configured in their user profile, notices must be turned **on**, and an important event must be received. Only users with administrative privileges can change user profiles and turn notices on or off.

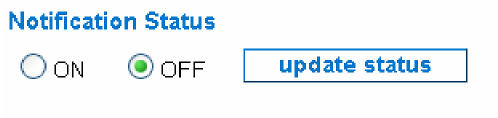
How to create new notification escalation plans, called *notification paths,* and then associate a notification path with a CC-NOC event is also covered in this chapter. Each path can have any arbitrary number of escalations or targets, that is, users or groups, and can send notices through email, pagers, etc. Each notification path can be triggered by any number of CC-NOC events and can further be associated with specific interfaces or services.

Enable/Disable Notifications

The **Notification Configuration** page provides both a visual reminder as to whether your users are being paged/emailed when important network events are received, as well as providing a way to turn the notification system on or off. This is a system-wide setting affecting all notifications and all users.

Note: *Notifications are disabled by default. You should enable Notifications after the initial discovery process has completed.*

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Notification Configuration**.



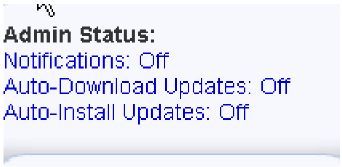
Notification Status

○ ON ● OFF

Figure 88 Notification Status

3. To change the status, click either **ON** or **OFF** and click **update status**.

The **Admin Status:** in the left-side of the page will change to reflect the new status.



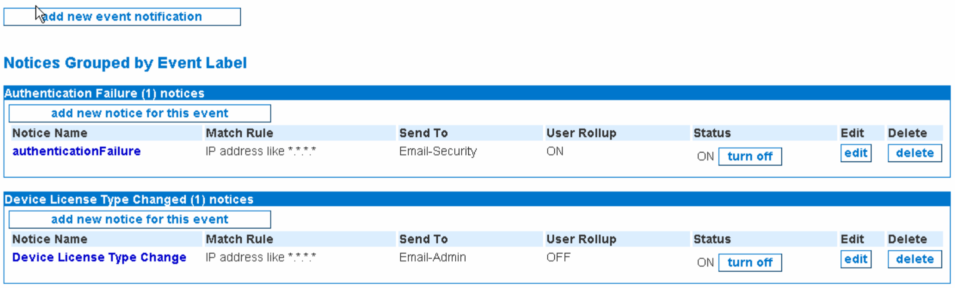
Admin Status:
Notifications: Off
Auto-Download Updates: Off
Auto-Install Updates: Off

Figure 89 Admin Status

Configure Event Notifications

By configuring event notifications, each system event can be configured to send a notification whenever that event is triggered.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Notification Configuration**.
3. Click **Configure Event Notifications**.



add new event notification

Notices Grouped by Event Label

Authentication Failure (1) notices

add new notice for this event

Notice Name	Match Rule	Send To	User Rollup	Status	Edit	Delete
authenticationFailure	IP address like *.*.*.*	Email-Security	ON	ON turn off	edit	delete

Device License Type Changed (1) notices

add new notice for this event

Notice Name	Match Rule	Send To	User Rollup	Status	Edit	Delete
Device License Type Change	IP address like *.*.*.*	Email-Admin	OFF	ON turn off	edit	delete

Figure 90 A Configuring Event Notifications

This page lists the default event notifications, grouped by Event Label. Each event is listed in its own panel, and you may turn these on/off, based upon your environment needs. The columns are as follows:

- The **Notice Name** column identifies the unique name of the notice. It reflects the event that will trigger the notification of the notice. Click the name to obtain details of the notice.
- The **Match rule** column shows which IP addresses and/or services are associated with this notification. It is an interface/service rule that will be matched against data to validate if this notification should be sent for the event. Please note that the ordering of the notices with the same Event Label is important. Notices with more specific rules should be placed before those that are more general to ensure that the correct notice is chosen. To change the ordering of the notices with the same event click **arrange these notices** for the particular list you want to order as shown below – see section **Arrange Notice Hierarchy** for additional information.
- The **Send To** column shows the *notification path* that the notice will be sent according to. Notification paths determine who the notice gets sent to and how to send the notice.
- The **User Rollup** column shows if this feature is ON or OFF. Use rollup is a feature that prevents a user's email or pager from being overloaded by simultaneous notifications by collecting notifications that occur over a short time period. The feature will then "roll up" the notifications into a single email or pager message with summary information about each individual notification.
- The **Status** column shows whether or not that particular event notification is currently being sent, provided notifications are turned on for the whole system. If you want to control the notifications sent out for a particular event, use its **turn on/off** toggle button. The text on the button will show the action that will be taken when pressed.

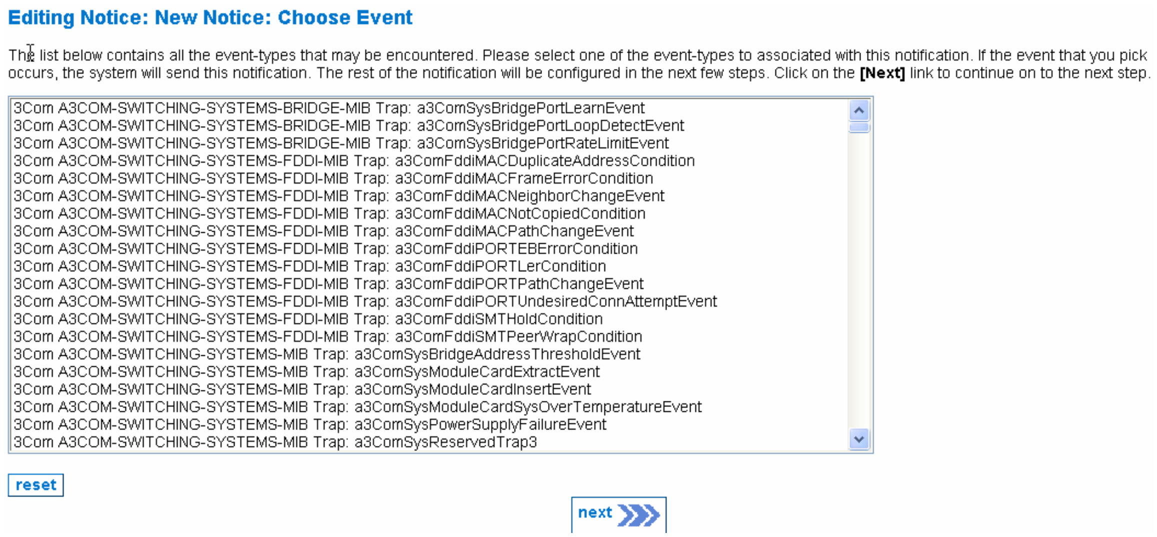
Add/Edit a Notification

To add a new notification, click **add new event notification** and you will be walked through the configuration of the new notification as described in the next few steps.

Clicking **edit** next to a notice follows the same steps, allowing you to edit information already defined for the notice. Clicking **add new notice for this event** also follows the same steps, but bypasses selecting an event type.

Select Event Type

The first step when adding or editing a notification is to select one event type to associate with the notification. Notice that if you are adding a new notice for an existing event, you will bypass this step.



Editing Notice: New Notice: Choose Event

The list below contains all the event-types that may be encountered. Please select one of the event-types to associated with this notification. If the event that you pick occurs, the system will send this notification. The rest of the notification will be configured in the next few steps. Click on the **[Next]** link to continue on to the next step.

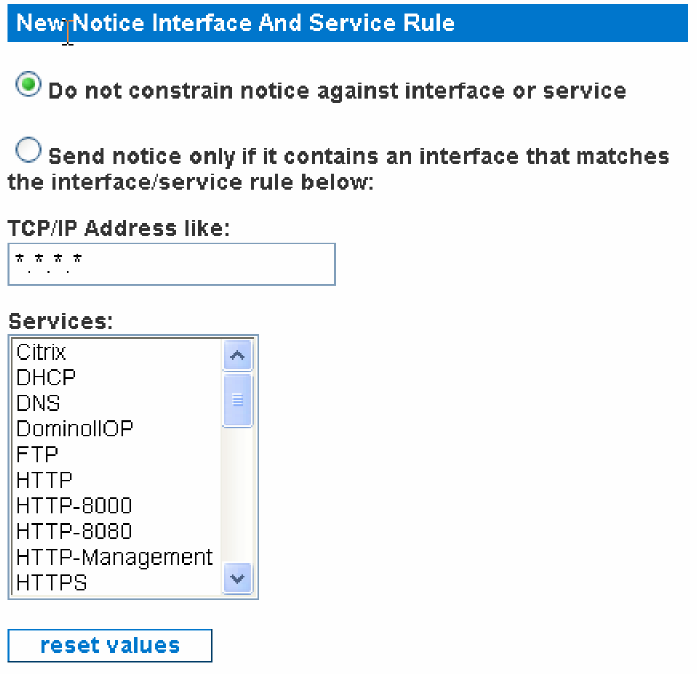
3Com A3COM-SWITCHING-SYSTEMS-BRIDGE-MIB Trap: a3ComSysBridgePortLearnEvent
3Com A3COM-SWITCHING-SYSTEMS-BRIDGE-MIB Trap: a3ComSysBridgePortLoopDetectEvent
3Com A3COM-SWITCHING-SYSTEMS-BRIDGE-MIB Trap: a3ComSysBridgePortRateLimitEvent
3Com A3COM-SWITCHING-SYSTEMS-FDDI-MIB Trap: a3ComFddiMACDuplicateAddressCondition
3Com A3COM-SWITCHING-SYSTEMS-FDDI-MIB Trap: a3ComFddiMACFrameErrorCondition
3Com A3COM-SWITCHING-SYSTEMS-FDDI-MIB Trap: a3ComFddiMACNeighborChangeEvent
3Com A3COM-SWITCHING-SYSTEMS-FDDI-MIB Trap: a3ComFddiMACNotCopiedCondition
3Com A3COM-SWITCHING-SYSTEMS-FDDI-MIB Trap: a3ComFddiMACPathChangeEvent
3Com A3COM-SWITCHING-SYSTEMS-FDDI-MIB Trap: a3ComFddiPORTEBErrorCondition
3Com A3COM-SWITCHING-SYSTEMS-FDDI-MIB Trap: a3ComFddiPORTLerCondition
3Com A3COM-SWITCHING-SYSTEMS-FDDI-MIB Trap: a3ComFddiPORTPathChangeEvent
3Com A3COM-SWITCHING-SYSTEMS-FDDI-MIB Trap: a3ComFddiPORTUndesiredConnAttemptEvent
3Com A3COM-SWITCHING-SYSTEMS-FDDI-MIB Trap: a3ComFddiSMTHoldCondition
3Com A3COM-SWITCHING-SYSTEMS-FDDI-MIB Trap: a3ComFddiSMTPeerWrapCondition
3Com A3COM-SWITCHING-SYSTEMS-MIB Trap: a3ComSysBridgeAddressThresholdEvent
3Com A3COM-SWITCHING-SYSTEMS-MIB Trap: a3ComSysModuleCardExtractEvent
3Com A3COM-SWITCHING-SYSTEMS-MIB Trap: a3ComSysModuleCardInsertEvent
3Com A3COM-SWITCHING-SYSTEMS-MIB Trap: a3ComSysModuleCardSysOverTemperatureEvent
3Com A3COM-SWITCHING-SYSTEMS-MIB Trap: a3ComSysPowerSupplyFailureEvent
3Com A3COM-SWITCHING-SYSTEMS-MIB Trap: a3ComSysReservedTrap3

Figure 91 Adding a New Event Notification

4. From the list of all events that may be encountered, select one of the event-types to associate with this notification. If the event that you pick occurs, the system will send this notification.
5. Click **next**.

Build and Validate an Interface/Service Rule

In this step, you can optionally decide to build a rule that determines if the notification is sent or not for this event. The rule is based on filtering the interface and service information contained in the event and if a match occurs, the notification is sent.



New Notice Interface And Service Rule

● Do not constrain notice against interface or service

○ Send notice only if it contains an interface that matches the interface/service rule below:

TCP/IP Address like: *.*.*.*

Services:
Citrix
DHCP
DNS
DominoIIOP
FTP
HTTP
HTTP-8000
HTTP-8080
HTTP-Management
HTTPS

Figure 92 Specifying an Interface/Service Rule for Event Notification

6. Click one of the radio buttons:

- To NOT build a rule, click Do not constrain notice against interface or service.
- To build a rule, click Send notice only if it contains an interface that matches the interface/service rule below.

7. If you selected to build a rule, specify TCP/IP address and service information that needs to match the interface and service information contained in the event to send the notification. Enter the following:
   a) A **TCP/IP address** where filtering can occur within any of the four octets. Functions/operators supported within an octet include:

   - Address lists (space-delimited)
   - Octet value ranges (the dash "-" operator)
   - Octet value lists (the comma "," operator)
   - Octet value wildcards (the asterisk "*" operator)

   For example:

TCP/IP Address Example	Explanation
192.168.1.1 100.101.102.103	Matches two specific addresses.
192.168.0,1,2,5,21.1	Matches 192.168.0.1, 192.168.1.1, 192.168.2.1, etc.
192.168.1.*	Matches any address with 192.168.1 in the first three octets.
192.168.0.1-99	Matches 192.168.0.1, 192.168.0.2, 192.168.0.3, etc.

Another example: The following fields are all valid and would each create the same result set--all TCP/IP addresses from 192.168.0.0 through 192.168.255.255:

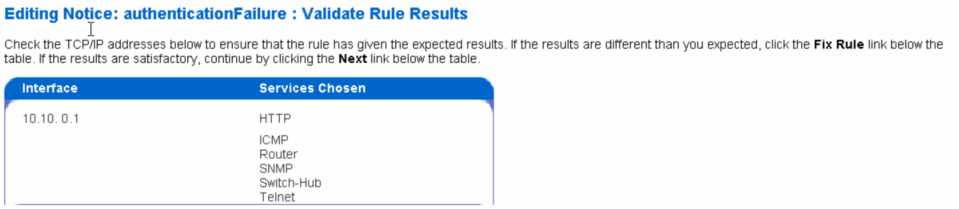
192.168.*.*
192.168.0-255.0-255
192.168.0,1,2,3-255. *

b) Once you've created the TCP/IP address filter, you can select any **service(s)** you would like to add as a filter constraint in conjunction with the TCP/IP address just specified. For example, highlighting both HTTP and FTP will match TCP/IP addresses that support HTTP **OR** FTP.

You can select multiple individual services by holding down the **Ctrl** key while clicking on your selections. Additionally, you can select ranges of services by clicking on one end of the range, holding down the **Shift** key, and clicking on the opposing end. This functionality is supported by most browsers. If it does not work in your browser, please consult the documentation provided by your browser vendor.

Note: *Choosing no services will include* ***all*** *services in this filter. To reset any TCP/IP address or services selected, click* ***reset values****.*

8. If you do not wish to validate the rule or did not define an interface/service rule, click **skip results validation** to continue. Otherwise, click **validate rule results** to provide a visual representation of the rule just built and check that the TCP/IP address(es) and/or service(s) specified returned expected results.



Editing Notice: authenticationFailure : Validate Rule Results

Check the TCP/IP addresses below to ensure that the rule has given the expected results. If the results are different than you expected, click the **Fix Rule** link below the table. If the results are satisfactory, continue by clicking the **Next** link below the table.

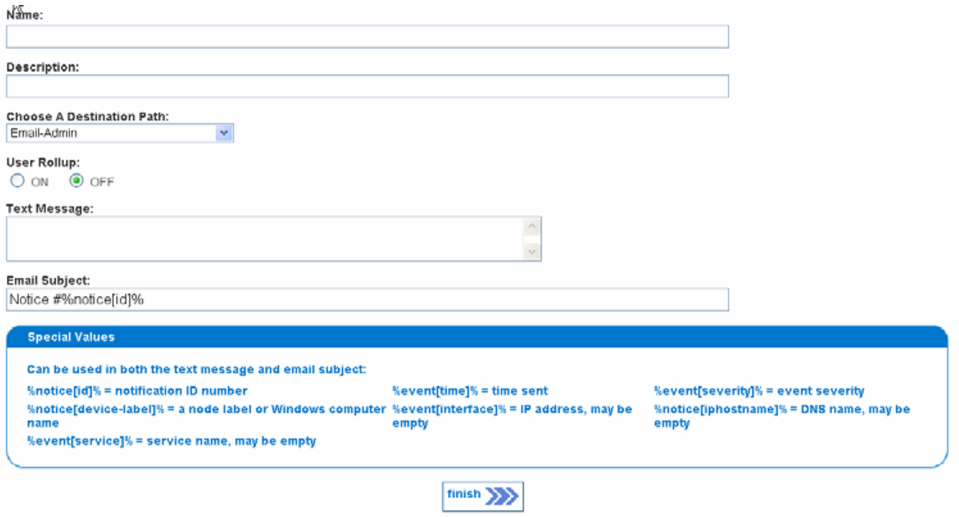
Interface	Services Chosen
10.10. 0.1	HTTP ICMP Router SNMP Switch-Hub Telnet

Figure 93 Validating an Interface/Service Rule

9. Click **Next** if the rule provides expected results; otherwise, click **fix rule** to edit the interface/service rule as described in the above steps.

Enter Content for Notification and Notification Path

In this step, you will enter information that will identify this event and how it appears in the Notification Browser and specify who this notification will be sent to.



Name:

Description:

Choose A Destination Path: Email-Admin

User Rollup: ○ ON ● OFF

Text Message:

Email Subject: Notice #%notice[id]%

Special Values

Can be used in both the text message and email subject:

%notice[id]% = notification ID number

%notice[device-label]% = a node label or Windows computer name

%event[service]% = service name, may be empty

%event[time]% = time sent

%event[interface]% = IP address, may be empty

%event[severity]% = event severity

%notice[iphostname]% = DNS name, may be empty

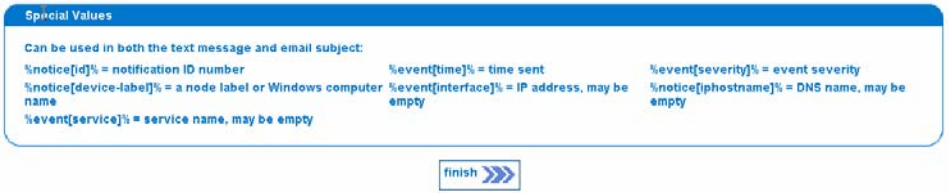
Figure 94 Entering Notification Recipient Information

10. Type a unique **Name** of the recipient for this notice. This is a required field. Use only letters, numbers, and underscore characters. If the name is not unique, the previous notice that had the name will be overwritten.
11. Type a textual **Description** for this event notification. This is optional.
12. Type the **Destination Path** that describes what users or groups will receive notifications, how the notifications will be sent, and who to notify if escalation is needed. This is a required field. You can custom-configure destination paths – please see section **Configure Notification Paths** later in this chapter for additional information).
13. Enable or disable **User Rollup** – a feature that prevents a user's email or pager from being overloaded by simultaneous notifications by collecting notifications that occur over a short time period. The feature will then "roll up" the notifications into a single email or pager message with summary information about each individual notification. This is very useful for notifications that may occur on many interfaces at once, such as **Service Down** or **Node Down** notifications.
14. Type a **Text Message** that is sent with this notification that should outline the reason why the event was triggered. This is a required field. The message will appear in the body of an email

and will also appear in the **Notification Browser** as described in Raritan's *CC-NOC User Guide*.

15. Type an **Email Subject** that will appear as the subject of the email sent as a result of this Event Notification. This is optional and a default subject "`Notice #%notice[id]%`" will be used if text is not provided.

The **Special Values** box outlines some strings that can be embedded in the **Email Subject** and **Text Message** fields to give more information about the event that triggered the notice. It is recommended that the notice id be placed in the subject or text of the notice, which can be accomplished by placing the string "`%notice[id]%`" in the **Email Subject** and **Text Message** fields. Ideally, you want the Email Subject and Text Message fields to be as detailed as possible so the recipient of the notification understands the problem quickly and can begin remediation immediately without having to log into the CC-NOC.



Special Values

Can be used in both the text message and email subject:

%notice[id]% = notification ID number
%event[time]% = time sent
%event[severity]% = event severity
%notice[device-label]% = a node label or Windows computer name
%event[interface]% = IP address, may be empty
%notice[iphostname]% = DNS name, may be empty
%event[service]% = service name, may be empty

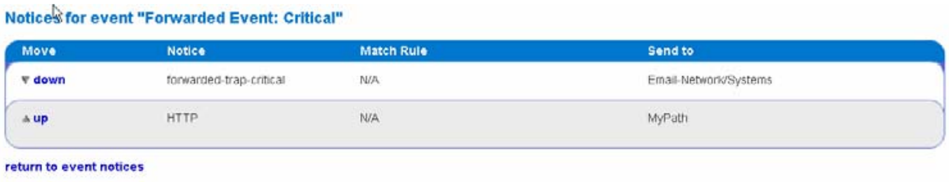
Figure 95 Special Values for Email Subject and Text Message Fields

16. Click **Finish**.

***Note:** You can also include asset table information in notification messages. This will allow you to provide detailed location information in your notifications, making it easier to locate the hardware responsible for the notification. Please see **Appendix F: Notification Parameters** for a list of asset table variables.*

Arrange Notice Hierarchy

If you created multiple notices for a single event class, it is important to go back and arrange the hierarchy of the notices by clicking **arrange these notices** within the Event class. This is because the Notification Engine will send out the first event that matches its rules set.



Notices for event "Forwarded Event: Critical"

Move	Notice	Match Rule	Send to
▼ down	forwarded-trap-critical	N/A	Email-Network/Systems
▲ up	HTTP	N/A	MyPath

Figure 96 Arranging Event Notifications

For example, you built a separate **NodeDown** notice to add into the default one that will notify the "custom" destination path, that is, certain users, when only a certain subnet (192.168.3.*) suffers NodeDown outages.

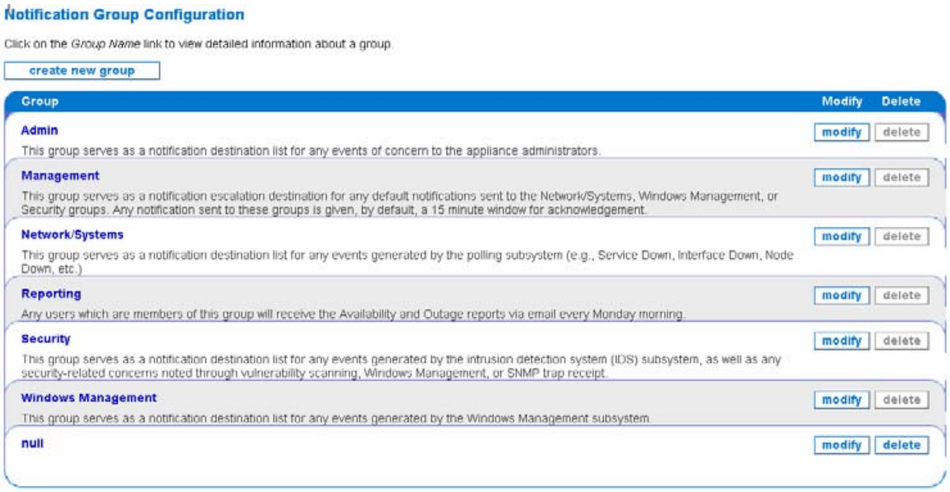
Notices with more specific rules should be placed before those that are more general to ensure that the correct notice is chosen. For instance, if you have two notices with the rules 'IPADDR IPLIKE *.*.*.*' and 'IPADDR IPLIKE 10.*.*.*' you should place the fully wild carded address last so that it could act as a catch all for the event. If the fully wild-carded notice were placed first it would always be chosen over the other more specific notice rules. To move notices**,** simply select either the up or down links beside the Notice name.

Configure Notification Groups

In this section, you will create groups and assign users to them to identify a group of people that should receive certain types of notifications. Notification groups are used when defining a notification path – please see section **Configure Notification Paths** later in this chapter for additional information.

***Note:** To assign users to a group, the users must be pre-defined – please see section **Add a New User** in **Chapter 8: Creating Users, Categories, Views** for additional information.*

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Notification Configuration**.
3. Click **Configure Notification Groups**.



Notification Group Configuration

Click on the *Group Name* link to view detailed information about a group.

Group	Modify	Delete
Admin This group serves as a notification destination list for any events of concern to the appliance administrators.	modify	delete
Management This group serves as a notification escalation destination for any default notifications sent to the Network/Systems, Windows Management, or Security groups. Any notification sent to these groups is given, by default, a 15 minute window for acknowledgement.	modify	delete
Network/Systems This group serves as a notification destination list for any events generated by the polling subsystem (e.g., Service Down, Interface Down, Node Down, etc.)	modify	delete
Reporting Any users which are members of this group will receive the Availability and Outage reports via email every Monday morning.	modify	delete
Security This group serves as a notification destination list for any events generated by the intrusion detection system (IDS) subsystem, as well as any security-related concerns noted through vulnerability scanning, Windows Management, or SNMP trap receipt.	modify	delete
Windows Management This group serves as a notification destination list for any events generated by the Windows Management subsystem.	modify	delete
null	modify	delete

Figure 97 Configure Notification Groups

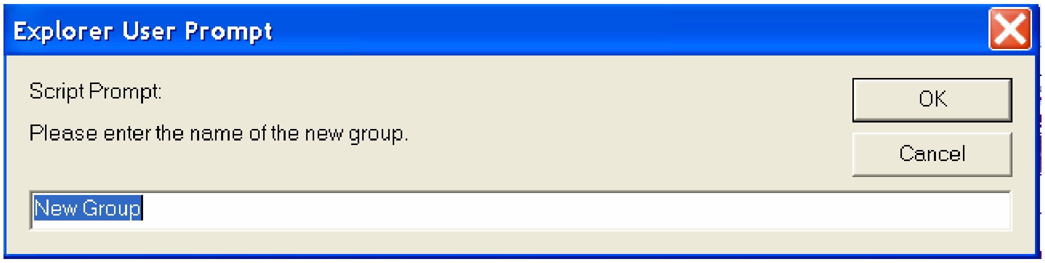
This page lists the default notification groups. Each group is listed in its own panel, and you may modify the definition of the group by clicking **modify** or remove a group by clicking **delete** next to it.

The next section explains how to add a new notification group or modify one.

Add/Modify a Notification Group

To add a new notification group, click **create new group** and you will be walked through the configuration of the new notification group as described in the next few steps.

Clicking **modify** next to a notification group follows the same steps, allowing you to modify information already defined for the group, but bypasses entering a new group name.



Explorer User Prompt

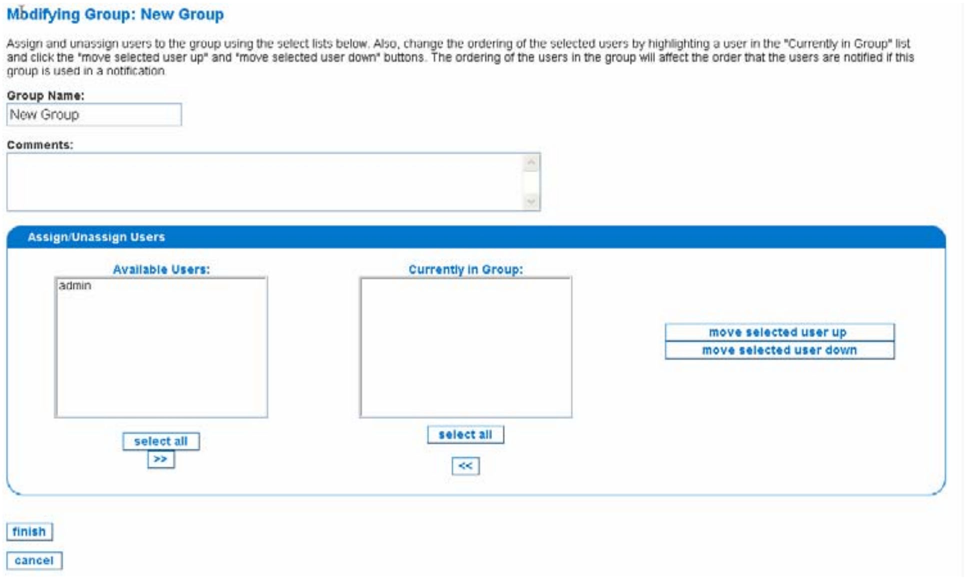
Script Prompt:

Please enter the name of the new group.

New Group

Figure 98 Assigning a Name to a Notification Group

4. Type a unique new group name and click **OK**.



Modifying Group: New Group

Assign and unassign users to the group using the select lists below. Also, change the ordering of the selected users by highlighting a user in the "Currently in Group" list and click the "move selected user up" and "move selected user down" buttons. The ordering of the users in the group will affect the order that the users are notified if this group is used in a notification

Group Name: New Group

Comments:

Figure 99 Assigning Users to a Notification Group

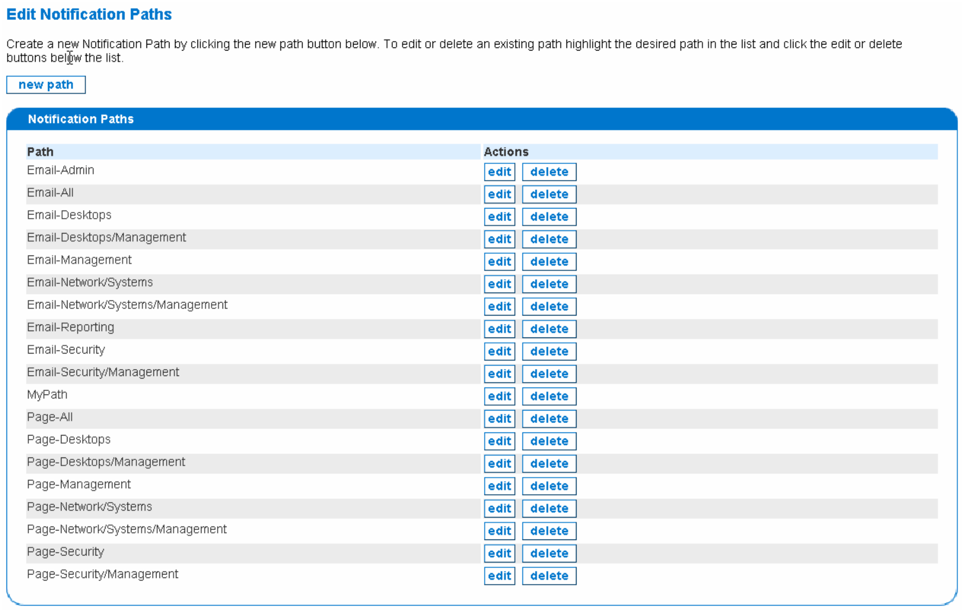
5. Type in comments that describe the group. This is optional.
6. Assign users to the group by clicking **select all**, or **Ctrl+click** to select more than one user, or hold down the **Shift** key and click on the opposing end to select a range of users. Select >> to move the users to the **Currently in Group:** box.
7. Change the ordering by selecting a user in the **Currently in Group:** box and clicking **move selected user up** or **move selected user down**. The ordering of the users in the group will affect the order that the users are notified if this group is used in a notification.
8. Click **finish**.

Configure Notification Paths

In this section, you will create notification paths that defines the users or groups who will receive notifications, how the notifications will be sent, for example, numeric or text pagers, email, and who to notify if escalation is needed. Notification paths are selected when configuring an event notification and should be created before configuring an event notification – please see section **Configure Event Notifications** earlier in this chapter for additional information.

***Note:** Numeric and text pagers can be used to communicate with Telocator alphanumeric protocol (TAP) paging providers. Please contact Raritan Technical Support for information about how to configure the paging functions.*

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Notification Configuration**.
3. Click **Configure Notification Paths**.



Edit Notification Paths

Create a new Notification Path by clicking the new path button below. To edit or delete an existing path highlight the desired path in the list and click the edit or delete buttons below the list.

Notification Paths

Path	Actions
Email-Admin	edit delete
Email-All	edit delete
Email-Desktops	edit delete
Email-Desktops/Management	edit delete
Email-Management	edit delete
Email-Network/Systems	edit delete
Email-Network/Systems/Management	edit delete
Email-Reporting	edit delete
Email-Security	edit delete
Email-Security/Management	edit delete
MyPath	edit delete
Page-All	edit delete
Page-Desktops	edit delete
Page-Desktops/Management	edit delete
Page-Management	edit delete
Page-Network/Systems	edit delete
Page-Network/Systems/Management	edit delete
Page-Security	edit delete
Page-Security/Management	edit delete

Figure 100 Configuring a Notification Path

This page lists the default notification paths. Each path is listed and you may edit the definition of the path by clicking **edit** or remove a path by clicking **delete** next to it. The next section explains how to add a new notification path or edit one.

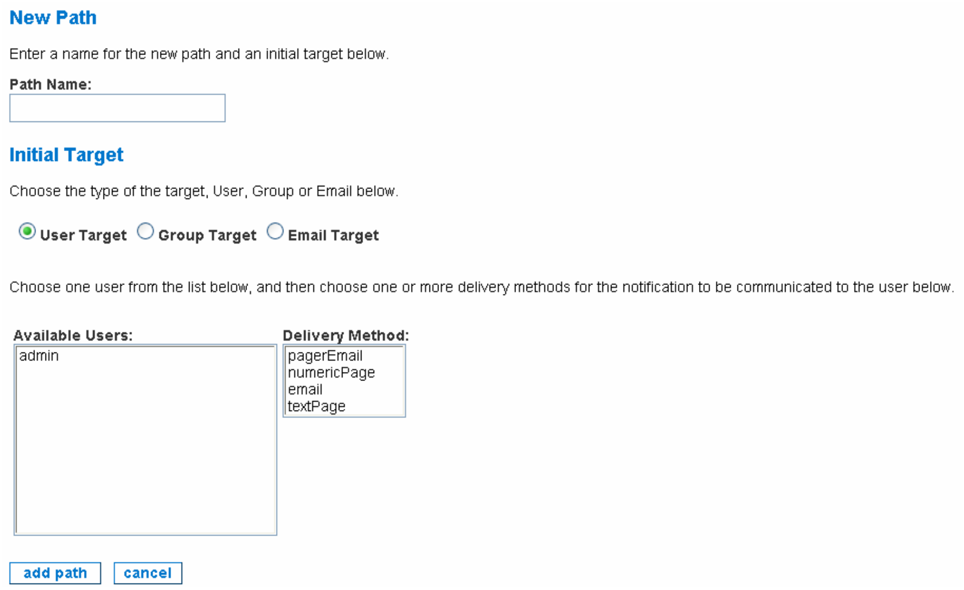
Add/Edit a Notification Path

To add a new notification path, click **new path** and you will be walked through the configuration of a new notification path as described in the next few steps.

Clicking **edit** next to a notification path follows the same steps, allowing you to edit information already defined for the path, but allows you to change the path name, path criteria, and escalation criteria instead of entering new data.

Create New Path Name and Specify Targets

In this step, you need to specify a new name and select a target, that is, user, group, or email.



New Path

Enter a name for the new path and an initial target below.

Path Name:

Initial Target

Choose the type of the target, User, Group or Email below.

● User Target ○ Group Target ○ Email Target

Choose one user from the list below, and then choose one or more delivery methods for the notification to be communicated to the user below.

Available Users:
admin

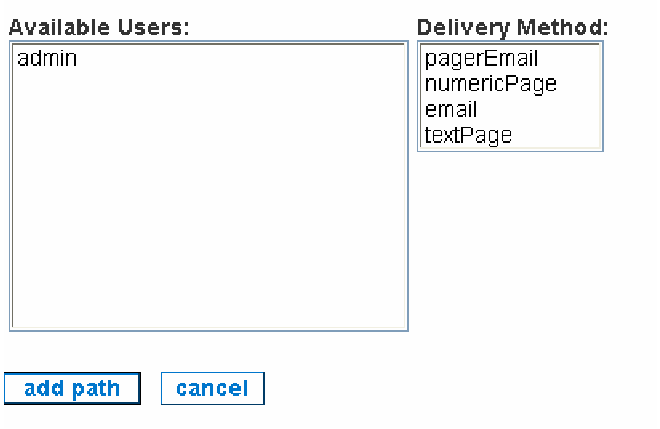
Delivery Method:
pagerEmail
numericPage
email
textPage

Figure 101 Configuring a Notification Path

To create a new notification path:

4. Type a unique new **path name**. The name must be alphanumeric and can include "/", and "–", and "_" characters.
5. Choose one of the **target types** for this notification path:

- For **User Target**, select only one user and select one or more delivery methods for that user.



Available Users:
admin

Delivery Method:
pagerEmail
numericPage
email
textPage

Figure 102 Configuring a User Target in Notification Path

- For **Group Target**, select only one group as previously defined, please see section **Configure Notification Groups** earlier in this chapter for details, and specify an interval, that is, minutes, hour, or days, to indicate how long to wait before sending the notification to users in this group. Then select one or more delivery methods for the group.

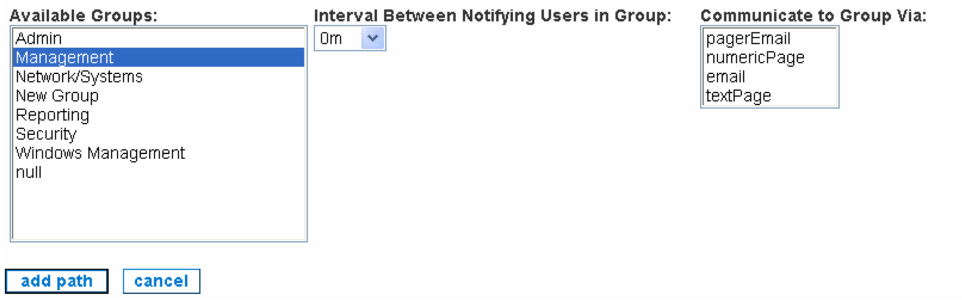


Figure 103 Configuring a Group Target in Notification Path

- For **Email Target** and type an email address for the notification path.

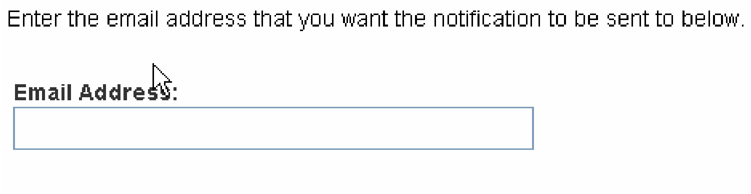
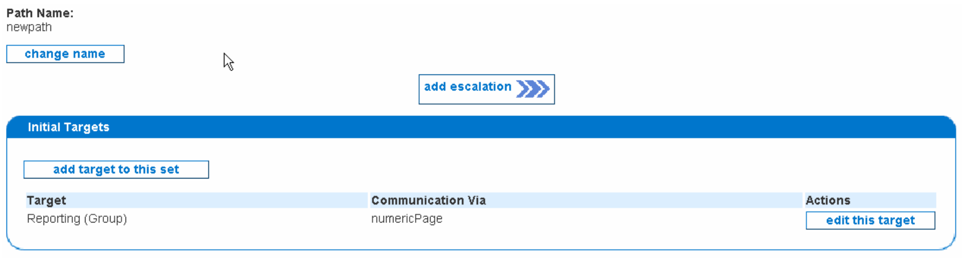

Enter the email address that you want the notification to be sent to below.

Figure 104 Configuring an Email Target in Notification Path

6. Click **add path**.

Modify a Notification Path

In this page, you can confirm the notification path name, add or edit targets, and continue to define the escalation for this notification path.


Path Name:
newpath

Target	Communication Via	Actions
Reporting (Group)	numericPage	edit this target

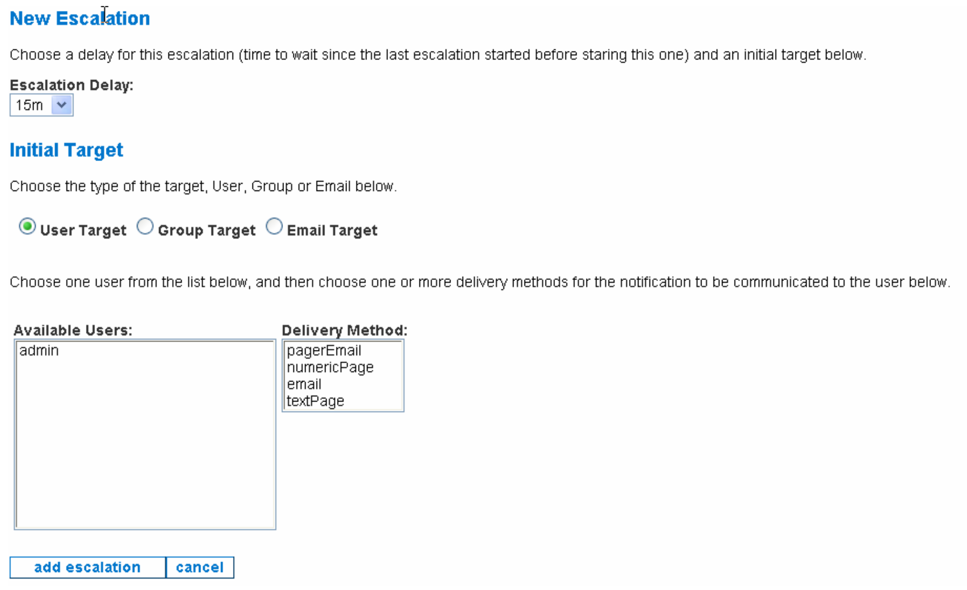
Figure 105 Modify Notification Paths

To modify a notification path:

1. Change the name of the notification path by clicking **change name.** This is optional.
2. Click **add target to this set** if you wish to add additional targets. This is optional.
3. Click **edit this target** to redefine the target information. This is optional.
4. Click **add escalation** to continue.

Define Escalation in Notification Path

In this step, you need to define how long the CC-NOC will wait until it sends a subsequent notification after sending out the first one. You also need to specify who will be receiving this subsequent notification.



New Escalation

Choose a delay for this escalation (time to wait since the last escalation started before staring this one) and an initial target below.

Escalation Delay: 15m

Initial Target

Choose the type of the target, User, Group or Email below.

● User Target ○ Group Target ○ Email Target

Choose one user from the list below, and then choose one or more delivery methods for the notification to be communicated to the user below.

Available Users: admin

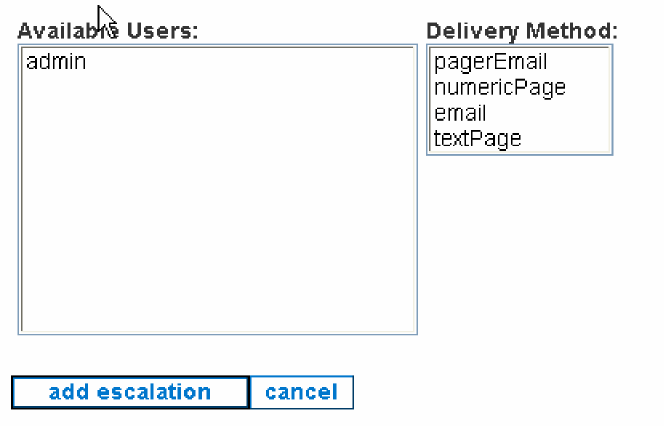
Delivery Method: pagerEmail, numericPage, email, textPage

Figure 106 Define Escalation in Notification Path

To define the escalation for a notification path:

5. Select a time interval, that is, minutes, hour, or days, that specifies how long to wait before sending the subsequent notification to users in the target as defined below.
6. Choose one of the **target types** for this escalation notification:

- For **User Target**, select only one user and select one or more delivery methods for that user.

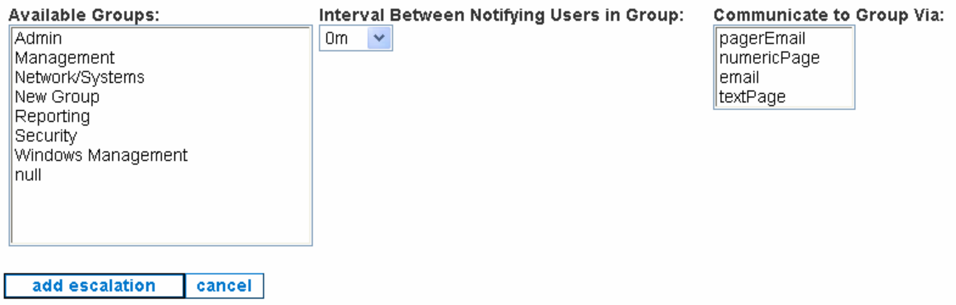


Available Users: admin

Delivery Method: pagerEmail, numericPage, email, textPage

Figure 107 Configuring a User Target for Escalation in Notification Path

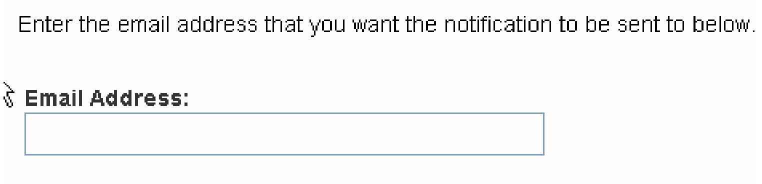
- For **Group Target**, select only one group as previously defined, see section **Configure Notification Groups** earlier in this chapter for additional information, specify an interval, that is, minutes, hour, or days, to indicate how long to wait before sending the notification to users in this group. Then select one or more delivery methods for the group.



Interval Between Notifying Users in Group: 0m

Figure 108 Configuring a Group Target for Escalation in Notification Path

- For **Email Target**, type an email address for the notification path.



Enter the email address that you want the notification to be sent to below.

Figure 109 Configuring an Email Target in Notification Path

7. Click **add escalation**.

Configure TAP Paging

This section explains configuring the Telocator Alphanumeric Protocol (TAP) for a specific paging service provider. This allows the CC-NOC to send notifications to users' pagers if the appliance has its modem connected to a telephone line.

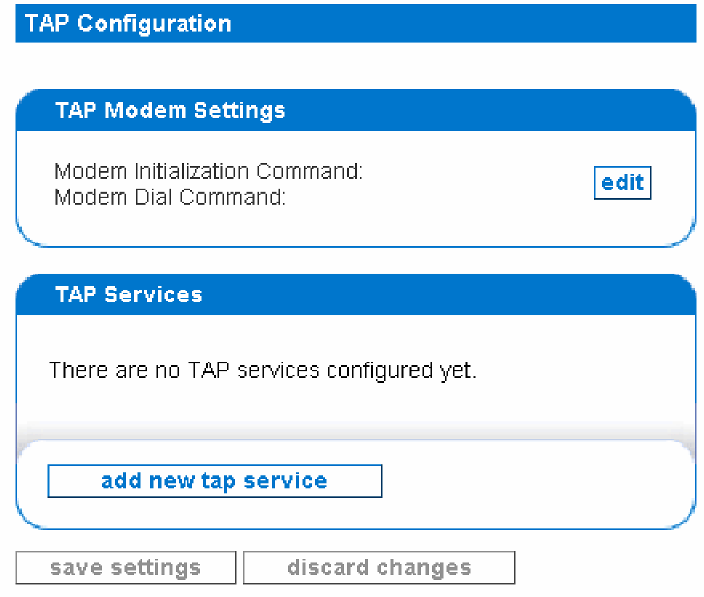
TAP is a standard protocol that enables modems to send text messages to pager systems. The CC-NOC can use TAP services to send notifications as text messages to pagers. There are several steps to get this working properly.

First, you need to attach a modem to the CC-NOC and to a phone line so that pager messages can be sent. Please contact Technical Support for a list of supported modem devices.

Next, you must set up the modem and service providers using this page. If your modem requires special parameters for initialization or dialing prefixes, such as dialing "9" to get an outside line, enter these parameters in the **TAP Modem Settings** box by clicking **edit**.

Note: *Type PIN numbers for an individual when adding or editing a user. Please see* ***Chapter 8: Creating Users, Categories, Views*** *for additional information.*

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Notification Configuration**.
3. Click **TAP Paging Configuration**.



TAP Configuration

TAP Modem Settings

Modem Initialization Command:
Modem Dial Command:

TAP Services

There are no TAP services configured yet.

Figure 110 Configuring TAP Paging

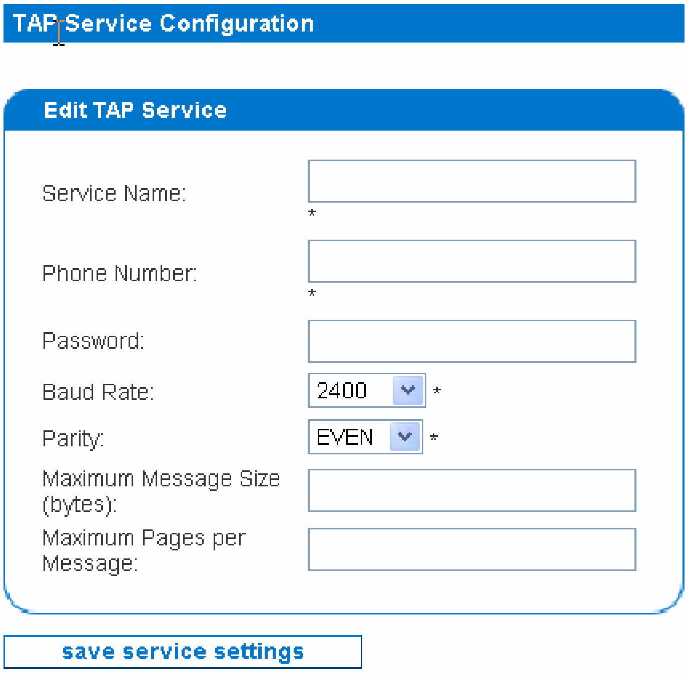
Add a new TAP Service

In this step, you need to enter the phone number, baud rate, and other information for a TAP service. Different phone carriers will typically have separate TAP services so if you have pagers from different phone carriers or from different manufacturers, you may need to enter settings for several TAP services. Refer to your phone carrier for more information about TAP service availability and settings.

These settings are necessary for the modem to dial out and connect to a TAP service. Fields that are required are marked with an asterisk.

To add a TAP provider:

4. Click **add new tap service**.



TAP Service Configuration

Edit TAP Service

Service Name: *

Phone Number: *

Password:

Baud Rate: 2400 *

Parity: EVEN *

Maximum Message Size (bytes):

Maximum Pages per Message:

Figure 111 Editing TAP Service

5. Type a unique identifier for this TAP service in **Service Name**. This is required.
6. Type the phone number of the TAP service in **Phone Number**. If the phone line that the modem will be attached to requires certain prefixes, such as "9" to dial out, enter those values while configuring TAP modem settings – please see the next section **Edit Modem Parameters** for additional information.
7. Type the **Password** for the TAP service.
8. Select the **Baud Rate** and **Parity** of the service. These are required fields.
9. Type a maximum message size in bytes. This is optional.
10. Type a maximum number of pages per message. This is optional.
11. Click **save service settings**.

Edit Modem Parameters

In this step, you will set up the modem parameters. If your modem requires special parameters for initialization or dialing prefixes, such as dialing "9" to get an outside line, you'll need to enter these parameters. These settings are necessary for the modem to initialize properly. All of the fields on this page are optional.

Note: *If you need assistance in setting up modem parameters, please call Technical Support.*

To edit modem parameters:

1. Click **edit** in the TAP Modem Settings box.

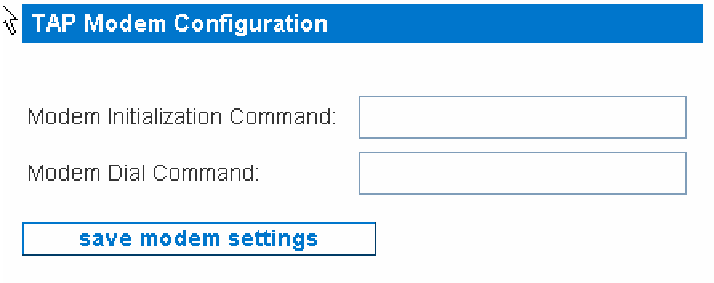


Figure 112 Editing Modem Parameters

2. Type the **Modem Initialization Command**, which should be an AT-command that is sent to the modem to bring it online.
3. Type the **Modem Dial Command**, which should be an AT-command that is sent to the modem to bring the modem online and ready to dial.

Revert to Original Configuration

If necessary, you can replace your current notification and destination path configuration with the default configurations that your CC-NOC came with.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Notification Configuration**.

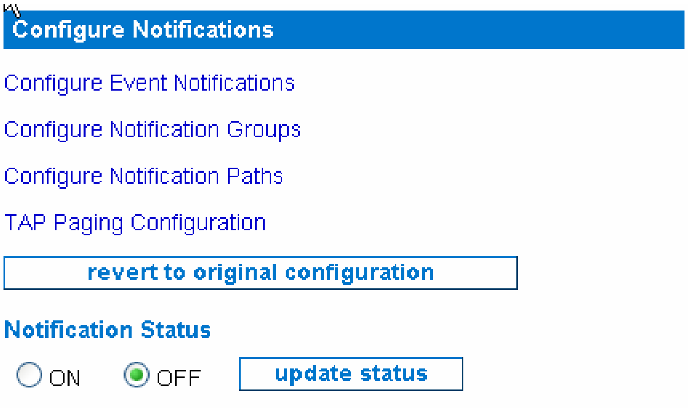

Configure Notifications
Configure Event Notifications
Configure Notification Groups
Configure Notification Paths
TAP Paging Configuration
revert to original configuration
Notification Status
○ ON
● OFF
update status

Figure 113 Editing Modem Parameters

3. Click **revert** to go back to the original configuration.

Chapter 7: Managing Assets

This chapter describes procedures to configure a CC-NOC so it can track and share important information about capital assets in your organization. This data, when coupled with information about your network that is obtained by the CC-NOC during network discovery, can be a powerful tool not only for solving problems, but in tracking the current state of equipment repairs as well as network or system related moves, additions, or changes. The information entered here can augment the information of an IP device – for example, it can be a keyboard, mouse, the printer, etc. of a discovered node. Typically, the asset information is mapped to a node – see section **Map Unassociated Assets to Nodes** later in this chapter for additional information. Asset inventory tracking delivers on-demand reports of hardware and software inventory enabling greater productivity, financial accountability, and end-user satisfaction.

Manage Assets

This section describes how to:

- Import Assets
- Export Assets
- Map Unassociated Assets to Nodes

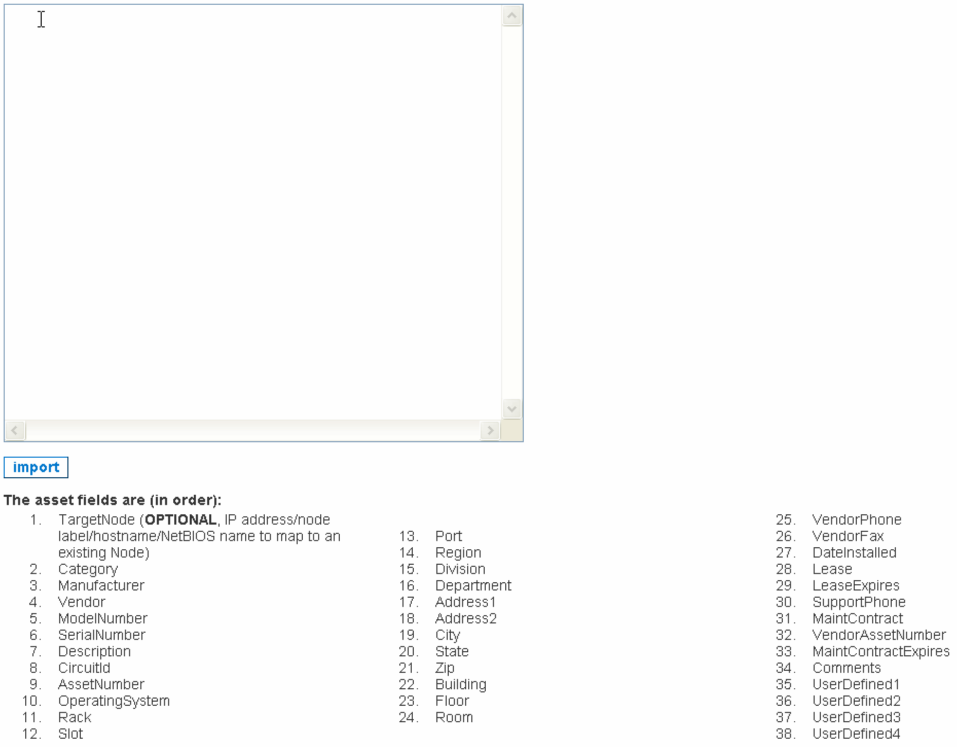
Note: *Creating and listing assets is described in the* ***CommandCenter NOC User Guide****.*

Import Assets

The second way in which to add or update asset data stored in the CC-NOC is to import a comma-separated value file (CSV) into the assets database. This file was most likely exported from a spreadsheet and this file format is supported by most spreadsheet and database applications. If the CSV file was created by previously exporting it from CC-NOC, then each record will have an asset ID. This will cause that row of data to be updated with the rest of the data in that row. If no asset ID is supplied, then a new asset will be created for that row of data.

1. Click on the **Assets** tab in the top navigation tab bar.
2. Click **Manage assets**.

3. Click **Import Assets**.



The asset fields are (in order):

1. TargetNode (**OPTIONAL**, IP address/node label/hostname/NetBIOS name to map to an existing Node)
2. Category
3. Manufacturer
4. Vendor
5. ModelNumber
6. SerialNumber
7. Description
8. CircuitId
9. AssetNumber
10. OperatingSystem
11. Rack
12. Slot
13. Port
14. Region
15. Division
16. Department
17. Address1
18. Address2
19. City
20. State
21. Zip
22. Building
23. Floor
24. Room
25. VendorPhone
26. VendorFax
27. DateInstalled
28. Lease
29. LeaseExpires
30. SupportPhone
31. MaintContract
32. VendorAssetNumber
33. MaintContractExpires
34. Comments
35. UserDefined1
36. UserDefined2
37. UserDefined3
38. UserDefined4

Figure 114 Importing assets

4. Paste your comma-separated values into this text field to import them into the assets database. There is one line per record, and the fields are delimited by commas. A new asset record will be created for each line.
5. Click **import**.

Note: *You MUST include all 38 fields – even if there is no data between the comma delimiters, the commas have to be included.*

If you are rebuilding the asset records from an export via the CC-NOC, you will need to clear the asset table prior to re-importing – please see section **Clear all Asset Records** later in this chapter for additional information. Otherwise, all asset records will be duplicated.

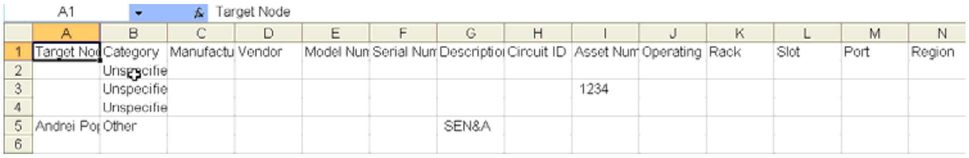
After importing, you can supply a **Target Node** field that will be used to do a "best guess" mapping between an asset and a node based on a match between the **Target Node** and the node's IP address, label, hostname or machine name. If no **Target Node** is supplied for an asset, it will not appear on the mapping page. You will be able to manually choose the node for any asset from its detail page. Please see section **Map Unassociated Assets to Nodes** later in this chapter for additional information.

You can also choose to ignore the mapping of an asset at this time by clicking **[skip mapping].** This marking will still allow this asset to be listed on this page with its best guess assets. Or you can exclude an asset that has a **Target Node** field from being included in this listing. You will still be able to manually associate a node to any assets marked in this way via the asset's detail page.

Export Assets

All the nodes with asset information can be exported to a comma-separated value file **(**CSV), which is suitable for use in a spreadsheet application. If you do an import into the CC-NOC with this CSV file**,** you will be asked to re-map all assets that were previously mapped to a node.

1. Click on the **Assets** tab in the top navigation tab bar.
2. Click **Manage assets**.
3. Click **Export Assets**.
4. Click **open** to view the assets in Excel.



A1 Target Node

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Target Nod	Category	Manufactu	Vendor	Model Nun	Serial Num	Descriptio	Circuit ID	Asset Num	Operating	Rack	Slot	Port	Region
2		Unspecifie												
3		Unspecifie							1234					
4		Unspecifie												
5	Andrei Po	Other					SEN&A							
6														

Figure 115 Exporting assets

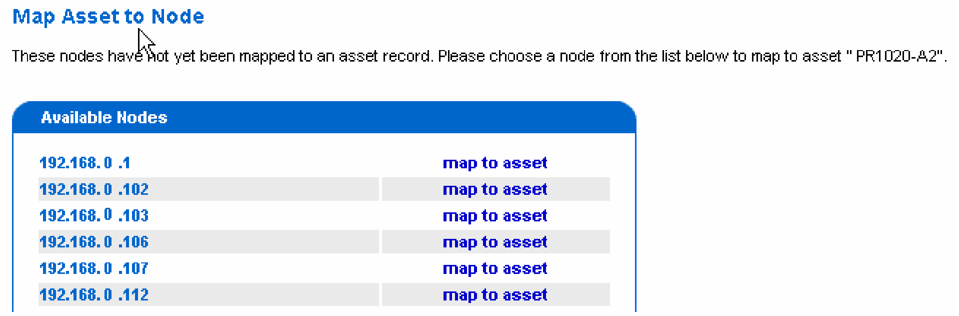
5. Save the file by clicking **File**, **Save As**.

Map Unassociated Assets to Nodes

Click **Map Unassociated Assets to Nodes** to display a list of all assets that have not yet been associated with a node. Any assets that you imported with a **Target Node** field and have not already been associated with a node will be listed along with a "best guess" as to what node it should be associated with based on a match between the **Target Node** and a node's IP Address, Node Label, Hostname or Machine Name.

By assigning assets to nodes, the notification process will be able to give you more information concerning the machines that are affected.

1. Click on the **Assets** tab in the top navigation tab bar.
2. Click **List all assets**.
3. Click on an asset.
4. At the top of the page, click **Associate asset to node**.



Map Asset to Node

These nodes have not yet been mapped to an asset record. Please choose a node from the list below to map to asset " PR1020-A2".

Available Nodes	
192.168.0 .1	map to asset
192.168.0 .102	map to asset
192.168.0 .103	map to asset
192.168.0 .106	map to asset
192.168.0 .107	map to asset
192.168.0 .112	map to asset

Figure 116 Mapping unassociated assets to nodes

5. Choose a node from the list and click **map to asset**.

Note: *Alternatively, you can click on the* ***Assets*** *tab, click* ***Manage Assets****, and click* ***Map Unassociated Assets to Nodes****.*

Clear All Asset Records

This allows you to remove all asset records from the CC-NOC. Be sure to export the assets if you ever need to recover this data in the future. If you are rebuilding the asset records from an export via the CC-NOC, you will need to clear the asset table prior to re-importing. Otherwise, all asset records will be duplicated.

1. Click on the **Assets** tab in the top navigation tab bar.
2. Click **Manage assets**.
3. Click **clear asset records**.

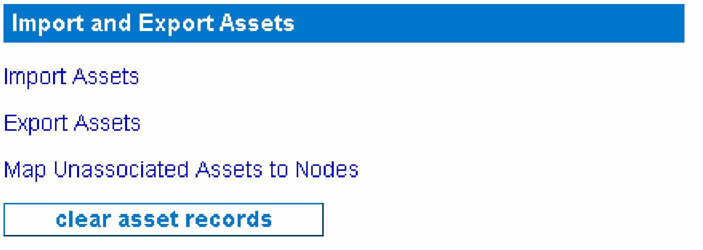


Figure 117 Clear all asset records

Chapter 8: Creating Users, Categories, Views

This chapter describes procedures to add users, delete and modify users, build views, and create categories. Build your own custom way of looking at your network, called views, and then assign them to your users. Categories allow you to define specific groups of systems and/or services. The rules created when defining categories will be used in the user interface, the reports, and availability calculations.

Create, Modify, Delete Users

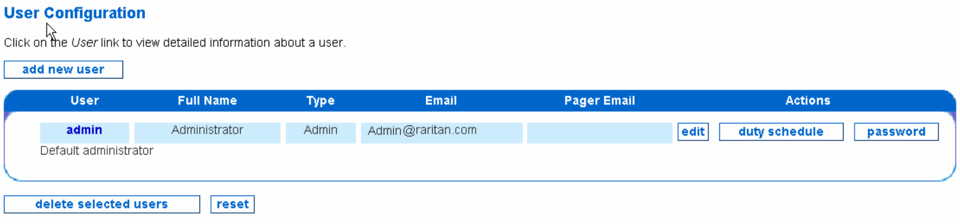
Only those with administrative privileges can add, modify or delete existing users. Users provide a way for you to control access to the appliance's web interface, as well as map email and pager destination addresses and duty schedules to individual technicians. If adding or modifying users, be prepared with user IDs, passwords, notification contact information, for example, email addresses and/or pager e-mails, and duty schedule information.

***Note:** To add a user to a notification group, refer to **Chapter 6: Configuring Notifications**. This way if a notification gets sent to an entire group, the user that is added to the notification group will also receive the notification.*

Add a New User

Use this option to add a new user.

1. Click on the **Admin** tab in the top navigation bar.
2. **Click User Configuration.**



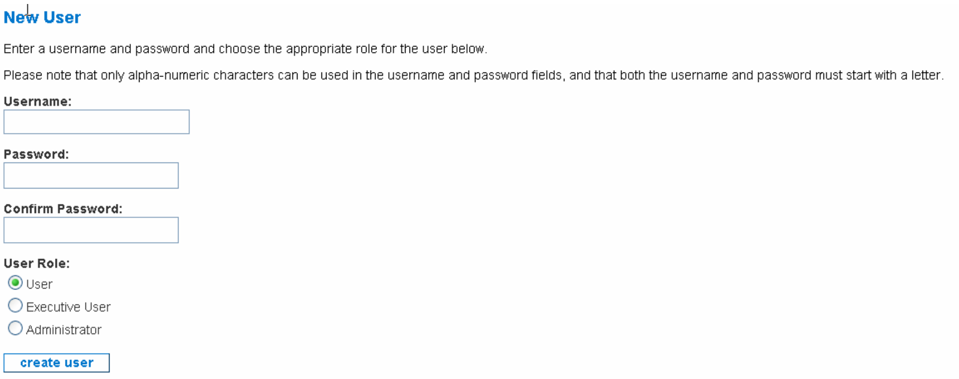
User Configuration

Click on the *User* link to view detailed information about a user.

User	Full Name	Type	Email	Pager Email	Actions
admin Default administrator	Administrator	Admin	Admin@raritan.com		edit duty schedule password

Figure 118 Managing users

3. Click **add new user**.



New User

Enter a username and password and choose the appropriate role for the user below.

Please note that only alpha-numeric characters can be used in the username and password fields, and that both the username and password must start with a letter.

Username:

Password:

Confirm Password:

User Role:

● User
○ Executive User
○ Administrator

Figure 119 Adding a New User

4. Type a **username**. The username must begin with a letter and can contain only alpha-numeric characters. Spaces and punctuation is not allowed.
5. Type and confirm a **password**, which must begin with a letter.
6. Select the role of the user you are adding:

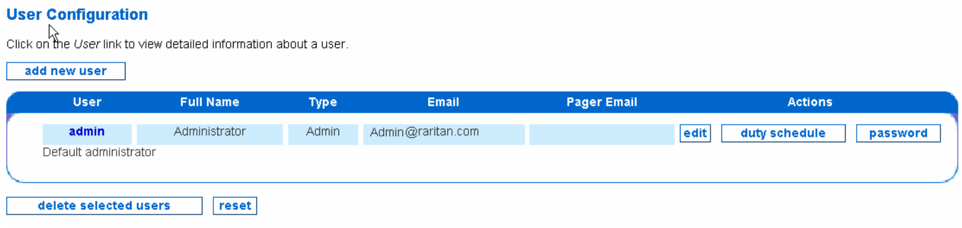
- **Operators —** have access to everything on the CC-NOC except administrative configurations.
- **Executive User —** have read-only access to only a few key reports that show the network health at a high level.
- **Admin —** have configuration access to the CC-NOC.

7. Click **create user**.

Edit a User

When adding or editing a user, the procedure below will be the same.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **User Configuration**.



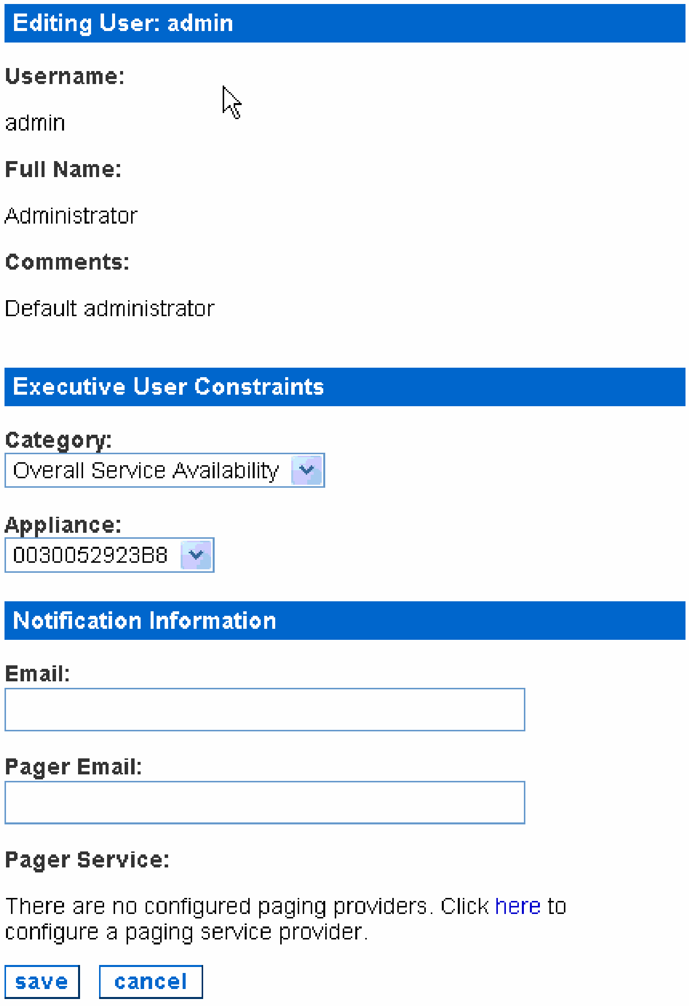
User Configuration

Click on the *User* link to view detailed information about a user.

User	Full Name	Type	Email	Pager Email	Actions
admin Default administrator	Administrator	Admin	Admin@raritan.com		edit duty schedule password

Figure 120 Editing a User

3. If you are changing the administrator password, click **password** next to the administrator account.
4. Click **edit** next to the user whose profile you wish to change.



Editing User: admin

Username:

admin

Full Name:

Administrator

Comments:

Default administrator

Executive User Constraints

Category:
Overall Service Availability

Appliance:
0030052923B8

Notification Information

Email:

Pager Email:

Pager Service:

There are no configured paging providers. Click here to configure a paging service provider.

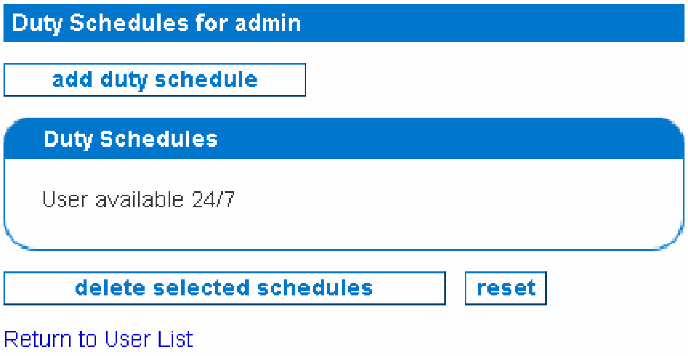
Figure 121 Creating/Editing a new user

5. Supply a full name and enter comments. This is optional.
6. If desired, provide **Executive User Constraints** to provide an executive-level user access only to the specified category and appliance that is specified. This user will not be able to see information on nodes outside of the specified category or data collected by appliances other than the specified appliance.
7. If desired, provide **Notification Information** to provide the ability to configure contact information for each user including email address, pager email in the case that the pager can be reached as an email destination, and text service for alphanumeric pagers or cell phone messaging services that cannot display text messages. To configure a TAP pager service now, gather your service provider's TAP information and click **here** – please see section **Configure TAP Paging** in **Chapter 6: Configuring Notifications** for additional information.
8. Click **save** to save the configuration.

Adding/Editing a Duty Schedule

Duty Schedules allow you the flexibility to determine when users should receive notifications. A duty schedule consists of a list of days for which the time will apply and a time range, with minutes in five minute increments, valid on those days that are checked.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **User Configuration**.
3. Click **duty schedule** next to the user you want to assign a schedule.



Duty Schedules for admin

add duty schedule

Duty Schedules

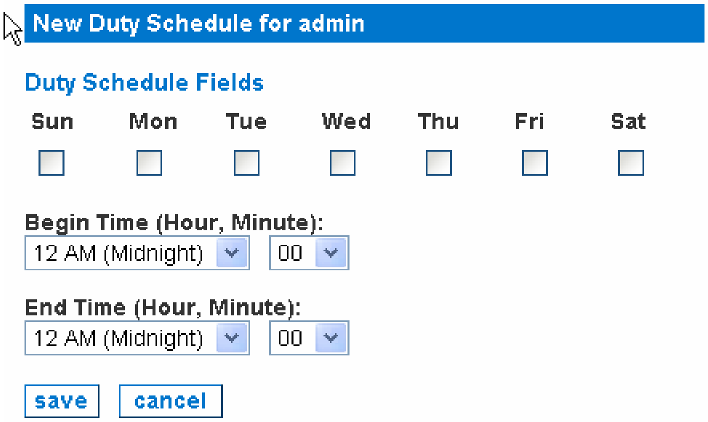
User available 24/7

delete selected schedules | reset

Return to User List

Figure 122 Create a duty schedule

4. Click **add duty schedule**.



New Duty Schedule for admin

Duty Schedule Fields

Sun	Mon	Tue	Wed	Thu	Fri	Sat
□	□	□	□	□	□	□

Begin Time (Hour, Minute):
12 AM (Midnight) | 00

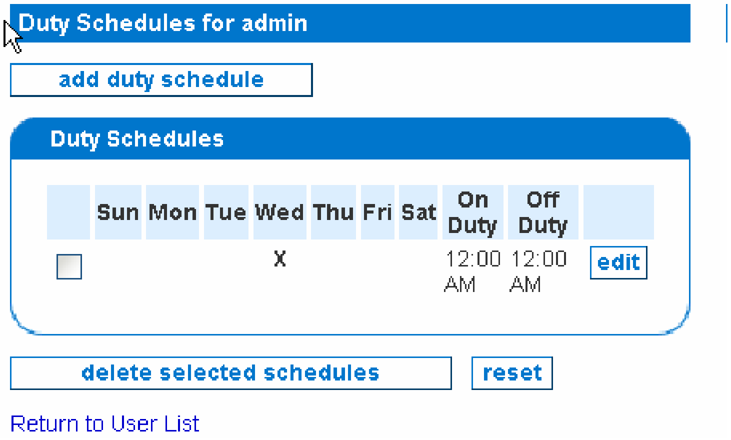
End Time (Hour, Minute):
12 AM (Midnight) | 00

save | cancel

Figure 123 Specifying duty schedule times

5. Check the appropriate days.

6. Choose the start time and stop time from the select boxes. If a user works a shift that spans midnight you will have to enter two duty schedules. One from the start of the shift till midnight, and the second on the next day from midnight till the end of the shift. Then, using the duty schedule fields you have just added, create a duty schedule from the start time to 2359 on one day, and enter a second duty schedule which begins at 0000 and ends at the end of that user's coverage.
7. Click **save**.



	Sun	Mon	Tue	Wed	Thu	Fri	Sat	On Duty	Off Duty	
☐				X				12:00 AM	12:00 AM	edit

Figure 124 Edit, delete, or reset a duty schedule

8. To remove configured duty schedules, put a √ next to the schedule and click **delete selected schedules**.
9. To edit a schedule, click **edit** and re-enter the schedule.

Configure Categories

Configure categories to define specific groups of systems and/or services in rules that will be used in the user interface, reports, and availability calculations. **Categories** are logical groupings of devices, based on filters that you create. CC-NOC provides these default categories:

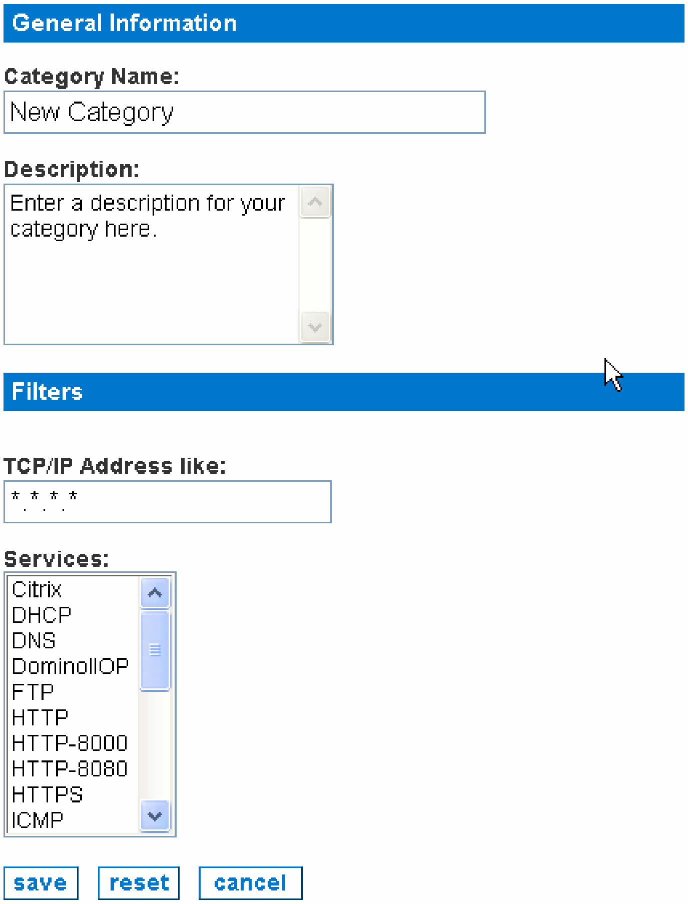
Category	Description
`DNS & DHCP Servers`	Includes all managed interfaces which are running either DNS (name resolution) or DHCP servers.
`Database Servers`	Includes all managed interfaces which are currently running PostgreSQL, Oracle, SQLserver, MySQL, Informix, or Sybase database servers.
`Email Servers`	Includes all managed interfaces that are running an Email service, including SMTP, POP3, or IMAP. This includes MS Exchange Servers running these protocols.
`Internet Connectivity`	Reflects the ability to 'ping' the router at the ISP-end of your Internet connection.
`Network Interfaces`	Reflects the ability to 'ping' managed devices. Ping uses the ICMP protocol, tests the network connectivity and availability of a device.
`Overall Service Availability`	Reflects availability of all services currently being monitored.
`Routers`	Includes all routers that were discovered via SNMP. Note that not all routers not support SNMP, so not all routers may be included in this category. The service availability is based on the ICMP service for the routers.

`Web Servers`	Includes all managed interfaces which are running an HTTP (web) server on port 80 or other common ports.

Categories can then be combined into *views*, providing you the ability to focus users on the nodes that are pertinent to their role. You have the ability to create, modify, and delete categories and the filters that populate them. Using CC-NOC's own TCP/IP address matching functionality, the filters can be created quickly and easily, while being extremely powerful as well.

Note: *Categories should be created first before building a view.*

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Category and View Configuration**.
3. Click **Configure Categories**.
4. Click **add new category**.



Category Name: New Category

Description: Enter a description for your category here.

TCP/IP Address like: *.*.*.*

Figure 125 Configure Categories

5. Type a **category name**.
6. Type a **description** for the category that will be visible on the Category Details pages. It might include information, such as:

- Who created the category
- The intent for why it was created
- When it was created
- An explanation of the filter

7. Specify either IP addresses/ranges or services that will be included in this category. The category will be populated with those nodes/services that you define here so you can design customized views for your users. For example, you could create one category for just Exchange servers, and another for any other mail servers you might have in the environment like a Linux box with Sendmail). Enter the following:

- A **TCP/IP address** where filtering can occur within any of the four octets. Functions/operators supported within an octet include:

  Address lists (space-delimited)
  Octet value ranges (the dash "-" operator)
  Octet value lists (the comma "," operator)
  Octet value wildcards (the asterisk "*" operator)

  For example:

TCP/IP Address Example	Explanation
192.168.1.1 100.101.102.103	Matches two specific addresses.
192.168.0,1,2,5,21.1	Matches 192.168.0.1, 192.168.1.1, 192.168.2.1, etc.
192.168.1.*	Matches any address with 192.168.1 in the first three octets.
192.168.0.1-99	Matches 192.168.0.1, 192.168.0.2, 192.168.0.3, etc.

  Another example: The following fields are all valid and would each create the same result set--all TCP/IP addresses from 192.168.0.0 through 192.168.255.255:

  192.168.*.*
  192.168.0-255.0-255
  192.168.0,1,2,3-255. *

- Once you've created the TCP/IP address filter, you can select any **service(s)** you would like to add as a filter constraint in conjunction with the TCP/IP address just specified. For example, highlighting both HTTP and FTP will match TCP/IP addresses that support HTTP **OR** FTP.

  You can select multiple individual services by holding down the **Ctrl** key while clicking on your selections. Additionally, you can select ranges of services by clicking on one end of the range, holding down the **Shift** key, and clicking on the opposing end. This functionality is supported by most browsers. If it does not work in your browser, please consult the documentation provided by your browser vendor.

Note: *Choosing no services will include* ***all*** *services in this filter. To reset any TCP/IP address or services selected, click* ***reset values****.*

8. Click **save**.
9. After saving the category, restart the CC-NOC.

Configure Views

Configuring views allows you to create a mapping between users and *views,* or sets of categories, they will see when logging into the CC-NOC. Views are simply the combination of categories that your users will see when logging in.

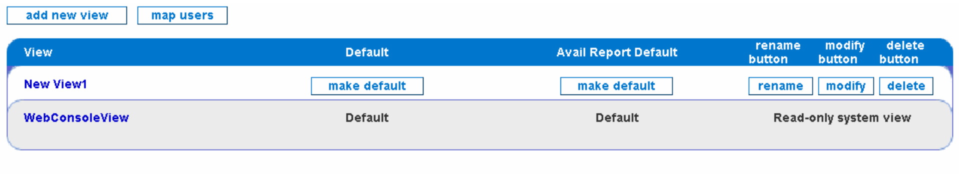
When configuring views, you have the ability to create new views, assign views to specific users, using map users, or set the default views used by the web interface, as well as the default view used by the reporting subsystem. Any new views that you add can be modified.

Note: *The WebConsoleView is considered a "system view" and is not editable.*

A view that is indicated as **Default** will be used for any users that do not have a specific view mapping. A user with no specific view mapping will receive the view that is alphabetically presented first. The view under the **Avail Report Default** column is used when creating the Availability Report – please see Raritan's *CC-NOC User Guide* for additional information on the Availability Report.

To obtain a preview of what the view will look like on the front page of the web console, click on the name of the view to go to the preview page.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Category and View Configuration**.
3. Click **Configure Views**.



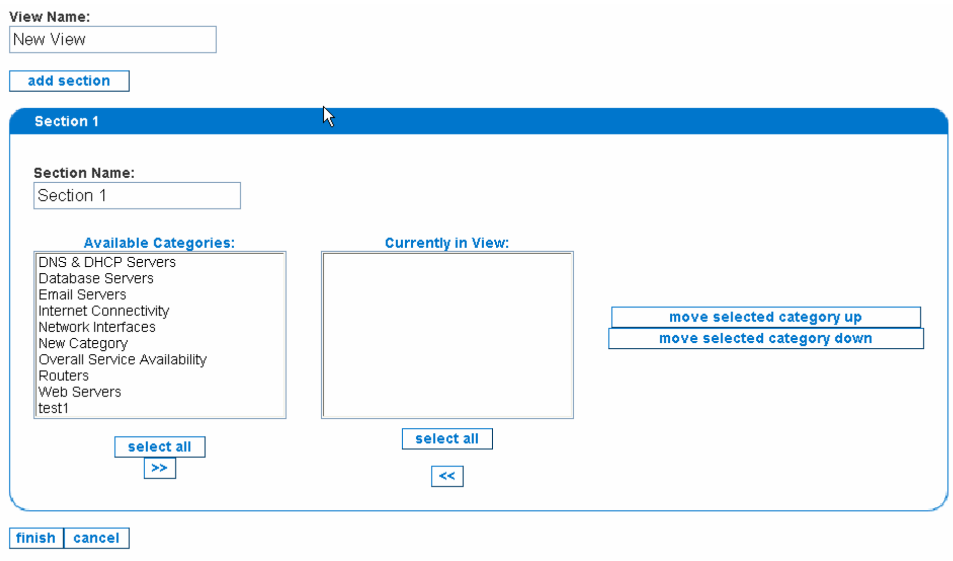
View	Default	Avail Report Default	rename button	modify button	delete button
New View1	make default	make default	rename	modify	delete
WebConsoleView	Default	Default	Read-only system view		

Figure 126 Configure Views

4. To select a default view for users who are not mapped to a view, click **make default** in the row of the desired view.
5. To select a default view for the Availability Report, click **make default** in the row of the desired view under the Avail Report Default column.
6. Click **rename**, **modify**, or **delete** to do any of these actions on the view. Clicking **modify** will display the same page when adding a new view.
7. To add a new view, click **add new view**.

Add/Modify an Existing View

In this page, you can add a new view or modify an existing one, including adding or removing sections, for example, logical groupings of categories under a common heading, as well as the categories within them. To create or modify the categories, including the filters that populate them, please see section **Configure Categories** earlier in this chapter for additional information.



View Name: New View

Section Name: Section 1

Available Categories:

- DNS & DHCP Servers
- Database Servers
- Email Servers
- Internet Connectivity
- Network Interfaces
- New Category
- Overall Service Availability
- Routers
- Web Servers
- test1

Currently in View:

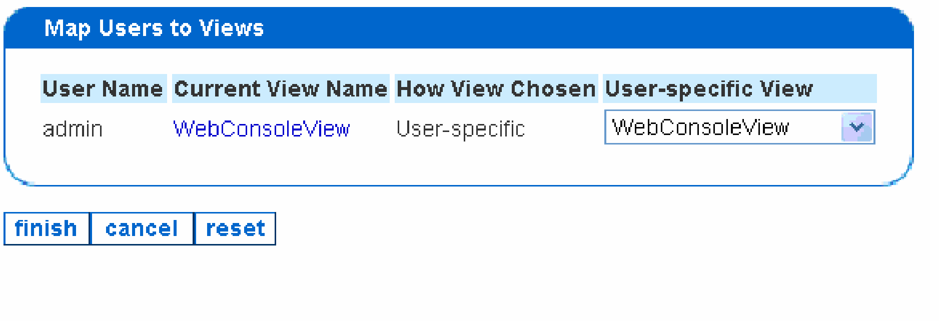
Figure 127 Add/Modify Views

1. To create a new view, type a new name.
2. Select the categories that will comprise the view by using >> and <<.
3. Organize the order in which the categories will be displayed by clicking **move selected category up** or **move selected category down**.
4. You can add a section by clicking **add section** to create a new grouping of categories. A view can comprise of one or more sections. This is optional.
5. Click **finish** to save your changes.

Map Users

After creating views, you can now map users to a view that will be displayed after they log into the CC-NOC. If users are not mapped to a specific view, then the Default view that was selected in section **Configure Views** will be displayed.

1. Click on the **Admin** tab in the top navigation bar.
2. Click **Category and View Configuration**.
3. Click **Configure Views**.
4. Click **map users**.



Map Users to Views

User Name	Current View Name	How View Chosen	User-specific View
admin	WebConsoleView	User-specific	WebConsoleView

Figure 128 Map users to views

5. Associate a view with a user by selecting the view from the pull-down menu.
6. Click **finish**.

Appendix A: Specifications

V1 Platform

General Specifications

Form Factor	1U
Dimensions (DxWxH)	24.21”x 19.09” x 1.75” 615mm x 485mm x 44mm
Weight	23.80lb (10.80kg)
Power	Single Supply (1 x 300 watt)
Operating Temperature	10℃- 35℃ (50℉- 95℉)
Mean Time Between Failure (MTBF)	36,354 hours
KVM Admin Port	(DB15 + PS2 or USB Keyboard/Mouse)
Serial Admin Port	DB9
Console Port	2 x USB 2.0 Ports

Hardware Specifications

Processor	AMD Opteron 146
Memory	2 GB
Network Interfaces	(2) 10/100/1000 Ethernet (RJ45)
Hard Disk & Controller	(2) 80-GB SATA @ 7200 rpm, RAID 1
CD/ROM Drive	DVD-ROM

Remote Connection

Modem	Not Applicable
Protocols	TCP/IP, UDP, RADIUS, LDAP, TACACS+, SNMP, SNTP, HTTP, HTTPS
Warranty	Two years with Advanced Replacement* Guardian Extended Warranty Also Available

Environmental Requirements

OPERATING	
Humidity	8% - 90% RH
Altitude	Operate properly at any altitude between 0 to 10,000 feet, storage 40,000 feet (Estimated)
Vibration	5-55-5 HZ, 0.38mm,1 minutes per cycle; 30 minutes for each axis(X,Y,Z)
Shock	N/A

NON-OPERATING	
Temperature	-40□ - +60□ (-40□-140□)
Humidity	5% - 95% RH
Altitude	Operate properly at any altitude between 0 to 10,000 feet, storage 40,000 feet (Estimated)
Vibration	5-55-5 HZ, 0.38mm,1 minutes per cycle; 30 minutes for each axis (X,Y,Z)
Shock	N/A

Electrical Specifications

INPUT	
Nominal Frequencies	50/60 Hz
Nominal Voltage Range	100/240 VAC
Maximum Current AC RMS	3A
AC Operating Range	100 to 240 VAC (+-10%), 50/60 Hz
OUTPUT	
+5 VDC, +12VDC	N/A
-5 VDC, -12VDC	N/A
Maximum DC Power Output	N/A
Maximum AC Power Consumption	Average Power Consumption: 249.7 – 250.8 Watts Max. Power Consumption: 250.8 Watts
Maximum Heat Dissipation	Average Heating Value: 214.74k – 215.69k cal Max. Heating Value: 215.69k cal
Volt-Ampere Rating	N/A

Appendix B: Troubleshooting

Raritan wants to be involved from the beginning of your deployment and throughout the entire lifetime of your use of Raritan products. We have identified the following as the three pillars on which the success of your deployment rests:

- Your network – Understanding and maintaining your network is key to success. This means understanding the technologies and equipment configurations that are deployed, as well as the technologies that the Raritan appliances employ to manage those devices.
- The Raritan products – The CC-NOC will be the centerpiece of your management platforms. Keeping it properly configured and integrated is key to success.
- Integration into the Raritan support structure – The Raritan support structure is here to make certain that your Raritan services are up to date and running smoothly. Leveraging the expertise of our staff is not only a benefit, but also a critical component of our mutual success.

We have placed these three pillars in this order because this is the order in which you are most concerned with them. Your network is always the most important. The Raritan products act as a foundation supporting the health of your network. As a foundation below the Raritan products, the Raritan support structure is there to keep the CC-NOC healthy.

Just as you would maintain a large building, we recommend keeping your foundations healthy. Therefore, we will present these pillars from the foundation up. If you first make certain that you can integrate into the Raritan support structure, we can help you in troubleshooting issues surrounding your CC-NOC. If you next make certain that your CC-NOC appliances are healthy, they will be the tools that help you heal your network.

The Raritan Support Structure

Raritan is here to support you. This is what sets Raritan apart from the vendors of other network management systems. You should, above all else, make certain that your Raritan services are installed such that you can take full advantage of this service. Here is what you will gain from our support structure:

- Automatic updates – We are constantly improving the Raritan services. If you are integrated into the Raritan support structure, we will provide these improvements to you immediately.

To integrate into the Raritan support structure, we ask only that you are aware of the following services and have an operational plan for utilizing them. In later sections of this chapter, see section **Raritan Support Structure**, we will provide details on how to maintain and troubleshoot these critical components.

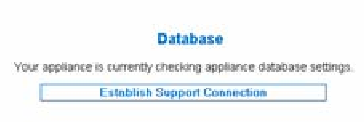
The CC-NOC's Ability to SSH to Raritan

The CC-NOC should be able to reach Raritan's central management servers. This is critical to downloading and installing updates and providing requested data back to Technical Support. These sessions, which only occur per user request, require that you allow the CC-NOC to SSH back to a secured facility and a disaster recovery site. The CC-NOC utilizes well-known protocols protected by industry-standard encryption for outbound communications.

Once a connection has been established, Technical Support can connect directly to the CC-NOC to diagnose or fix problems with the appliance. The connection is completely private and secure and uses industry-standard encryption schemes to encrypt all traffic to and from the appliance for the duration of the connection.

Checking Appliance Database Settings

From time to time, you may see this message:



Database

Your appliance is currently checking appliance database settings.

It is recommended you contact Technical Support, who can then request SSH access to your appliance. You can allow this access and open an SSH connection by clicking the **establish support connection** button. Opening the connection may take between 10 to 30 seconds. Your firewall must allow out-going connections from the CC-NOC on both port 22 (SSH) and port 443 (HTTPS).

Note: *Establishing the connection does not necessarily alert the support staff so it is still necessary for you to call or email Technical Support in the event of an issue that requires attention.*

RAID Array Failure

CC-NOC contains two hard disks in a RAID mirror array for increased data integrity. Notifications will appear (in the Event Browser and by email, if so configured) if there is an error in the mirrored data or with the array itself.

If the error is one of data integrity, CC-NOC will rebuild the RAID array to synchronize the data, with additional notification updates on its progress. If the error is with the array itself, CC-NOC will display one of the following messages:

- Degraded RAID Array
- RAID Array Failure
- RAID Array Dissapeared

These are critical errors and you should contact Raritan Tech Support immediately if they occur.

Important: If instructed to replace the hard disks in your CC-NOC appliance, the disk drives CANNOT be removed while the appliance is on. All Disk drive swaps must be done while the machine is powered off.

The CC-NOC Services

Understanding the CC-NOC will help you understand how to troubleshoot most issues. Here, we will give you an overview of how the CC-NOC and its core services function and interrelate. Each of these services will be covered in more detail in the following sections.

Discovery

The discovery service performs a daily scan of your managed IP addresses and address ranges. This is the first step towards polling a new device. Once per day, the discovery service will *ping* each IP address from your managed IP addresses and ranges. If a new IP address responds to pings, it will generate a new event inside the CC-NOC, notifying other services that a *suspect node* has been discovered. The "ping" utility relies on the ICMP protocol, specifically ICMP's ECHO (Code 8) and ECHO REPLY (Code 0) capabilities. You must allow both of these to pass between your CC-NOC and managed devices in order for discovery to recognize the node and generate the *suspect node* event.

Capability Scanning

The capability scanning service scans individual nodes to discover which services are supported on that node. It uses an intelligent service discovery mechanism and relies heavily upon communication over the TCP protocol (and sometimes UDP). In its initial state, the capability scanning service waits and listens for *suspect node* events. When a *suspect node* event occurs, it begins scanning the node. If it finds a new service, it will generate an event to notify the other services that a new service has been discovered. You will see these events as the first events associated with any given node.

In addition to responding to *suspect node* events, the capability scanning service runs once per day to check each existing node for new services. Additionally, a validated user within the CC-NOC's user interface can request a rescan of a device. The capability scanning daemon, whether during initial population of the database, during the daily scans, or during a forced rescan, will add any new services discovered to that node. However, it will **not** remove those services. Service removal is a function of the *pollers*.

Pollers

For monitoring the availability of individual services, the CC-NOC maintains a number of pollers (or polling services). When a poller runs, it performs an intelligent test against a service to confirm that it is responsive. The actual test varies from service to service, but most of the pollers rely heavily on TCP communications.

Pollers run on independent schedules, depending on the node and the service they are monitoring. The default for most pollers is to run every five minutes, unless an outage occurs. You can adjust the polling interval from the **Admin** page, but it is strongly advised that you consider the potential impact before making such a change. Adjusting polling intervals (they were initially set at 5 minutes after extensive testing), timeouts and/or retries without proper planning or forethought runs the risk of a) having the poller (s) get behind, b) adding unreasonable amounts of network traffic in the environment, and/or c) mis-diagnosis of outages (in the case of low retries).

If an outage occurs, the poller adjusts its scheduling to check much more frequently at first and then less often if the outage lasts for a long period of time.

In addition to running already scheduled pollers, a service constantly runs which listens for newly discovered services and schedules them for polling. Whenever a poller discovers an outage, it generates an event to let the other services (and the concerned users) know that the outage occurred.

Notifications

The notifications service listens to every event generated and (depending upon the configuration) notifies the concerned users. These notifications are performed via email or a paging server. This is one of the most critical services to maintain on the CC-NOC, because you will not be aware of outages unless the notifications are reaching you. The notifications service evaluates each event against the notifications rules you configured in the administrative interface. If it matches one or more rules, it will perform a notification and then schedule itself for the next escalation in the escalation path. If nobody has confirmed the notification before the scheduled time, it will notify the next person in the escalation.

The notifications service does not generate any events; it only reacts to them. It does, however, save its history in the database so that you can review past notifications.

SNMP Data Collection

The SNMP data collection service collects additional data from nodes that support SNMP. Just like the pollers, the SNMP data collection service runs every five minutes by default. If a scheduled device is available, it will collect as much information as it possibly can. This information is stored in a database so that you can run historic reports on it.

The SNMP data collection service will also look for exceptional conditions. If a given value exceeds a threshold or signifies an outage, it will generate an event. This event may (depending on your configuration) trigger a notification. The SNMP data collection service relies solely on the SNMP protocol, which works over TCP/IP.

Vulnerability Scanning

The vulnerability scanning service scans specified nodes to check for potential security vulnerabilities. It relies heavily on some very advanced features of each TCP and UDP service on your nodes.

The vulnerability scanning service runs upon request, scanning each specified node at the scanning level it was assigned to. If a vulnerability is discovered on a target system, it will be identified in the scan list and all relevant information available for that vulnerability will be listed.

Events, Historic Data, and Graphs

All events and historic data are stored or summarized in one or more databases. This is so that you can analyze the history of troubled network nodes or provide reports to demonstrate certain behaviors.

Note: *Systems management through WMI is an add-on component in the CC-NOC. The CC-NOC runs effectively without collecting WMI data—it is not required. WMI, however, provides to a good deal more information than the CC-NOC can obtain remotely.*

Some data is summarized over time to keep disk utilization consistent. Most of the data that is summarized will come from sources such as the SNMP data collection service or the System management sub-system.

Windows Management

The CC-NOC, through the use of a CC-NOC appliance and a configured proxy, collects information about Microsoft Windows systems (2000, 2003, and XP) that cannot be collected through other means (such as TCP, UDP, or SNMP). WMI is a special software program, developed by Microsoft, which runs silently on a Microsoft Windows machine and makes key data available to the CC-NOC.

The data collected by WMI is handled in much the same way as data from the SNMP data collection service. Most data is stored for historic purposes. If, however, an exceptional condition occurs, it will generate an event to notify the other services. This event may (depending upon the configuration) trigger a notification.

Your Network

Understanding and maintaining your network is the key to success. The Raritan services will help you understand and troubleshoot your network, as it relates to the CC-NOC. This chapter, however, is about troubleshooting the CC-NOC.

Raritan Support Structure

Before troubleshooting anything else, you should always make sure that your basic connectivity to the Raritan support structure is available should you need to utilize it. Maintaining these connections is the foundation to the health of your CC-NOC.

Contacting Raritan

The CC-NOC will attempt to contact the Raritan server(s) via SSH if you click **[establish support connection]** on the **Help** tab. You may be requested by Technical Support to establish this connection so we might help you diagnose certain issues.

To ease the administrative burden associated with this function, Raritan ships all CC-NOC appliances with the ability to attempt SSH connections on multiple ports. These ports map back directly to the list of protocols most commonly allowed out through firewalls:

- 22 – ssh
- 25 smtp
- 80 – http
- 443 – https

If any of these ports are open in a pure “any traffic outbound” mode, then our SSH connectivity will be successful. Our secured servers, to support this, run SSH daemons on each of these ports.

Discovery

To troubleshoot discovery, you must first understand when it runs and how it runs. The discovery service initially runs after the managed IP address ranges are configured. After that point, it will run once per day for the entire time that the CC-NOC is installed. It will continue to check your managed IP address ranges to see if any new devices have appeared on the network.

When you first configure your managed IP addresses, discovery may take a significant amount of time. This depends on how many addresses you are attempting to discover. A large network, with multiple class C devices can take as much as 24 hours to complete. Discovery runs as a low priority task to avoid flooding your network with discovery traffic. Since it is spaced out over time, the impact on your network will be nearly invisible.

For a device to be discovered, the CC-NOC must be able to PING the device. For ping to work, the CC-NOC must be allowed to send an ICMP ECHO (Code 8) to the device and must be able to receive an ICMP ECHO REPLY (Code 0) back from the device. These packets must route correctly between the CC-NOC and the devices. If any firewalls exist between the CC-NOC and the device, they must allow the ICMP ECHO to pass through to the device and must allow the ICMP ECHO REPLY to pass back to the CC-NOC.

To test whether or not ping should work, attach a computer to the same subnet as the CC-NOC. From that computer, open up a command line and type:

```
ping <ip address>
```

where `<ip address>` is the IP address of the device for which you are troubleshooting discovery.

If you are confident that the CC-NOC can ping the node in question, the next step is to confirm that the CC-NOC has discovered a device correctly. Check the following things:

If the ping was successful, the CC-NOC will generate a suspect node event. The text of the event will look like "A new node (hostname) was discovered."

The node status will be listed as "Active", if it has an interface within the current managed ranges. The node status can be found on the detail page for the node.

Once you have confirmed these things, you have confirmed that discovery was successful for the node in question.

Why Don't I See the Machine Name for my Windows 2000 Systems?

When resolving machine names for managed Win32 devices, Raritan leverages the CIFS protocol. This allows us to request, in Windows own language, a machine's *computer name.*

With the introduction of Windows 2000, it is possible to shut off a machine's ability to respond to these requests over TCP/IP. In these cases, it's merely a matter of configuration to re-enable this functionality, and once enabled, your network management appliance will correctly identify and resolve these names for you in the web user interface.

Here are the steps to enable *NetBIOS over TCP/IP* in Windows 2000:

1. Click on the *Start* menu.
2. Select on *Settings.*
3. Select Network and Dial-up Connections.
4. Right-click on Local Area Connection.
5. Select Properties.
6. Select Internet Protocol (TCP\IP).
7. Select *Properties* Select *Advanced* Select the *WINS* tab.
8. If *Enable NetBIOS Over TCP/IP* is not selected, select it and click *Ok.*
9. You may need to reboot.

Capability Scanning

The capability scanning service consists of two main functions:

- Scanning interfaces for known services
- Re-parenting interfaces under the correct node

The following sections provide details on how to troubleshoot these functions.

Scanning Interfaces

When the capability scanning service sees a “Suspect Node” event, it will begin scanning that node to discover which services it supports. After the initial scan is complete, it will repeat this scan once per day. You can also force the capability scanning service to rescan a device, by clicking the force rescan link on the **node detail** in the CC-NOC web user interface. Forcing a rescan is a very useful tool in troubleshooting the capability scanning service.

When the capability scanning service scans a node, it uses an *intelligent services scan.* This is different from a port scan, because it uses *synthetic transactions*. Synthetic transactions perform a much deeper check than simply connecting to a port via TCP and provide more accurate capabilities profiling. During an intelligent services scan, it will test the device for each of the services supported by your CC-NOC. A list of the supported services can found by clicking on the **Admin** tab, **Network Management**, and **Configure Pollers**. For each service that responds during the intelligent service scan, the system will generate a “Node Gained Service” event. The text of this event will look like the following:

The X service has been discovered on interface WWW.XXX.YYY.ZZZ

Typically, this will also be the signal to the Pollers that they should begin polling this new service for availability.

Re-Parenting

The capability scanning service is also responsible for *re -parenting.* Re-parenting occurs when two IP addresses are discovered to be part of the same node. This is common with network devices, for example, routers and switches. Some of your workstations and servers may also have multiple network adapters. During a routine scan, the capability scanning service can notice that these interfaces are related. If it does, it will re-parent them under the correct node.

Re-parenting will take place if one or more of the following happens:

- The SNMP table for a device lists both IP addresses as interfaces for the device.
- The NetBIOS node name for both IP addresses is the same

If re-parenting is not occurring correctly, you should check to see that the managed device is providing the necessary information. Depending on the type of device and the services it provides, you will need to check either the NetBIOS node names are resolving correctly or that the SNMP interfaces table contains both addresses. Details on each are provided below.

Do the NetBIOS Node Names Match?

To check that the NetBIOS node names match, you will need to do a reverse lookup on the IP Address, using NetBIOS name resolution. On a Windows 2000 system, you can use a command line utility called **nbtstat.** From the command line, type the following commands. Replace <ip1> with the address of the first interface and <ip2> with the address of the second interface:

```
nbtstat –A <ip1>
nbtstat –A <ip2>
```

For each command, you will see output that looks like the following. If the first line of each output matches, then you have confirmed that both interfaces resolve to the same NetBIOS node name:

Name		Type	Status
LARRY	<00>	UNIQUE	Registered
RARITAN	<00>	GROUP	Registered
LARRY	<03>	UNIQUE	Registered
LARRY	<20>	UNIQUE	Registered
RARITAN	<1E>	GROUP	Registered

Are Both IP Addresses in the SNMP Interfaces Table?

To check that both IP addresses are in the SNMP interfaces table, you will need to use a tool that allows you to query SNMP information from a remote host. First, run a query to retrieve the IP interfaces table. Next, check the table to confirm that both addresses are present.

For Microsoft Windows systems, we recommend the use of GetIF. See section **GetIF** later in this appendix for details.

Why Can’t My CC-NOC Manage X Service?

ICMP - If a device responds to a "ping", which uses ICMP for its transport, the device will be flagged as supporting ICMP and will be tested for ICMP availability on the standard polling interval.

Microsoft Exchange - If a device is determined to support Microsoft Exchange, it means that we have discovered email-related services (IMAP, POP3, or SMTP) on one of its interfaces, and the banner received from that service identified the server as Microsoft Exchange. The MSExchange service indicates that the CC-NOC was able to recognize that the server is Microsoft Exchange, but due to potential configurations of the server that could disable banners, we do not guarantee that all Microsoft Exchange servers will be identified as such.

Router - If a device is identified to support the "Router" service, it must first support either SNMP or SNMPv2, and it must respond positively to a query of the ip.ipForwarding OID. This service is not polled on a regular polling interval, but instead, is used to help maintain appropriate contextual displays in the CC-NOC's user interface.

SNMP/SNMPv2 - The CC-NOC will discover if a device supports SNMP version 2 (SNMPv2). SNMPv2 support implies that the devices supports the GET-BULK operator, which allows the CC-NOC to pull performance data from the device using a far more efficient query, reducing network overhead, and freeing up the CC-NOC to poll the next device in less time. **Note:** If a device supports both SNMP (which implies SNMP version 1) and SNMPv2, the CC-NOC will query the device with SNMPv2 only, as it's more efficient and there is no need to retrieve redundant data.

Pollers

The pollers decide what to poll by analyzing the interfaces and services in the database and comparing them to the Managed Ranges - if the interface is in the managed range, it will get polled, if it's not, it won't.

The complete list of pollers is available under the **Admin** tab, **Network Management**, and **Configure Pollers**. The Pollers use *synthetic transactions* to test, where possible. In essence, *synthetic transactions* communicate with the polled service, with minimal impact. For example, some pollers use banner grabbing. Some pollers interact more directly, for example, the HTTP service poller simulates the user viewing a URL from a browser. Other pollers use simple port connectivity to test, for example, telnet. All pollers are standards-compliant.

Some services are TCP based, for example, connection-oriented, and some are UDP based, for example, connectionless. An example of a TCP-based poller would be telnet – you will connect through port 21 and if that connection was successful, then you can assume the service is operating correctly (you will know almost immediately). An example of an UDP-based poller would be DNS - the poller generates a name query packet, and sends it out UDP to the server and simply has to wait for a response.

There are benefits and problems associated with not doing authentication as part of polls. Raritan does not use any authentication-based polling - instead, we exercise protocols. Yes, you can get more information by actually “logging in” to a service, but the security risks outweigh the benefits.

If a service "fails" a poll, a "Node Lost Service" event is generated. The text of that event looks like:

XXX outage identified on interface WWW.XXX.YYY.ZZZ

If a service successfully connects, but otherwise "fails", a "service unresponsive" event is generated. An example of this would be a poller sends a TCP connect request… and gets a connecting, but within the “timeout” period there is no response. Thus, the Service is “up”, but it is not performing up to an adequate level. This could be caused by the service itself, or through network congestion – but in either case, it is a condition that warrants investigation.

Notifications

There are two ways to configure notifications: Easy: Add members to groups

~ More difficult: Configure Notifications

The easy way works for most people, as the CC-NOC comes with a set of default notifications already created and all you have to do to use them is to create Users and add them to the default Groups. The options provided by the Notification Configuration link, found on the **Admin** page, are very powerful, but can become very time-consuming - as you have to create not only custom paths, but also new notifications. If you are creating either IP, single or Range, or service-based pollers, then you also need to take into account the built-in escalation that the CC-NOC will do, for example, Service -> Interface -> Node, and create multiple notifications. Notifications can be sent via:

- Email from the CC-NOC to email clients.
- Email from the CC-NOC to pager/mobile destinations.
- Via TAP from the CC-NOC to a paging system that supports TAP - TAP provides a dial-around mechanism, but is not universally supported.

When building new notifications, it is always prudent to create an outage to test your notifications, for example, pull a plug on a non-critical box. Also, test your emails to make sure that you are able to receive the notifications that you do generate. There is a **test SMTP settings** button on the **Outgoing Email Communications** page under the **Admin** tab, **Appliance Network Settings -** use it to verify that the email system is configured. You can easily change the configuration from this page to test. You can find more information about configuring notifications in **Chapter 6: Configuring Notifications**.

Also, take time to send notifications to pagers/phones, if applicable, and verify that there aren't messaging limits.

Why am I Not Receiving Notifications?

The most common reason that users don't get notified is that they have not been added as a member of a notification group. To receive notifications, you must be a member of the **Network/Systems, Windows Management, Security, Management, Admin, Reporting,** or “Customized” groups, or an individual user configured in a user-defined Notification Path. Assuming the default configuration, the standard notification process is defined below.

The **Network/Systems** group receives notifications related to the CC-NOC's polling subsystems (for example, Service Down, Interface Down, Node Down, etc.).

The **Windows Management** group receives notifications related to Windows Management. When important desktop events happen, including system faults and software installation/removal, email notifications are sent to members of this group.

The **Security** group receives notifications related to the CC-NOC Intrusion Detection subsystem (IDS), as well as any security-related concerns noted through vulnerability scanning, Windows Management, or SNMP trap receipt. When intrusion events are generated by the CC-NOC that meet the configuration requirements for generating notifications, these notifications are sent to members of the **Security** group. Please note that the **Security** group receives notifications all at once, as opposed to using the escalation system that the **Network/Systems** group leverages. This is due to the time-critical nature of security-related events.

The **Admin** group receives notifications for any events of concern to the appliance administrators.

The **Management** group receives notifications for any default notifications sent to the Network/Systems, Windows Management, or Security groups. Any notification sent to these groups is given, by default, a 15 minute window for acknowledgement.

The **Reporting** group receives the Availability and Outage reports via email every Monday morning.

What Conditions Cause a Notification to be Sent?

Notifications are sent when the CC-NOC notes that a service has experienced an outage. This will generate a pager notification to the **Network/Systems** group. When that service is restored, an email is sent confirming the service restored to the **Network/Systems** group. When a coldStart or warmStart SNMP trap is received, an Email notification is sent to the **Network/Systems** group. When an authenticationFailed trap is received at the CC-NOC, an Email notification is sent to the **Security** group.

When a new node is discovered, an email notification will be sent to the **Network/Systems** group. **Note:** Because many nodes are discovered in a relatively short period of time following the initial discovery process, **we highly recommend leaving Notices “Off” until the initial discovery process has completed.** Likewise, when a service has been down for an extended period (7 days, by default), that service will be deleted from the CC-NOC's polling lists. When this occurs, an email notification will be sent to the **Network/Systems** group. Also, if critical Node information has changed, the **Network/Systems** group will receive an Email notification.

Additionally, when the Windows management sub-system identifies a system fault or software installation/removal on a managed desktop, an email will be sent to the **Windows Management** group.

CC-NOC notifications are fully user-configurable.

SNMP Data Collection

A key feature that the CC-NOC provides is its ability to not only collect data via SNMP, but to do so automatically with sensible default configurations in place that will work for most deployments. However, to truly understand the benefit of all this, we first must step back and review some SNMP basics.

SNMP – What it is and What it Does

SNMP, or the Simple Network Management Protocol, was created to provide a rudimentary set of standards to allow hardware vendors to provide management information to external sources. What has evolved since then is one of the most convoluted schemes for sharing information ever contrived. SNMP has grown like a house that has had addition after addition built on, without ever consulting an architect. Despite its relative kludginess, it works and works fairly consistently despite some vendors’ implementations.

The basic architecture of SNMP includes two basic components: A manager and an agent. In our case, the CC-NOC is the manager and the managed device, for example, router, server, switch, etc., hosts the agent. The agent is merely a standardized interface that allows us to send specific requests and in return, receive specifically formatted replies.

SNMP version 1, which is the most commonly seen version deployed today, supports five basic transactions:

- GET
- SET
- GET RESPONSE
- GET NEXT, and
- TRAP

Of these five, Raritan only uses three:

- GET - A message sent from the Manager to the Agent requesting information
- GET RESPONSE – The message the Agent sends to the Manager in reply to a GET transaction, and
- TRAP – An unsolicited message from an Agent to the Manager advising the Manager of some abnormal condition

Of these three, only the first two are used in data collection.

When the CC-NOC discovers a device and the capabilities scanning daemon identifies that it supports SNMP, the CC-NOC then consults the SNMP Community String ranges, configured under the **Admin** page, to see what "Community String" to use. Community Strings in SNMP are very similar to passwords. The manager must query the agent with the correct Community String, or the request is denied. Unfortunately, the Community Strings are transmitted in plain text, so their use as a password is rather limited, but that's another story for another day…

Once the CC-NOC determines the appropriate Community String to use, which you can provide in either the CC-NOC **First-time Configuration Wizard,** or via the Edit the SNMP Ranges page under the **Admin** tab, **Network Management Configuration**, it will query the newly discovered device to determine what type of device it is. It does this by sending a request for the device's sysObjectID, a value that most SNMP agents will provide that uniquely identify the type of device that is hosting that agent. In the case of an NT Server, that sysObjectID might look something like:

.1.3.6.1.4.1.311.1.1.3.1

which when decoded, reveals an embedded series of qualifiers that look something like: .iso.org.dod.internet.private.enterprises.microsoft. software.systems.os.winnt

The details of how and why this works like this is well beyond the scope of this document, so at this point - just trust us. If you want more details, check out Marshall Rose's *The Simple Book,* or Mauro & Schmidt's *Essential SNMP*, which is available from O'Reilly.

So just as we have a mapping that points us to the kind of agent that is being queried, so also does that system have the ability to map specific data points for us. For example, on that NT server:

.1.3.6.1.4.1.311.1.1.3.1.1.1.1

maps to

.iso.org.dod.internet.private.enterprises.microsoft.software.systems.os.winnt.performance.
memory.availableBytes

Unfortunately, every vendor puts most of their data in unique places, each of which must be researched independently and added to the CC-NOC configuration. But the good news is that Raritan has already done that for you. And as new equipment is released or equipment is deployed that we haven't yet addressed, our support team is right on it. Don't be afraid to utilize our team! They are very good at what they do and can make you look like a hero, even if you don't know all the intricacies of SNMP.

Troubleshooting SNMP Data Collection

One handy thing about troubleshooting SNMP is that usually, it either works or it doesn't. And usually, the solution follows Occam's Razor—the simplest solution is usually the right one.

In most cases, if the CC-NOC is not collecting data from a particular device, it's usually because of a misconfiguration on the remote device. Often, incorrect community strings are the culprit, or the SNMP service has not been turned on or configured correctly.

There are several ways you can test the SNMP configuration for your devices:

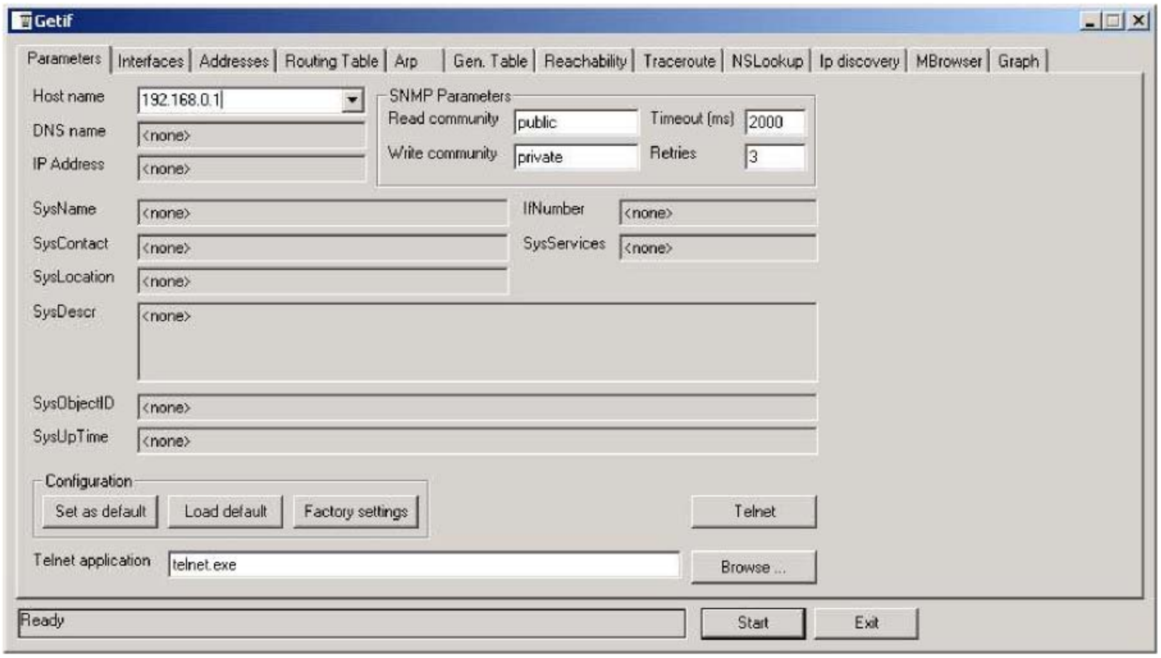
- Use the **SNMP Walk** tool on the Network Infrastructure Tools page from the **Tools** tab. This is the quickest and easiest method.
- Using a freeware utility, like GetIF. It is available at http://www.wtcs.org/snmp4tpc/getif.htm . This utility has some additional functionality, other than just confirming strings, and bears further discussion.

GetIF

The GetIF utility, which runs on Windows 2000/2003/XP, allows you to type in a hostname and a community string, click a button, and see if data is available from the agent. If data is available, it will not only pull it from the agent, but it will organize it very handily for troubleshooting purposes. A screen shot of GetIF that shows some of the examples used earlier:

The power of GetIF is in using it to minimally expose the ability the gather data. On the main panel, you have a series of fields that, if data is available, are automatically populated. In the case that they are, you know you have the correct community string and simply need to update the CC-NOC, if you can't get data, you know have a tool that can help you in the troubleshooting process.

A screenshot of that main panel:



Host name: 192.168.0.1
DNS name: <none>
IP Address: <none>
Read community: public
Write community: private
Timeout (ms): 2000
Retries: 3
SysName: <none>
IfNumber: <none>
SysContact: <none>
SysServices: <none>
SysLocation: <none>
SysDescr: <none>
SysObjectID: <none>
SysUpTime: <none>
Telnet application: telnet.exe
Ready

Be sure to add GetIF to your toolbox of network troubleshooting tools. It can also come in handy when troubleshooting some potential "re-parenting" problems in your environment as well. For example, if you click on GetIF's *Addresses* tab, you'll get a listing of the interfaces that the SNMP agent on that device knows about. This can be VERY handy when troubleshooting re-parenting problems. Armed with GetIF, you'll likely figure out a little more about SNMP and be able to provide additional information to us as you deploy new gear and new networking technologies.

Vulnerability Scanning

The vulnerability scanning service relies heavily on some very advanced features of the TCP and UDP services on your nodes. As a basic test, you should make certain that you could connect to the open services on the device before initiating a scan. This will at least verify that you can route from the CC-NOC to the device and that TCP and UDP are working. If you have already performed the troubleshooting steps for Pollers and Capability Scanning on the node in question, you have adequately tested this. If you are having trouble with vulnerability scanning, try the troubleshooting steps below:

1. If you are not getting vulnerability information, make sure that you set the scan parameters correctly in **Admin-> Vulnerability Scanning Configuration**.
2. If you are **only** getting open port information, make sure you have configured vulnerability scanning for at least Level 2 scans.
3. If you configured Level 3 and 4 to run, make sure you are not targeting mission critical devices before pressing the [perform scan now] button.
4. If you have devices that are being adversely impacted by vulnerability scanning, you can **exclude** them from scanning. Visit the **Admin-> Vulnerability Scanning Configuration** page and enter their IP addresses in the exclude list.

In addition to these troubleshooting steps, you can get overall vulnerability information from the **Vulnerabilities** tab. For details on vulnerabilities for specific nodes and interfaces, visit the node and interface pages.

Historic Data and Graphs

Troubleshooting historic data and graphs is usually more about understanding the calculations than it is about troubleshooting. If, after understanding the items in this section, you still believe that your data is incorrect, please contact Technical Support with as much information as you can provide, for example, sample reports, time of day, the values you expected, etc. Since most issues with reports are usually presented as a question, rather than a problem, each section in this chapter will cover a common question. In our next section, we will return to the normal troubleshooting format.

How is Performance Data Summarized?

Performance data is the best example of summarization. As data is collected, it is relevant in its most granular form only for a little while. Later, more broad generalizations, for example, averages, minimums, and maximums, are most important. For example, a router’s CPU performance is collected every 5 minutes. If you are looking to fix immediate problems, you might be interested in that 5-minute granularity, viewed over the last two hours. However, if you are looking for CPU performance trending and historical usage information, a view of that data over the period of one year to 6 months ago is probably more relevant, and for that view you don’t need 5-minute granularity. Raritan aggregates data once it reaches one month old, but archives it for a full year, making it available for these types of long-range reports.

How are Service Level Availabilities Calculated?

It's easiest to envision this number as number of successful polls divided by the number of attempted polls over the past 24 hours:

Successful polls over past 24 hours = SLA percentage Attempted polls over past 24 hours

The calculation is completed over a rolling 24 hour window, and the window size of 24-hours is not a user-configurable parameter.

Why isn’t SNMP Part of my Service Level Availability Calculations?

When development of the Raritan network management technologies began, a decision was made that the service level availability calculation should reflect the availability of services that can potentially impact the core business of the company. In most cases, the inability to poll for SNMP data is not integral to the core business of a company, thus it is excluded from the calculation.

SNMP, used for collection performance data for reporting, is still considered a service and as such, if a poll fails, it will still generate an outage that is integrated with the notification system.

To determine if an interface supports SNMP, check the appropriate Interface page for that node. To find the Interface page, search for the appropriate node by name or by TCP/IP address from the **Search** page, then click on the appropriate interface. The interfaces are represented as indented TCP/IP addresses under the header of the node's label.

How Do I Interpret the SNMP Graphs/Reports?

The traffic report in the SNMP performance graph will help you visually determine how much of your bandwidth you are using during a given period of time.

The traffic report is calculated with the following formula, and will display the percentage of bandwidth utilization:

(((inOctets+outOctets)*8bits)/Interface Speed))*100

The traffic report graph indicates maximum, minimum and average usage during the graphed timeframe. The units on these are very important:

x = x percent utilized

x m = x thousandths of a percent (divide by 1000 to get percentage)

x µ = x 10 thousandths of a percent (divide by 10000 to get percentage)

Additional Support

For additional support, you can contact Technical Support. We are here to help you. In addition to our support team, we have discussed a few tools and resources within this guide. Details on obtaining these resources are below.

The Tools Discussed in this Chapter

GetIF – GetIF is a freeware tool developed by Philippe Simonet. You can download it at: http://www.wtcs.org/snmp4tpc/getif.htm

Ping – ping is a command line utility that comes with most operating systems, including all variants of Microsoft Windows. Some network troubleshooting programs also include their own ping utilities.

Telnet – many telnet clients exist, tailored for different purposes. If you have a Microsoft Windows system, the one included is sufficient for troubleshooting. Most Unix variants also include telnet in their default installation.

NBTstat – nbtstat is available only on Microsoft Windows. It is a command line tool for querying the status of systems available via NetBIOS, which is a Microsoft proprietary networking protocol.

Documentation

Our documentation is available from the CC-NOC, under the **Help** tab, and is also available on http://www.raritan.com/support.

How do I get Help?

- See the Raritan web site for more information
- If you are an end-user, please contact your reseller.

- If you are a reseller seeking technical resources, please send an email to tech@raritan.com.
- For technical support, call the number as stated in the front of this document. Note that Technical Support is intended to provide resellers and customers with technical assistance if necessary. All callers will be asked to provide their reseller or customer number before any questions can be answered.

Appendix C: Performance Monitoring

Overview

The CC-NOC is designed to provide you with the information necessary to support critical decisions in your environment. Depending on your role, the nature of those decisions may be different, from a help desk technician analyzing memory usage on a CC-NOC to determine if upgrades are appropriate, to a network designer using router buffer failures in support of better sizing decisions in equipment acquisition.

In Raritan's quest to provide the right information to the right people with as little administrative overhead as possible, we have worked with vendors and industry professionals to identify the key metrics available that best support critical decisions. This document identifies those key metrics, how the CC-NOC gathers them, and helps to provide an understanding of how they might be used.

SNMP Data Collection

Leveraging SNMP, the CC-NOC has access to a wealth of information on devices of varying types. This information can vary from network performance information to system component utilization, for example, CPU, Memory, drives, etc., to very specific metrics that are critical for very specific reasons.

The CC-NOC, upon discovering that a device supports SNMP, determines whether the device supports SNMPv1 and/or SNMPv2. SNMPv2 introduced several mechanisms for making data collection more efficient, and if the device supports it, we will opt for the most effective means of collecting data. Once done, the device type is determined. This device type indicator allows the CC-NOC to determine which specific data collections should be put into place for this device. For example, if the device is a Windows NT server, the CC-NOC recognizes this and gets both Windows-specific information as well as MIB2 standard information related to network traffic on the interface. If that server is also running Checkpoint software or the Compaq Insight agent, data metrics will be harvested from those sources as well.

The chart on the following pages identifies the current set of performance metrics collected and their importance. Remember, all metrics are additive, so for example, a Windows device that support RFC1213 will share both Windows-specific metrics, as well as those supported by MIB2.

Note: SNMP data collections require that the managed device supports SNMP and that the CC-NOC has been configured with the appropriate community string. In many cases, adding SNMP support is merely a case of device configuration. In other cases, it means that software may need to be loaded onto the platform. Please consult the documentation for your network equipment and/or servers for more information on SNMP support.

Equipment Vendor	Device Type	Metric(s)	Relevance
All	Any device supporting MIB2 (RF 1213)	In/Out Octets In/Out Discards In/Out Errors	Provides basic information on the network traffic that an interface has transmitted/received.
All	Linux or Unix variants running Net-SNMP	Drive Size & Utilization (1)System Uptime Number of current users Number of processes Total memorySystem load average for 1, 5, and 15 minute intervals	Provides overall health of system and indicates if crucial resources are being taxed.
Microsoft	Windows	CPU Utilization Drive Size & Utilization (C:) Drive Size & Utilization (D:)	Provides insight as to processor scalability and drive usage
Novell	NetWare	CPU Utilization Number of NLMs loadedTotal Memory Cache Buffer Size & Utilization Memory Size & Utilization Current Open Files Current connections Free drive space on SYS Freeable space on SYS Free drive space on VOL2 Freeable space on VOL2	Provides deep insight as to server health and performance. Critical metrics to support sizing and performance decisions include CPU Utilization, Number of NLMs loaded, Cache Buffer Size & Utilization, Memory Size & Utilization, Current Open Files, Current connections, and Free space on SYS

Checkpoint	Firewall products	State information stored Process Contexts Allocated storage CPU Utilization Packets accepted Packets rejected Packets dropped Packets logged	This information is critical for the firewall administrator making sizing or upgrade decisions on firewalls. A device that must maintain both high network speed and low latency is critically impacted by CPU utilization, State information stored, and Packets dropped
Lotus (IBM)	Domino/Notes Servers	Current users Maximum users Dead Mail Delivered Mail Transferred Mail Waiting Mail Messages waiting for delivery Average mail delivery time Average mail size delivered Mail transmission failures Replication failures Average transactions/minute Total calendar users Total Appointment Reservations Allocated memory Free memory Free drive space (1 st drive) Free drive space (2nd drive)	The Domino metrics provide a comprehensive suite of all information that a Notes administrator needs to diagnose performance related problems, as well as general server functionality concerns. Sizing, scaling, and licensing can also be addressed using this data.
Compaq	Insight Agent	Drive Utilization (1st drive) Drive Utilization (2nd drive) CPU Utilization	These data points are often used to augment other data sources, or to verify other sources for the same.

Cisco	Network gear	CPU Utilization Free Memory Buffer failures Buffer memory allocation failures	Provides insight as to router sizing and performance, especially as augmented by MIB2 data.
Bay/Wellfleet	Routers/Switches	Total kernel tasks Total kernel tasks in queue Free memory Free buffers	Provides key sizing data, especially in concerning the system demands to CPU capabilities comparison
3Com	Routers/Switches	Total memory CPU Utilization Buffer memory available Buffer allocation failures Buffer memory total Buffer memory total available	These statistics provide an overview of the device's performance, as well as the device's ability to handle its current traffic load

SNMP Data Collection Enhancements

As a standard part of the Raritan service offering, data collection enhancements are regularly rolled into the core product offering at no additional charge beyond the base CC-NOC subscription rate. Additionally, we work very closely with our customer and reseller base to identify a logical priority for new collections. If your equipment is currently unaddressed, or you feel should be addressed differently, please let us know at Technical Support.

Windows Performance Metrics

Windows monitoring has been re-engineered from the ground-up to better allow Raritan to enhance the core feature set on a more regular basis. One of the key enhancements of the CC-NOC includes better and more appropriately targeted performance metrics, gleaned from more reliable system locations on differing platforms. The CC-NOC, through the use of CC-NOC appliances, collects the performance metrics from managed systems, 25 Servers and 5 "promoted" Workstations, and then presents the data for viewing and archival. All Windows metrics are saved in five-minute granularity for one month and then aggregated to one-hour granularity and stored for a year. The following table reflects the performance metrics gathered by the CC-NOC from various platforms.

Measured Component	**Metric**	**Relevance & Notes**
Memory	Available bytes Percent Free Physical Memory Percent Free Logical Memory Total Physical Memory Physical Memory In Use Percent Physical	These data points provide a collective overview of how memory is being handled on the platform. Per Microsoft, these data points are the critical pieces necessary to formulate a stance on OS performance regarding memory usage and potential "thrashing" that may occur on

	Memory In Use Free Physical Memory Total Logical Memory Logical Memory In Use Percent Logical Memory In Use Free Logical Memory Memory Pages per Second[1]	underpowered devices.
Processor (CPU)	Total Processor Time Processor Queue Length[1] Interrupts per Second[1]	Microsoft summarizes the usage of all processors (for SMP systems) into a single statistic. This indicates the Platforms overall ability to handle the workload.
Network	Network Utilization[1] Bytes Sent per Second[1] Bytes Received per Second[1] Packet Receive Errors[1] Packet Transmit Errors[1] Output Queue Length[1]	Microsoft's implementation of networking for Windows 98 and ME does not provide any statistics. This is a known problem identified by Microsoft. Windows NT requires that the SNMP service be loaded and running, however, we interface with that service at the system level, not via the SNMP protocol.
Logical Drives	Free Space Free Kilobytes Total Kilobytes Kilobytes In Use	This information is reported on a per partition basis, and maps directly to logical drives (for example, C:, D:, E:), not to physical drives. The information is reported for every local logical drive.

[1] Not available on Windows 98 or Millenium Edition

Leveraging Performance Data in Network Management

The keys to successfully gathering and using performance data are straightforward:

- Gather appropriate information
- Display it so it can be readily recognized and acted upon Act on it when appropriate

Determining what data to gather with Raritan is easy—our experts have already culled through the available information and are only presenting the pieces you need. Raritan's graphical display of this information is also easy to navigate and understand, yet powerful enough to be customized on demand. The remaining item is determining when performance metrics have reached a point at which they should be acted upon. And with the CC-NOC's capability of managing performance thresholds, that's easy too!

Thresholding

An exciting new feature significantly improved with the CC-NOC is threshold alerts. This allows the CC-NOC to notify you of potential problems pro-actively, before they occur, based on performance metrics gathered by the CC-NOC through SNMP and WMI.

How it works

The CC-NOC gathers performance data directly from managed devices using SNMP, and through a proxy system for Windows Servers, and 5 workstations, using a CC-NOC appliance. Each time the data is collected or reported, the CC-NOC compares certain data points against configurable *threshold* values. Click the **Admin** tab, **Network Management**, **Configure Performance Thresholds** for details on how to configure thresholds. If the value is higher or lower, depending on the type of threshold, than the threshold value, an event will be generated. This event can be configured for notification through the notification configuration option under the **Admin** tab.

There are four key pieces to threshold monitoring: type, value, trigger, and rearm.

Type

A threshold can be a high or low threshold. A high threshold means that an event will be generated if the actual value is higher than the threshold value. Conversely, a low threshold will cause an event to be generated when the actual value reported is lower than the threshold value.

Value

Value refers to the point at which the threshold is exceeded, whether it is a low or high threshold. For instance, if the value for a high threshold is 80, any reported value over 80 will exceed the threshold.

Trigger

The trigger is the number of times in a row the threshold must be exceeded before an event is generated. If a trigger is set at 3, for example, the threshold must be exceeded for three consecutive reports before an event is generated.

Rearm

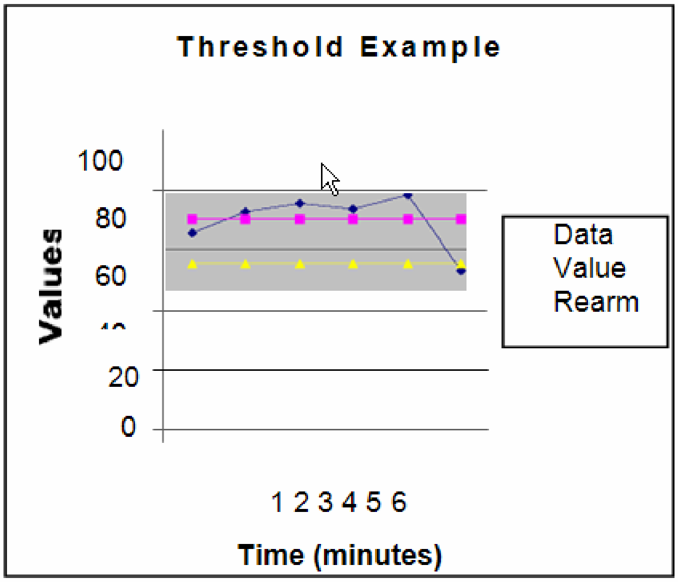
After an event is generated, no further events will be generated for the same threshold until the rearm value is reached. The rearm value protects you from a flurry of events when the value bounces *around* the threshold value—just above and just below. The rearm value must be reached in the *opposite* direction of the threshold type. For example, if a disk drive had a high threshold of 90% utilization and no rearm value, an application that wrote a temporary file and deleted it on exit might cause the utilization to bounce between 89% and 90%. The rearm value protects you from this condition by enforcing that the utilization problem must be addressed, as opposed to temporarily repaired. Until the utilization drops below 80%, you will not receive another notification.

Example

Here's an example. There is a high threshold set with a value of 70, a trigger of 3, and a rearm of 55. A new value is generated every minute. The first reported value is 65, which is less than our high threshold of 70, so no action is taken. The next poll is 72. This is above 70, so the trigger is checked. As this is the first time the threshold was exceeded, a trigger counter is started, but no further action is taken. The next two polls are 75 and 73, respectively. As each poll is over 70, the triggers are checked and the last poll satisfies the trigger requirements. At this point an event is generated.

The next reported value is 78. Since an event has been generated, and the reported values have not fallen below the rearm value of 55, no action is taken. Eventually, the reported value is 53. This is below the rearm value, so the threshold is active again. The next time the reported value exceeds 70 three times in a row, another event will be generated.

Here is a graphical representation of this example. An event would be generated at minute 4 (3 reported values over 70) and rearmed at minute 6.

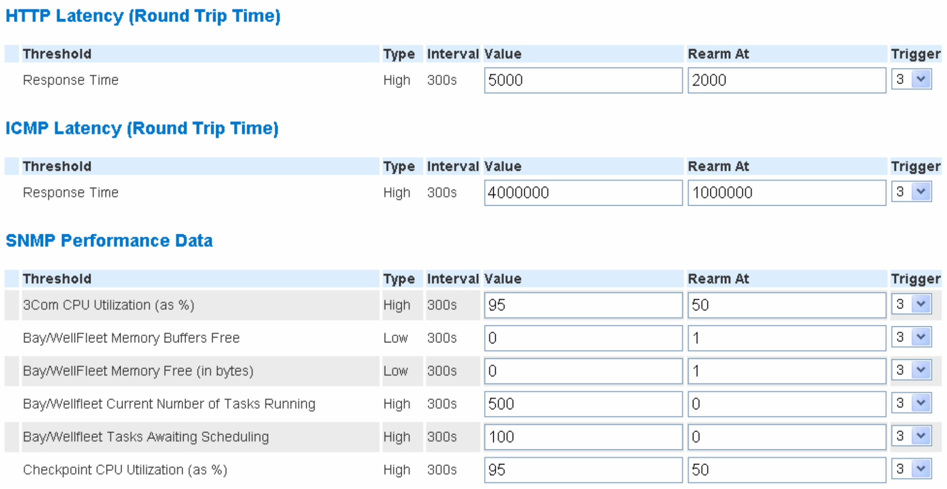


SNMP Performance Metric Thresholds

These values apply to data gathered through SNMP polling. The event associated with an SNMP value violating a threshold is "High Threshold Exceeded" for a High threshold type, and "Low Threshold Exceeded" for a low threshold type.

These thresholds are the default values, but are user-customizable.

Raritan is continually adding SNMP data collection definitions for new devices. As new devices are configured, appropriate thresholds will be added as well. If you have equipment for which you would like to have data collections defined or thresholds configured, please contact Raritan support at tech@raritan.com.



HTTP Latency (Round Trip Time)

Threshold	Type	Interval	Value	Rearm At	Trigger
Response Time	High	300s	5000	2000	3

ICMP Latency (Round Trip Time)

Threshold	Type	Interval	Value	Rearm At	Trigger
Response Time	High	300s	4000000	1000000	3

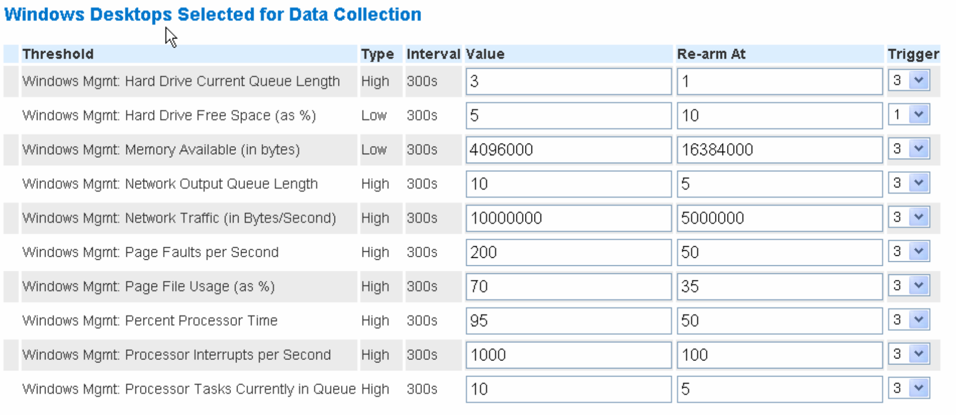
SNMP Performance Data

Threshold	Type	Interval	Value	Rearm At	Trigger
3Com CPU Utilization (as %)	High	300s	95	50	3
Bay/WellFleet Memory Buffers Free	Low	300s	0	1	3
Bay/WellFleet Memory Free (in bytes)	Low	300s	0	1	3
Bay/Wellfleet Current Number of Tasks Running	High	300s	500	0	3
Bay/Wellfleet Tasks Awaiting Scheduling	High	300s	100	0	3
Checkpoint CPU Utilization (as %)	High	300s	95	50	3

Windows Performance Metric Thresholds

The following values apply to data reported by Windows boxes. Note that there are separate events for Workstations and Servers – this is due to what data points Microsoft reveals. The event associated with a reported value violating a threshold is "High Threshold Exceeded" for a High threshold type and "Low Threshold Exceeded" for a low threshold type.

Note that all threshold defaults are set conservatively, to avoid the possibility of overwhelming operators with notifications related to transient conditions. If you do decide to change any of the values, do so only with a clear evidence of need and thorough testing.



Windows Desktops Selected for Data Collection

Threshold	Type	Interval	Value	Re-arm At	Trigger
Windows Mgmt: Hard Drive Current Queue Length	High	300s	3	1	3
Windows Mgmt: Hard Drive Free Space (as %)	Low	300s	5	10	1
Windows Mgmt: Memory Available (in bytes)	Low	300s	4096000	16384000	3
Windows Mgmt: Network Output Queue Length	High	300s	10	5	3
Windows Mgmt: Network Traffic (in Bytes/Second)	High	300s	10000000	5000000	3
Windows Mgmt: Page Faults per Second	High	300s	200	50	3
Windows Mgmt: Page File Usage (as %)	High	300s	70	35	3
Windows Mgmt: Percent Processor Time	High	300s	95	50	3
Windows Mgmt: Processor Interrupts per Second	High	300s	1000	100	3
Windows Mgmt: Processor Tasks Currently in Queue	High	300s	10	5	3

Appendix D: Setting up WMI on Target Machines

Configuring a Windows 98/ME box for Remote WMI Management

The ability of the CC-NOC to manage Windows 98 and Windows ME systems is limited by the design of the Windows platform. Windows 98 and ME are consumer operating systems and are not as feature rich as the Microsoft systems based upon Windows NT. As a result, the management information available from any Windows 98 or ME system will be a subset of the information available from NT based systems.

By default, Windows ME comes with WMI installed, but it is disabled. Windows 98 does not come with the WMI agent, but it is available from Microsoft. Due to license restrictions, Raritan Computer cannot redistribute the WMI agent software. To download a copy of the Windows agent software, use the following link:

http://msdn.microsoft.com/library/default.asp?url=/downloads/list/wmi.asp

On the page from the link above, click the link titled **Windows Management Instrumentation (WMI) Core 1.5**. Once the agent is downloaded and installed on Windows 98, the procedure is the same for both Windows ME and 98.

For more information, refer to the following MSDN knowledge base article:
http://support.microsoft.com/default.aspx?scid=kb;en-us;322363

The page provides good information on Win98, Win98 Second Edition, and Windows ME. A link is available there to download the WMI agent for Windows 98.

Once you confirm the Windows agent software is present on the box, configure the Windows 98/ME box for remote WMI management as follows:

1. Use the registry editor (regedit.exe) and navigate to the following locations and edit/create the necessary keys:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLE
   EnableDCOM (Type REG_SZ) = "Y"
   EnableRemoteConnect (Type REG_SZ) = "Y"

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\wbem\cimom
   AutostartWin9x (Type REG_SZ) = "2"

2. Add the program `c:\windows\system\wbem\winmgmt.exe` to the startup folder so that the program runs when a user logs in.

3. Add the machine to the domain using the control panel, network settings by doing the following:

- Start->Settings->Control Panel->Network.
- Select Client for Microsoft Networks from the tab.
- Click on the tab named **Properties**.
- Check the box for **Log on to Windows NT Domain** and specify the domain name.
- Click **OK** to save the network settings.

4. Configure User level access to the system using the network control as follows:

- Start->Settings->Control Panel->Network.
- Select User-level access control from the Access Control tab.
- Specify the domain name in the entry field.
- Click **OK** to save the new settings.

5. Specify access to the WMI namespaces by running the WMI control application `c:\windows\system\wbem\wbemcntl.exe` by using these steps:

- Select in the folder menu of the Security tab Root->**CIMv2**.
- Click Security.
- Add the user names for access in the form **DOMAIN\USER**. For example, **RARITAN\Administrator**.
- Select all permission boxes to enable full permission to the agent for the new user.
- Click **OK** to save the permissions.

6. Repeat for the namespace **Root-default**.

Configuring a Windows Proxy Details

WMI, also known as WBEM, is Microsoft's technology for providing a consistent systems management interface to their platform. In many respects is it very similar to the well-known and venerable SNMP agent that exists on many platforms. However, instead of data being accessed via obscure numeric strings and often arranged into tabular views, WMI uses an object hierarchy based upon CIM.

CIM (Common Information Model) is a standard defined by the DMTF (Desktop Management Task Force). CIM is targeted at being an object-oriented repository of information for management data. Microsoft took the idea of CIM, wrote an agent, and dubbed the system WMI. The DMTF didn't define a protocol up front like SNMP for the exchange of information between management applications and agents. Thus Microsoft chose to implement the information exchange using DCOM (Distributed Component Object Model).

In order for the CC-NOC to be able to communicate with a network of Windows systems, it needs to have at least one system to act as a proxy. The reasons have to do with low-level details in the implementation of the WMI system and its COM objects. By default, only local processes on a Windows box may access the WMI objects that leaves network based COM system with a method to communication.

Microsoft has provided a workaround to this shortcoming of in process COM servers in the form of a program called 'DLLHOST.EXE'. This program can act as a surrogate process loading the in process COM server and making it available to the network. To do this, a system must be prepared. The preparations are relatively simple and only involve modifications to the system registry for either a Windows 2k Pro or XP Pro system.

Note: *Using Windows 98/ME, XP Home, or any NT 4.0 system is not recommended or supported as a proxy system. Additionally, although Servers are supported, it is not advisable to utilize them as your proxy due to error logging issues.*

To enable a Windows proxy system for the CC-NOC, Raritan provides a binary that can be downloaded and run. The binary tweaks the registry to enable remote communications with the WMI scripting system on the local box.

Running the binary with –u option reverses the changes to the system. Below is the detailed list of changes to the system registry. It as strongly advised that you NEVER modify the registry without serious consideration to the ill effects it can have. User modifications to the Windows registry can result in unstable and/or unusable systems.

Registry Changes [configuration]:

This is a list of the changes that will be made to the system registry by the binary provided by Raritan.

Note: *HKCR is short for HKEY_CLASSES_ROOT. All values are of type REG_SZ (strings).*

HKCR\AppID: (key, value)

/* Wbem Scripting Object Path */

SetValue: HKCR\AppID\{172BDDF8-CEEA-11D1-8B05-00600806D9B6}\(Default), ""
SetValue: HKCR\AppID\{172BDDF8-CEEA-11D1-8B05-00600806D9B6}\DllSurrogate, ""

CLSID:

/* Wbem Scripting Object Path */

SetValue: HKCR\CLSID\{172BDDF8-CEEA-11D1-8B05-00600806D9B6}\AppId, "{ 172BDDF8-CEEA-11D1-8B05-00600806D9B6}"

/* WBEM Scripting Object Path */

SetValue: HKCR\CLSID\{5791BC26-CE9C-11D1-97BF-0000F81E849C}\AppId, "{ 172BDDF8-CEEA-11D1-8B05-00600806D9B6}"

/* WBEM Scripting Sink */

SetValue: HKCR\CLSID\{75718C9A-F029-11D1-A1AC-00C04FB6C223}\AppId, "{ 172BDDF8-CEEA-11D1-8B05-00600806D9B6}"

/* WBEM Scripting Locator */

SetValue: HKCR\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}\AppId, "{ 172BDDF8-CEEA-11D1-8B05-00600806D9B6}"

/* WBEM Scripting Named Value Collection */

SetValue: HKCR\CLSID\{9AED384E-CE8B-11D1-8B05-00600806D9B6}\AppId, "{ 172BDDF8-CEEA-11D1-8B05-00600806D9B6}"

/* Wbem Scripting Last Error */

SetValue: HKCR\CLSID\{C2FEEEAC-CFCD-11D1-8B05-00600806D9B6}\AppId, "{ 172BDDF8-CEEA-11D1-8B05-00600806D9B6}"

Appendix E: Managing and Responding to Intrusion Detection Events

This appendix is intended to provide a little insight as to how Raritan goes about assessing the traffic that the CC-NOC sees, determining what constitutes an *event,* and in turn, what that event should mean to you.

How the Intrusion Detection works

The CC-NOC can act as a network-based intrusion detection system (NIDS), listening to network traffic and indicating when certain behaviors are identified, traffic patterns appear, or recognized character strings are passed. This provides an easy-to-deploy and technically sound approach to analyzing your traffic for things that probably shouldn't be there.

Raritan's team of security experts is constantly monitoring security-related news sources, as well as doing internal testing and analysis, ferreting out information related to the latest hacker threats and system vulnerabilities. Once identified, these threats and vulnerabilities are distilled down to their simplest form—the network traffic they generate. Armed with this information, our team creates a series of "signatures" that uniquely, or as uniquely as possible, identify those threats that could be encountered in your network. However, because it's impossible to say that a specific behavior, traffic pattern, or character string could be associated only with malicious traffic, there are times that the CC-NOC will trigger an event not associated with an actual threat. These situations are referred to as *false positives,* and are inevitable in the world of intrusion detection. Raritan falls on the side of "better safe than sorry", and would rather give you the information to disprove, then to let a hacker have his way. And we're not alone—this approach is considered by many to be an industry best practice. But too many false positives is not good either, so Raritan has taken great strides to help you reduce them in your environment by leveraging the information you have about your IT infrastructure.

Reducing False Positives with the Signature Profiler

Because Raritan provides signature files for your CC-NOC as part of our Advanced Administration options, you needn't worry about keeping up to date on all of the latest threats – we will do the investigation and make the new signatures available. But no two networks are alike, we must provide all of the available signatures to each of our CC-NOCs that are in the field. This means that every CC-NOC has a copy of every signature that we distribute. And in many cases, not all of these signatures are necessary for the environment in which the CC-NOC is installed. For example, one of our signatures watches for traffic attempting to exploit the ToolTalk database server on Sun Solaris platforms. And by default, if we see the traffic that indicates this particular threat, we will notify you—even if you don't have any Sun Solaris platforms running the ToolTalk database server. This is specifically why we've built the Signature Profiler.

The Signature Profiler is a way for you to deploy an CC-NOC with customizations for its environment once, and our rules engine will maintain those customizations for you as new signatures and features are rolled out. How does it work? Good question!

Signature Profiler and the Rules Engine

The Signature Profiler provides an easy-to-use, web-based interface that asks simple questions: Are you running this platform or that? What platforms do you use for email? Web services? What kinds of routers do you use? By simply moving through the web page and checking or un-checking the boxes that correspond to your configuration, you are building the rules necessary to keep the CC-NOC up-to-date. Once complete, the Rules Engine makes decisions on your behalf as to whether or not new signatures should be applied to a given CC-NOC. This reduces your workload, while automating the most difficult part of intrusion detection—keeping it up-to-date.

Responding to Events and Notifications

Once you've used the Signature Profiler to build a model of your network and systems infrastructure, your CC-NOC is now ready to start generating events and notifications. Now the question becomes "What events/notifications will I receive, and what will I do with them once I've got them?"

Event Categories

- Successful Administrator Privilege Gain: This category includes threats in which the traffic indicates that an attempt to compromise the security on a system at an administrator level has occurred, and that attempt was successful.
- Attempted Administrator Privilege Gain: This category includes threats in which an attempt to compromise the system security at an administrator level has occurred, but there are no indications as to whether or not the attempt succeeded.
- Successful User Privilege Gain: This category includes attempts to compromise
- systems at a user level, and the traffic indicates that this attempt was successful.
- Attempted User Privilege Gain: This category includes attempts to compromise
- systems at a user level, with no indication as to whether or not the attack succeeded.
- Unsuccessful User Privilege Gain: This category includes attempts to compromise
- systems at a user level that have failed.
- Denial of Service: This category identifies traffic patterns designed to disable a service or user access to a machine through excessive network traffic or system exploits.
- Attempted Denial of Service: This category identifies attempts to generate the traffic or exploits necessary to create a denial of service attack.
- Large Scale Information Leak: This category includes attacks in which the loss of system or environmental information across a number of nodes was incurred, including access to password lists or user information. This is significant, as these types of attacks usually precede more in-depth and destructive attacks.
- Information Leak: This category includes attacks where some system information is compromised which could aid in future attacks.
- Attempted Information Leak: This category includes attacks that indicate an attempt to
- gather information about systems or users that could aid in future, larger scale attacks.
- Potentially Bad Traffic: This category includes any traffic that may be normal in the
- course of business, but is likely to be traffic that really should not occur.
- Unknown traffic: This category includes traffic recognized as abnormal, but that is not associated with a known attack or intrusion. Events from this category are ignored by default.
- Normal traffic: This category includes traffic that doesn't fit into any other categories, because it hasn't triggered a signature, and is really useful only for troubleshooting the CC-NOC. Events from this category are ignored by default.

What do I do when...

The CC-NOC's job is to inform when you and your infrastructure are potentially at risk, and the decision as to how to respond is left to you—the one with the understanding of your infrastructure and your business. While we cannot provide a list of how to respond to each particular potential threat, we can share this list of things to consider when receiving events and notifications from your CC-NOC:

- Does this event mean that traffic is coming through my firewall that shouldn't be? Can I further refine my firewall configuration to disallow this type of traffic? What about traffic to/from this source/destination address?

- Are all of your systems at the most recent revision of operating system and patch
- level? Patches and hot-fixes are extremely important for Microsoft platforms.
- Have my network platforms been upgraded to avoid unnecessary risks? SNMP, if
- leaked to the outside world, can be a troublesome protocol.
- Have I used the Signature Profiler to tune the CC-NOC to watch for the traffic I'm really concerned about? The Signature Profiler is available under the **Admin** menu on your CC-NOC. Click the Configure Intrusion Detection link.
- Have I drilled down into the detail view of the event and checked the other sources for information? CVE, Bugtraq, Whitehats, and Raritan are all reliable, trusted sources for information on security threats.
- Has someone installed something on my network that I'm not aware of? This might include new applications as well as new systems or network gear.
- Is this event or notification part of a category that I'm not interested in? Can I review my CC-NOC event configuration details, on the CC-NOC: **Admin** tab under **Intrusion Detection Configuration**, and not receive these events/notifications in the future?
- Is this a false positive? Have I checked out this potential threat and am confident that this is not a risk?

What if I have been hacked?

Unfortunately, there's not often much you can do to react gracefully to a successful intrusion event—the important thing is to react quickly.

Depending on the nature of your business, the type of attack and possible loss involved, and the potential for further loss, your reactions may vary. However, you might want to consider one or more of the following responses. They might not save you this time around, but considering the threats at play and the responses you'll need to take, developing a planned response before an event is a critical piece of an overall solution as well. Forewarned is forearmed.

- Are you still connected to the source of the attack? If the intruder came in via the Internet, is your connection still up? Should it be?
- Is only one system compromised or are there others? Are you sure?
- Once a system is compromised, it's difficult to recover cleanly, as you have no idea what tools the offender may have left behind. Plan for a complete drive format and reinstall of the compromised platforms, restoring from a known good backup, if at all possible.
- Have passwords been compromised? Force your users to change their passwords immediately.
- Have you confirmed the attack and verified that it has in fact occurred?
- Are there preventative steps you can take to keep this from happening again?
- Establish a relationship with a local, trusted "go-to" partner who can provide security-related expertise, insights, and assistance when needed.
- Do you have a comprehensive security policy documented and in force?
- Will you be pursuing legal action in response to the attack? Are you preserving the necessary evidence to support that action?
- Is it possible to overreact?

Security – An Elusive Goal

While intrusion detection alone is not a security plan, it certainly is a critical component in the complete approach. And as is so often the case, the best weapon is knowledge. Having the right information at the right time is paramount when protecting your mission critical business infrastructure from threats unknown.

Raritan is here to help provide that information and the tools you need to get it to the right people. As before with network and systems management and now in security, Raritan *is* your eye on the network.

Appendix F: Notification Parameters

Notification Parameter Substitution

The notification subsystem is very robust and flexible, allowing the appropriate notification of the appropriate personnel at the appropriate time. One feature you have control over is the content of the notification message. You can include any text, and use parameter substitution to fill in values the CC-NOC knows. Simply include the appropriate variable in the %type[key]% format, and the notification engine will determine and include the correct information to substitute when sending the notification.

If for some reason the CC-NOC cannot determine what information to substitute, the value will be blank.

Available values

The following notifications parameters are available for substitution:

Notification:

%notice[id]%	database id of the notice (This is the ID you use when you acknowledge notices).
%notice[iphostname]%	Host name of the device referenced in the event if node id is provided in the event
%notice[nodelabel]%	replaced by nodelabel if node id is provided in the event

Events:

%event[uei]%	Raritan's internal representation of the event
%event[source]%	The system or process generating the event
%event[nodeid]%	Raritan internal node Identifier (integer) (not in all events)
%event[time]%	Time of event
%event[host]%	Serial number of the box generating the event
%event[interface]%	Interface ID in the event
%event[snmphost]%	Host name in an SNMP trap
%event[service]%	Service in event (not in all events)
%event[snmp]%	SNMP attributes, comma delimited (id, idtext, version, specific, community). "Undefined" is substituted for any attribute not set.
%event[id]%	SNMP Object ID of trap
%event[idtext]%	Not Implemented
%event[version]%	Version of SNMP
%event[specific]%	SNMP specific trap Identifier
%event[generic]%	SNMP generic trap identifier
%event[community]%	SNMP community string
%event[severity]%	Severity of event
%event[operinstr]%	Not implemented
%event[mouseovertext]%	Not implemented
%event[parm[values all]]%	All parameter values (space separated)
%event[parm[names all]]%	All parameter names (space separated)
%event[parm[all]]%	All parameter values and names (space separated, format is name="value")

%event[parm[name]]%	replaced by the value of the parameter named 'name', if present
%event[parm[##]]%	replaced by the total number of parameters
%event[parm[#]]%	replaced by the value of the parameter number '#', if present

Assets:

The format of an asset parameter is simply %asset[Field Name]% where field name matches the labels (with formatting changes) in the asset information screen.

%asset[address 1]%	%asset[operatingSystem]%
%asset[address2]%	%asset[port]%
%asset[assetNumber]%	%asset[rack]%
%asset[building]%	%asset[region]%
%asset[circuitId]%	%asset[room]%
%asset[city]%	%asset[serialNumber]%
%asset[comment]%	%asset[slot]%
%asset[dateInstalled]%	%asset[state]%
%asset[department]%	%asset[userLastModified]%
%asset[description]%	%asset[vendor]%
%asset[division]%	%asset[vendorAssetNumber]%
%asset[floor]%	%asset[vendorFax]%
%asset[lease]%	%asset[vendorPhone]%
%asset[leaseExpires]%	%asset[zip]%
%asset[maintContract]%	%asset[user_defined_1]%
%asset[maintContractExpires]%	%asset[user_defined_2]%
%asset[supportPhone]%	%asset[user_defined_3]%
%asset[manufacturer]%	%asset[user_defined_4]%
%as set [modelNumber] %	

Appendix G: Network Traffic Overhead: Network Management's Necessary Evil

On five-minute intervals, the CC-NOC polls services on managed nodes using Raritan's 'synthetic transactions'. These transactions serve to better test the service's availability, as they actually exercise the service, as opposed to simply "pinging" the box, making the leap of faith that the services you rely on are still responding appropriately.

It's important to note that Raritan, throughout the initial development of our product, went to great lengths to gather as much valuable information as possible without unnecessarily impacting the network. Some overhead is necessary, but between load-leveled polling, spreading polls out over time, and configurable concurrency, only a limited number of devices are allowed to be polled simultaneously, the overhead appears as more of a constant "hum" in the background, as opposed to the regular, significant spikes you may see generated by other network management tools.

On an arbitrary box, we measured the traffic generated by four different CC-NOC poll types:

- ICMP pings
- TCP socket reachability (used for monitoring database listeners)
- HTTP synthetic transaction
- SNMP data collection

As each poll happens on five-minute intervals, we'll use 300 seconds as the denominator in calculating average bandwidth impacts. We'll also include the actual time it took to complete the poll.

ICMP Pings

Raritan considers ICMP a service provided an interface. As such, we discover and monitor that service independently. We also use the availability via ICMP as our "lowest common denominator" in determining if a service outage is actually symptomatic of an interface or node outage.

In the case of this arbitrarily chosen node:

ICMP Ping issued:	90 bytes (720 bits)
ICMP Ping response:	90 bytes (720 bits)
Total Traffic:	180 bytes (1440 bits)
Transaction time:	.000057 seconds
Average bandwidth:	4.8 bps
% of 10Mbps Ethernet:	.00000048%
% of 100Mbps Ethernet:	.000000048%

TCP Socket Reachability

As a test of a services ability to accept TCP session requests, one synthetic transaction type we use, predominantly for database connectivity testing, is that of TCP socket connects. For those versed in the protocol, this is the standard SYN-SYN/A

CK-ACK three-way handshake, which when completed, indicates that the port is listening and accepting connections. This handshake is a pre-cursor to any TCP session and is also embedded within most other synthetic transactions, including HTTP, which we'll discuss later.

In the case of this node:

TCP SYN issued:	74 bytes (592 bits)
TCP SYN/ACK response:	74 bytes (592 bits)
TCP ACK response:	66 bytes (528 bits)
Total Traffic:	524 bytes (1712 bits)
	.000219 seconds
Transaction Time:	524 bytes (1712 bits)
Average bandwidth:	.000000571%
% of 10Mbps Ethernet:	.0000000571%
% of 100Mbps Ethernet:	

HTTP Synthetic Transaction

This test of HTTP service availability includes the TCP session setup, as described above, a web page request, typically a HTTP re-direct in response, a downloaded page, and a session close. Due to the nature of the protocol, this carries significantly more overhead than other, more simple tests, but it also proves conclusively that the server is responding and is capable of serving web pages.

In this case:

TCP Setup (from above):	524 bytes (1712 bits)
HTTP GET Request:	84 bytes (672 bits)
HTTP Response and page:	1054 bytes (8432 bits)
Session Close:	198 bytes (1584 bits)
Total Traffic:	1860 bytes (14880
Transaction time:	.11 seconds
Average bandwidth:	49.6 bps
% of 10Mbps Ethernet:	.00000496%
% of 100Mbps Ethernet:	.000000496%

SNMP Data Collection

The collection of performance metrics from SNMP agents happens independently of SNMP availability testing, which by default, is OFF. When an agent is discovered, a suite of performance metrics specific to that device type is collected from the agent every five minutes. Because the type of data and number of data points collected varies by host type, the following describes a "typical" host, specifically, a Linux host from which we collect ten metrics for the host, and an additional five metrics per managed interface. The host used in this example has two interfaces, so the results reflect metrics for a second interface as well as the de facto first interface.

The traffic generated by the data collection process, in this case:

SNMPv2c GETBULK Requests:	748 bytes (5984 bits)
SNMPv2c Responses:	869 bytes (6952 bits)
Total Traffic:	1617 bytes (12936 bits)
Transaction time:	.0536 seconds
Average bandwidth:	43.12 bps
% of 10Mbps Ethernet:	.00000431%
% of 100Mbps Ethernet:	.000000431%

This data is extremely system, time, and network specific--your results WILL undoubtedly vary. However, for the sake of our argument, let's proceed to look at the overall network impact.

The running total of traffic generated on the network:

ICMP Ping:	180 bytes
TCP Synthetic Transaction:	180 bytes
HTTP Synthetic Transaction:	1860 bytes
SNMP Data Collection:	1617 bytes
Aggregate Total:	4181 bytes
Aggregate Total Bits:	33,448 bits
Aggregate Network Utilization per five minute interval:	111.5 bps
Reflected in Kbps:	.1 Kbps
Reflected in Mbps:	.0001 Mbps

As a percentage of bandwidth:

56 Kbps WAN Circuit:	1.79%
1.54 Mbps DS-1 Circuit:	.00722%
10 Mbps Ethernet:	.00001 %
100 Mbps Fast Ethernet:	.0000001%

In addition to polling overhead, our services scan will run less than once a day and generate traffic roughly equivalent to a single polling interval. If vulnerability scanning is enabled, the CC-NOC will also generate the traffic associated with completing those tests. Benchmarks as to those tests are not currently available.

In summary, the overhead introduced by any network management tool is not necessarily trivial, given some network types. However, as "speeds and feeds" increase dramatically, corresponding costs drop, and better-engineered network management platform, for example, Raritan's CC-NOC, emerge, this overhead will become increasingly nominal.

Additional Notes

The design team at Raritan has gone to great lengths to minimize impacts on networks we are managing. We believe that the numbers called out in this report reflect that conscious attempt at traffic minimalization, and we believe if compared to other systems on the market today, these numbers would prove to be not only competitive, but industry-leading. However, if you decrease the polling interval, you will see a larger impact to the environment. Take this into consideration before performing any significant changes to the polling engine.

The numbers in this document reflect a given point-in-time test in a controlled environment. The test was conducted with a production CC-NOC in a stock configuration.

255-80-5301-00

World Headquarters

Raritan Computer, Inc.
400 Cottontail Lane
Somerset, NJ 08873
USA
Tel. (732) 764-8886
Fax (732) 764-8887
Email: sales@raritan.com
www.raritan.com

Raritan OEM Division

Peppercon USA, Inc.
111 E. Wacker Dr, Suite 2626
Chicago, IL 60601
Tel. (847) 466-1392
Fax (312) 729-1375
Email: info@peppercon.com
www.peppercon.com

Asia Pacific Headquarters

Raritan Computer Taiwan, Inc.
5F, 121, Lane 235, Pao-Chiao Road
Hsin Tien Taipei
Taiwan, ROC
Tel. (886) 2 8919-1333
Fax (886) 2 8919-1338
Email: sales.asia@raritan.com
http://www.rcit.com.tw

Raritan China Offices

Shanghai Representative Office of
Raritan Computer, Inc.
Rm 17E Cross Region Plaza
899 Lingling Rd., Shanghai
China 200030
Tel. (86) 21 5425-2499
Fax (86) 21 5425-3992
Email: sales.china@raritan.com
http://www.raritan.china.cn

Guangzhou Representative Office of
Raritan Computer, Inc.
1205/F, Metro Plaza
183 Tian He Bei Road
Guangzhou
China 510075
Tel. (86-20)8755 5581
Fax (86-20)8755 5571
Email: sales.china@raritan.com
http://www.raritan.com.cn

Beijing Representative Office of Raritan
Computer, Inc.
Unit 1310, Air China Plaza
No.36 XiaoYun Road, Chaoyang District
Beijing
China 100027
Tel. (86) 10 8447-5706
Fax (86) 10 8447-5700
Email: sales.china@raritan.com
http://www.raritan.com.cn

Raritan Korea

Raritan Computer Korea Inc.
#3602, Trade Tower, World Trade Center
Samsung-dong, Kangnam-gu
Seoul, Korea
Tel. (82) 2 557-8730
Fax (82) 2 557-8733
Email: sales.korea@raritan.com
http://www.raritan.co.kr

Raritan Computer Japan, Inc.

4th Floor, Shinkawa NS Building
1-26-2 Shinkawa, Chuo-ku
Tokyo, Japan 104-0033
Tel. (81) 03-3523-5991
Fax (81) 03-3523-5992
Email: sales@raritan.co.jp
http://www.raritan.co.jp

Raritan Computer Japan Osaka Office
Honmachi Phoenix Bldg 8F
1-15-8 Nishihonmachi Nishi-ku
Osaka, Japan 550-0005
Tel. (81) (6) 4391-7752
Fax (81) (6) 4391-7761
Email: sales@raritan.co.jp
http://www.raritan.co.jp

Raritan Australia

Level 2, 448 St Kilda Road
Melbourne, VIC3004
Australia
Tel. (61) 3 9866-6887
Fax (61) 3 9866-7706
Email: sales.au@raritan.com
http://www.raritan.com

Raritan Computer Taiwan Inc India Liaison Office

210 2nd Floor Orchid Square
Sushant Lok 1, Block B, Mehrauli
Gurgaon Rd, Gurgaon 122 002
Haryana
India
Tel. (91) 124 510 7881
Fax (91) 124 510 7880
Email: sales.india@raritan.com
http://www.raritan.com

European Headquarters

Raritan Computer Europe, B.V.
Eglantierbaan 16
2908 LV Capelle aan den IJssel
The Netherlands
Tel. (31) 10-284-4040
Fax (31) 10-284-4049
Email: sales.europe@raritan.com
http://www.raritan.com

Raritan Computer France

120 Rue Jean Jaurés
92300 Levallois-Perret
France
Tel. (33) 14-756-2039
Fax (33) 14-756-2061
Email: sales.france@raritan.com
http://www.raritan.fr

Raritan Computer Deutschland GmbH

Lichtstraße 2
D-45127 Essen
Germany
Tel. (49) 201-747-98-0
Fax (49) 201-747-98-50
Email: sales.germany@raritan.com
http://www.raritan.de

Raritan Computer Italia

Via dei Piatti 4
20123 Milan
Italy
Tel. (39) 02-454-76813
Fax (39) 02-861-749
Email: sales.italy@raritan.com
http://www.raritan.com

Raritan Canada

Raritan Computer Inc.
2085 Hurontario St., Suite 300
Mississauga, Ontario
Canada
L5A4G1
Tel. (905) 949-3650
Fax (905) 949-3651
Email: sales.canada@raritan.com
http://www.raritan.com

Raritan Computer U.K. Limited

36 Great St. Helen's
London EC3A 6AP
United Kingdom
Tel. (44) 20-7614-7700
Fax (44) 20-7614-7701
Email: sales.uk@raritan.com
http://www.raritan.com