CCM

Contivity Configuration Manager 2.3 Release Notes

315768-F

Document status: Standard
Document version: 01.01
Document date: March 2006

Printed in the United States of America.

Trademarks

Restricted rights legend

Statement of conditions

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks Inc. software license agreement

This Software License Agreement ("License Agreement") is between you, the end-User ("Customer") and Nortel Networks Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

"Software" is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. **Licensed Use of Software.** Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. **Warranty.** Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. **Limitation of Remedies.** IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. **General**

    a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Contivity Configuration Manager 2.3 Release Notes

Before you begin

ATTENTION

You must, at a minimum, have the full Integrated Framework Release Build of CCM 2.2 installed before you can upgrade to CCM 2.3. If you have CCM 2.2 or CCM 2.2.1 installed, you may proceed with the upgrade to CCM 2.3.

CCM 2.3 does not use InstallAnywhere for its installation. Therefore you **must** follow the installation procedure given in the document *Installing Contivity Configuration Manager 2.3* (318218-C).

This document does the following:

- lists the books with changes for the CCM 2.3 Release
- describes the new features for the CCM 2.3 Release
- makes usage recommendations for CCM
- describes the resolved anomalies for CCM, Contivity 221*, and Contivity 251*
- describes the known anomalies for CCM, Contivity 221, and Contivity 251

Contivity Configuration Manager 2.3 supports the Contivity CES version 6.0 devices, the 5.05 and 5.07 devices, the Contivity 221 version 2.5 device, and the Contivity 251 version 2.2 device. CCM 2.3 does not provision OSPF totally stubby areas. This must be configured on the CES.

Note: Contivity is also known as VPN Router, and Contivity Configuration Manager is also known as VPN Router Multi-Element Manager.

Books included in this release

The following books are updated for the CCM 2.3 Release:

- *Using Contivity Configuration Manager to Configure Contivity*
- *Installing Contivity Configuration Manager 2.3*
- *Contivity Configuration Manager 2.3 Release Notes*
- *Using Contivity Configuration Manager to Configure Contivity 221*
- *Using Contivity Configuration Manager to Configure Contivity 251*

Note: The on-line help system does not contain the new feature information for the 2.3 release.

How to get help

This section explains how to get help for Nortel* products and services.

Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support web site, and you have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Supported platforms for CCM 2.3

Tables 1 to 3 list the platform requirements you need to run the CCM software components.

Note 1: Windows systems require a video card that supports 256 colors. CCM will not install on Windows systems with a video card that only supports 16 colors.

Note 2: The disk space requirements for Windows platforms are for the Windows NT* file system (NTFS). Windows systems with FAT file systems require more disk space.

Note 3: BNR does not run on the Windows 2003 Server operating system. BNR works on Windows NT, Windows 2000, Windows XP, and Solaris systems only.

Table 1
CCM Server with a Cloudscape database

Processor	Memory	Disk space	Operating system
Intel* Pentium III, 1 GHz or faster	1 GByte	300 MBytes + 5 additional MBytes for each managed network element	Windows 2003 Server, Windows 2000 Professional Service Pack 3, Windows XP Professional Service Pack 1, or Windows NT 4.0 (Server or Workstation) and Service Pack 6a or greater
Sun* Ultra 60	1 GByte	300 MBytes + 5 additional MBytes for each managed network element	Solaris 8 (with J2SE patch cluster)

Table 2
CCM standalone client

Processor	Memory	Disk space	Operating system	Web browser
Intel Pentium II, 500 MHz or faster	256 MBytes	100 MBytes	Windows 2003 Server, Windows 2000 Professional Service Pack 2, Windows XP Professional Service Pack 1, or Windows NT 4.0 (Server or Workstation) and Service Pack 6a or greater	Netscape* 4.7 (or later) Microsoft Internet Explorer 5.0 (or later)
Sun Ultra 1	256 MBytes	200 MBytes	Solaris 8 (with J2SE patch cluster)	Netscape 4.7 (or later)

Table 3
CCM Web Client

Processor	Memory	Disk space	Operating system	Web browser
Intel Pentium II, 500 MHz or faster	256 MBytes	20 MBytes	Windows 2003 Server, Windows 2000 Professional Service Pack 2, Windows XP Professional Service Pack 1, or Windows NT 4.0 (Server or Workstation) and Service Pack 6a or greater	Netscape 4.7 (or later) Microsoft Internet Explorer 5.0 (or later)
Sun Ultra I	256 MBytes	20 MBytes	Solaris 8 (with J2SE patch cluster)	Netscape 4.7 (or later)

Installing CCM 2.3 on Windows 2003 Server

If you wish to install CCM 2.3 on the Windows Server 2003 operating system, you must go to www.nortel.com/support and download Installer Patch V2.2.0.1_124. After you have applied the patch, you can proceed with the CCM 2.3 installation.

Note: This Installer Patch (v2.2.0.1) for CCM 2.2 addresses the issue where InstallAnywhere would not allow a successful installation of the CCM 2.2 release onto the Microsoft Windows Server 2003 platform.

New features in CCM 2.3

The following sections describe the new features for this release.

802.1q VLAN Routing Phase II

The 802.1q Virtual Local Area Network (VLAN) Routing Phase II features facilitate routing between virtual Local Area Network (LAN) segments. The features provide integration with LAN equipment, and environments utilizing VLANs, for traffic segregation. With the VLAN Phase II 802.q enhancements:

- public VLAN subinterfaces can dynamically obtain their IP address from the Dynamic Host Configuration Protocol (DHCP) server
- multiple DHCP-client subinterfaces on the same physical LAN can negotiate their Internet Protocol (IP) address without interfering with each other
- private VLAN subinterfaces can act as DHCP servers for their own virtual LANs
- multiple DHCP servers can operate on the same physical LAN without interfering with each other
- private interfaces can enable DHCP servers
- Virtual Router Redundancy Protocol (VRRP) can operate on private VLAN subinterfaces
- VRRP routers from different VLANs can operate without interference when sharing the same physical LAN
- public or private VLAN subinterfaces can be used as the Local Gateway Interface of an asynchronous Branch Office tunnel (ABOT) Initiator
- Differentiated Services Code Point (DSCP) can offer either standard (fixed) mappings or new custom mappings

AES 256 Support for Branch Office

The Advanced Encryption Standard (AES) offers a computationally more efficient and cryptographically stronger algorithm than the Data Encryption Standard (DES) and replaces 3DES as the National Institute of Standards and Technology standard. CCM 2.3 supports AES 256 bit encryption for Branch Office groups, providing protection for sensitive data. The new feature includes both 256 bit AES with Group 8 (ECC 283-bit prime) and 256 bit AES with Group 5 (1536-bit prime) encryption.

Asynchronous Data over TCP

CCM 2.3 supports Asynchronous Data over Transport Control Protocol (TCP).

BGPv4

Border Gateway Protocol (BGP) version 4 provides a new set of mechanisms for supporting classless inter-domain routing. These mechanisms include support for advertising an IP prefix, which eliminates the concept of network

class within BGP. BGP-4 also introduces mechanisms that allow aggregation of routes, including aggregation of autonomous system (AS) paths. BGP is supported over IPSec, L2TP, L2TP/IPSec and PPTP tunnels.

Change Default Admin HTTP and HTTPS Server Ports

CCM 2.3 now allows users to change the default Administration server port numbers for Hypertext Transfer Protocol (HTTP) and HTTP over Secure Sockets Layer (HTTPS).

Clear Do Not Frag Bit

The Clear Do Not Frag Bit feature allows Contivity to clear the Don't Fragment (DF) bit on fragmented packets when the Stateful Firewall or interface filters are enabled. This prevents the dropping of a packet that requires fragmentation, but has the DF bit set.

Cone NAT/NAT Hairpinning

Cone Network Address Translation (NAT) allows a host (behaving as a Simple Traversal of UDP through NAT [STUN] client) on a private network to obtain its mapped public address from a STUN server. The CCM 2.3 Cone NAT features support changes needed to support address and port discovery mechanisms for VoIP. With Cone NAT, private clients can use STUN to determine their public IP address and facilitate peer-to-peer communication.

CCM 2.3 also supports the NAT Hairpinning feature. Hairpinning is the process of sending data back towards the source to reach its destination. Hairpinning must be used with STUN if two addresses are bound to the same NAT.

Configurable Ethernet Interface Speed for SNMP Queries— IfSpeed Enhancement

With the CCM 2.3 Configurable Ethernet Interface Speed for SNMP Queries feature, a user can configure an Ethernet interface speed, which could be T1, DLS, or Frame Relay, rather than the standard 10 or 100 Mbps Ethernet interface speed. The interface speed is displayed when Simple Network Management Protocol (SNMP) queries the Management Information Base (MIB). You can now configure an interface speed of 0 to 1 Gbps.

Configurable Warning Time for Certificate Expiration

CCM 2.3 users can query the MIB through SNMP to find the expiration date for any certificate. This simplifies the monitoring and automation of certificate management. Users can configure the certificate expiration warning period of 7 to 365 days.

Dial on Demand

The CCM 2.3 Dial On Demand (DoD) feature replaces the Backup Interface Services (BIS) feature. DoD interfaces are assigned a priority level, allowing the creation of multiple definitions for a single physical interface.

A DoD interface can be:

- Idle: Trigger event has not occurred.
- Activated: Trigger event has occurred.
- Connecting: Connection attempts in progress.
- Connected: Connection completed, traffic is flowing.

  Only the highest priority DoD interface will be Connecting or Connected.

  In the DoD feature, a traffic trigger immediately adds defined routes to the route table. Any IP traffic sent to the defined route activates the DoD interface. The DoD interface deactivates when no outgoing traffic is sent over the defined period.

  Unlike the BIS feature, DoD no longer distinguishes a *default route*. Instead, a remote network of 0.0.0.0. is defined. Additionally, a CCM user can assign separate usernames and passwords to each of the three phone numbers, which allows dialing to different accounts.

Framed E1

With CCM 2.3, the CES can use Framed E1 WAN interfaces. Framed E1 is the European counterpart to the North American T1. With Framed E1 users are allotted a fraction of an E1 circuit through timeslot provisioning.

In Framed E1, time slot 0 is reserved for framing. 31 data timeslots are available in an E1 if timeslot 16 is set to data, corresponding to a data rate of 1.984 Mbps. If time slot 16 is set to signaling, 30 timeslots are available for data, corresponding to a data rate of 1.920 Mbps. In Unframed (UF) E1, the full 32 timeslots are used, for a corresponding data rate of 2.048 Mbps.

Frame Relay Phase II

The CCM 2.3 Phase II Frame Relay feature supports the interleaving, encapsulation, prioritization, compression, and fragmentation of data.

Frame Relay Fragmentation 12 (FRF.12) defines Frame Relay extensions through which a sender can fragment the packets within a virtual circuit (VC). With this feature, high-priority packets can be interleaved between fragments of lower priority packets. Such fragmentation and interleaving is required to ensure high voice quality for calls using Voice over Internet Protocol (VoIP) when transmitting voice and data over a wide-area network (WAN).

When this feature is enabled, packets of less than the fragment size and voice packets are transmitted without fragmentation. If a fragment is detected as missed on the receive side, all other fragments for that packet are discarded. Fragmentation can be used if the VC protocol is Multiprotocol over Frame Relay (MPoFR). The Frame Relay features support end-to-end fragmentation, and is restricted for use on private VCs only.

LDAP Proxy User and Password Management

You can use the LDAP Proxy User Authentication and Password Management feature to authenticate network users through a Lightweight Directory Access Protocol (LDAP) proxy. The feature also provides password management abilities. The feature supports the IBM RACF server, the Netscape directory server, and the Novell directory server.

Management Virtual Address

In CCM 2.3, a Management Address is no longer associated with the physical private interface. The Management Virtual Address is now a reserved Circuitless Internet Protocol (CLIP) address. A user can configure a Management Virtual Address on the same subnet as any of the directly connected private LANs on the CES. A user can also configure a Management Virtual Address on a different subnet if the Virtual Management Address is not already included in one of the private subnets. All services available for pre-CCM 2.3 interface Management Addresses are available for the new Virtual Management Address feature.

Multinetting

CCM 2.3 supports the use of Multinetting. You can create up to eight IP subnetworks on one physical LAN interface on a CES.

Next Hop Traffic Filters

With CCM 2.3, filtered traffic can be forwarded to next hop destinations across private or public tunnelled interfaces. This feature preserves existing IP traffic filter functionalities.

The Next Hop traffic filter forwards traffic using the next hop address configured in the filter. If the specified next hop address becomes unreachable, the Contivity defaults to traditional destination-based routing using the routing table.

The CES utilizes the Berkeley Packet Filter (BPF) to inspect each packet to determine whether the packet should be allowed, denied or redirected. The BPF, defined by the user, is compiled by the BPF compiler to generate a BPF filter program. The BPF filter program can be applied at various points along the data path within the CES to determine whether to permit, deny or redirect traffic from entering or exiting these checkpoints. Each packet arriving at the Checkpoint is subject to a state-less packet inspection.

Each IP interface can have inbound and/or outbound filters, which will cause an action to be taken on an incoming packet if the packet properties match the filter criteria. An interface configured to use the Next Hop feature in the inbound filter rule will accept the packet and use Next Hop forwarding.

This feature is only applicable for inbound filters per physical or virtual interface per protocol.

Ping to Validate Public Route

The Ping to Validate Public Route feature allows Contivity to verify the status of a link from the CES Public Interface, through the asymmetric digital subscriber line (ADSL) modem, to a remote endpoint on a Broadband Remote Access Server (BRAS). This feature preserves data traffic that may otherwise have been lost; without this feature, the CES cannot detect a link failure beyond the ADSL link.

Enabling the Ping to Validate Public Default Route feature causes the CES to periodically ping the remote tunnel endpoint. If the ping fails, the public default route is disabled. If the ping succeeds, the public default route is enabled, or continues to be enabled. Traffic is forwarded through the tunnel only if the tunnel endpoint is reachable.

Secure LDAP on Public Interface

With the Secure LDAP on Public Interface feature, the user can configure port numbers and LDAP services for the LDAP Proxy Authentication Server.

Unlock user that has Administrative rights

With the Unlock user that has Administrator rights feature, a user with an Administrator account can be unlocked when the account is blocked.

New features in Contivity 221

The following sections describe the new Contivity 221 features for this release.

802.1x over Ethernet

The 802.1x standard is an IEEE standard for passing Extensible Authentication Protocol (EAP) data over a LAN. The EAP messages are packaged in Ethernet frames to provide authentication.

Bandwidth Management

With the Bandwidth Management feature, you can allocate the outgoing capacity of an interface to specific types of traffic. You can also ensure that the Contivity 221 forwards certain types of traffic (especially real-time applications) with minimum delay. This feature allows you to manage bandwidth for the Contivity 221 by configuring classes and filters for LANs and WANs.

Certificate Management

The Contivity 221 uses certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. Certificates provide a way to exchange public keys for use in authentication.

Configuring Contivity Client Global Setting for VPN

The Contivity Client Global Setting features provides configuration support for client global settings for VPNs. You can use this feature to configure exclusive use mode for client tunnels.

IPSec Tunnel Nail Up

This feature ensures that the Contivity 221 automatically renegotiates an IPSec tunnel when the IPSec Security Association (SA) lifetime expires. When the Contivity 251 restarts, it automatically renegotiates any nailed-up tunnels. In effect, the IPSec tunnel becomes an *always on* connection after the tunnel is initiated.

Multi-user Configuration

With this Contivity 221 feature, you can manage multiple users through the import and export of user information.

SSH/HTTPS for Remote Management

Secure Shell (SSH) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. Hypertext Transfer Protocol over SSL (HTTPS) is a web protocol that encrypts and decrypts web pages. The Contivity 221 device supports these protocols for remote management purposes.

New features in Contivity 251

The following sections describe the new Contivity 251 features for this release.

Bandwidth Management

With the Bandwidth Management feature, you can allocate the outgoing capacity of an interface to specific types of traffic. You can also ensure that the Contivity 251 forwards certain types of traffic (especially real-time applications) with minimum delay. This feature allows you to manage bandwidth for the Contivity 251 by configuring classes and filters for LANs and WANs.

Certificate Management

The Contivity 251 uses certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. Certificates provide a way to exchange public keys for use in authentication.

IPSec Tunnel Nail Up

This feature ensures that the Contivity 251 automatically renegotiates an IPSec tunnel when the IPSec Security Association (SA) lifetime expires. When the Contivity 251 restarts, it automatically renegotiates any nailed-up tunnels. In effect, the IPSec tunnel becomes an *always on* connection after the tunnel is initiated.

SSH/HTTPS for Remote Management

Secure Shell (SSH) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. Hypertext Transfer Protocol over SSL (HTTPS) is a web protocol that encrypts and decrypts web pages. The Contivity 251 device supports these protocols for remote management purposes.

Usage recommendations

This section provides steps that help you avoid issues when configuring the supported devices of CCM.

Before starting the Client

Wait for the CCM Server to complete its start before starting the Client.

Before using CCM

You must activate certain device features before you use CCM to configure devices:

Enabling the Execute Wizards and Launch Applications functions

Before you use CCM to manage Contivity devices, enable the Execute Wizards and Launch Applications functions. To enable the Execute Wizards function:

Step	Action
1	In the CCM navigation pane, go to **Server Startup** and select **User Groups**.
2	Select your Administrator user group and click the **Properties** tab.
3	Click the **Function Security** tab and, in the **Tools** section, select the **Execute Wizards** check box.

—End—

After you enable the Execute Wizards function, you can see the Wizards tab in addition to the Palette and Properties tabs.

To enable the Launch Applications function:

Step	Action
1	In the CCM navigation pane, go to **Server Startup** and select **User Groups**.
2	Select your Administrators user group and click the **Properties** tab.
3	Click the **Function Security** tab and, in the **Tools** section, select the **Launch Applications** check box.
4	In the CCM menu, go to **View > Context Pane** and select **Applications**.

—End—

After you enable the Launch Applications function, you can see the Applications tab in addition to the Palette, Wizards, and Properties tabs. If you cannot see this tab, you must import (not re-import) the device to produce the Applications tab.

Using Launch Applications after installing CCM 2.3

ATTENTION

To use BNR or FPM, you MUST do one of the following workarounds after installing CCM 2.3.

After you install CCM 2.3, you must choose one of two workarounds for accessing or launching applications. The two options for launching or accessing the BNR and FPM applications are:

- Modify the application launch command syntax, or
- Create a shortcut to the application on your desktop.

The following sections describe each option.

Modifying the application launch command syntax

To launch BNR and FPM from within CCM, you MUST change the application launch command syntax. Because this option applies on a per-device basis, Nortel recommends that you do this to the first device in

the CCM navigation tree. After you have changed the command syntax on the first device, you can use this device to launch the application with no loss of functionality to the BNR and FPM tools.

To modify the application launch command syntax:

Step	Action
1	In the CCM navigation tree, select the first CES device, and then click the **Applications** tab. ***Note:*** You can repeat this procedure for each CES device if you wish. However, you can launch the application from the first device, then use the application for other devices.
2	Select the application you wish to launch, and click **Modify**.
3	On Windows systems, in the **Command** field, change classes to ptclasses. For example, change "jre\bin\java" -jar "classes\bandr.jar" to "jre\bin\java" -jar "ptclasses\bandr.jar". OR On Solaris systems, in the **Command** field, change classes to ptclasses, remove all quotation marks ("), and change any backslash characters (\) to forward slash characters (/). For example, change "jre\bin\java" -jar "classes\bandr.jar" to jre/bin/java -jar ptclasses/bandr.jar. ***Note:*** Reference the known anomaly "Launch Applications on Solaris: BNR and FPM—quotation marks cause launch errors" (page 40) for more information about this issue.
4	Click **OK**.
5	To launch BNR or FPM, select the application and click **GO!**

—End—

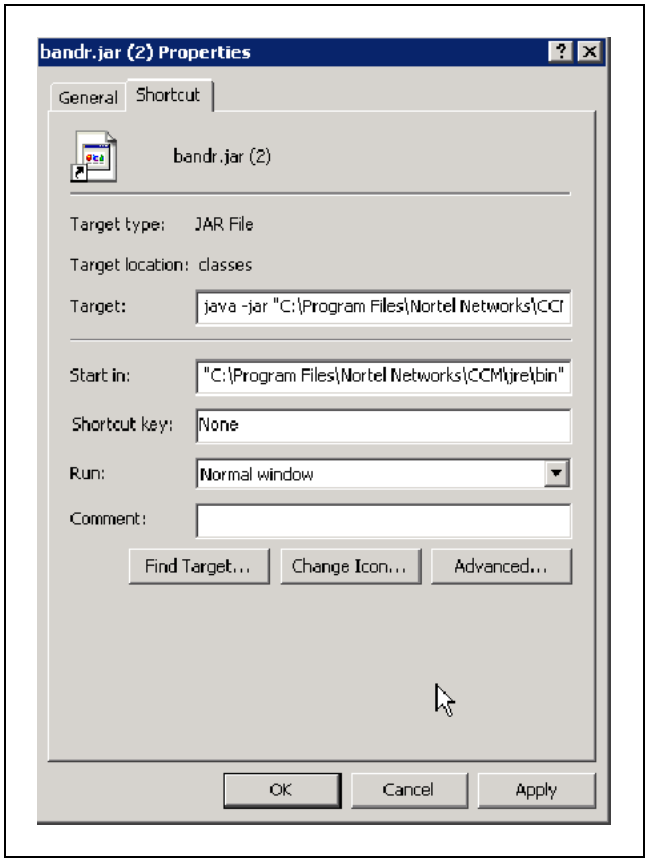
Creating a shortcut to the application on your Desktop

The BNR and FPM applications do not have to be launched from within CCM—they can be run independently by creating a shortcut on your desktop.

On Windows systems, use the following procedure to create a shortcut to the application on your Desktop:

Step	Action
1	On the Desktop, create a shortcut to the appropriate application file. These files are located in the ptclasses subdirectory of the CCM installation directory. The files are named: • bandr.jar file for BNR • fwpolmgr.jar file for FPM
2	After you have created the shortcut, select the shortcut, right-click, and choose **Properties**.
3	On the **Shortcut** tab, in the **Target** field, enter java -jar followed by the path to the application file. For example, if CCM is installed in the default directories, enter java -jar "C:\Program Files\Nortel Networks\CCM\ptclasses\fw-polmgr.jar"
4	In the **Start in** field, specify the path to the jre\bin directory. For example, if CCM is installed in the default directories, enter "C:\Program Files\Nortel Networks\CCM\jre\bin" See Figure 1 "Shortcut parameters" (page 23).

Figure 1
Shortcut parameters



5 Click **OK**.

6 Double-click the shortcut you created.

A DOS window appears, then the application window appears.

—End—

On Solaris systems, use the following procedure to create a shortcut to the application on your desktop:

Step	Action
1	Create a text file. Name the file bnr.run (or fpm.run) and save it to the $HOME directory.

2 Use a text editor, such as vi, to edit the file you created (bnr.run or fpm.run). Assuming that CCM is installed in the default directories, add the following lines to the file.

For Backup and Restore (BNR):

```
cd /opt/CCM/ptclasses
/opt/CCM/jre/bin/java -jar bandr.jar
```

For Firewall Policy Manager (FPM):

```
cd /opt/CCM/ptclasses
/opt/CCM/jre/bin/java -jar fwpolmgr.jar
```

If CCM is not stored in the default directories, then make the appropriate changes to the /opt/CCM line.

3 Change the file permissions so that it can be executed. For example, you can use the following command:

```
chmod +x bnr.run
```

or

```
chmod +x fpm.run
```

4 Copy the file to the Desktop.

5 Double-click the file you copied to the Desktop to run the application.

If a window appears which asks for options and arguments, click **OK**. After you close the application, if a **Run** window is still open, close it.

—End—

ATTENTION

For security reasons, Nortel recommends that you lock your screen if you must leave the computer unattended while CCM, BNR, or FPM are still running.

For Contivity configurations using any access mode

Because CCM relies on File Transfer Protocol (FTP) to send configuration instructions and to collect the results, enable FTP on the Contivity device before using CCM. This applies to any access mode (private network, branch tunnel, or control tunnel) you use. By default, FTP is disabled for Contivity devices. To enable this protocol, use the Services > Available menu options from the Contivity Web UI.

For Contivity configurations using Branch Office access mode

In this access mode, enable FTP Management on the appropriate tunnel filter. To configure this feature from the Web UI, select Profiles > Filters > Edit Tunnel Filter (choose the appropriate filter).

SNMP for Contivity Auto-detect

Since auto-detect in CCM relies on SNMP to discover Contivity devices before importing their configurations from the network, enable SNMP before using CCM. To enable this protocol, use the Service > Available menu options from the Contivity Web UI.

For auto-detect to work properly, you must also add the IP address of the CCM server to the Contivity list for the device. Do this by using the Admin > SNMP menu options from the Contivity Web UI.

For information about SNMP for Contivity Branch Access, see SNMP for Contivity Branch Access Auto-detect.

FIPS (applicable to FIPS-certified products only)

CCM manages products running in Federal Information Processing Standard (FIPS) mode if management is through a tunnel. To configure features through the Web Graphical User Interface (GUI), select Profiles > Filters > Allow Management Traffic > For These Local Services.

CCM 221—CCM and Web GUI

When you configure devices, do not switch between CCM and the Web GUI interface. Complete each configuration task using one or the other, but not both.

CCM 221 SUA/NAT

In Single User Account (SUA)/NAT, the Trigger Port accepts spaces in the name field, but the device does not allow spaces.

CCM warning for illegal value

When you make changes to a device configuration, if you leave required fields without a valid value, the fields appear yellow or red. This means that the information related to that incomplete field is not exported to the device.

Certificates

This section gives information about configuring various certificates.

Configuring a CA certificate

CCM supports the Certificate Authority (CA) certificate configuration in the following form: to configure a CA certificate, first obtain a PKCS#7 Base-64 Certificate encoding from the CA Authority, either using the CA Authority Web site or through an e-mail. Paste the PKCS#7 Base-64 Certificate code

in CCM under Certificates > Tunnel Transport > Trusted CA Certificate Properties in the PKCS#7 Base-64 field. When exported to the box, this string creates the certificate. After exporting the PKCS#7 code, you must import the certificate into CCM. You can use the same string for any number of devices.

Configuring an SSL-based certificate

CCM supports SSL certificate configuration in the following form: to configure an SSL certificate, first obtain a PKCS#7 Base-64 Certificate encoding from the CA Authority, either using the CA Authority Web site or through an e-mail. Paste this PKCS#7 Base-64 Certificate code in CCM under Certificates > SSL Cert > SSL Cert Properties in the PKCS#7 Base-64 field. When exported to the box, this string creates the certificate. After exporting the PKCS#7 code, you must import the certificate into CCM. You can use the same string for any number of devices.

Operations with server certificates

CCM is an off-line configuration tool and does not support generating new server certificates. It supports import operations for the server certificates.

The certificates are imported so that they are available for the Groups and Users configuration. In CCM, you can delete Server certificates when they are no longer needed. To generate a Server certificate using the Web UI, do the following:

Step	Action
1	Using the Web UI, select **System** > **Certificates**, click the **PKCS#10 Certificate Request** tab.
2	Enter the required information and retrieve the encrypted string that the Web UI generates.
3	Send this information to the CA Authority using the Authority Web site or an e-mail. The CA Authority generates the PKCS#7 Base-64 Certificate encoding based on the data that it receives.
4	Using the Web UI, navigate to the **Import Tunnel or Transport Certificate** tab and select **Server Certificate**. Paste the code in the window.
5	Click **OK** to obtain the certificate.

—End—

Note: You must import the Server certificate into CCM for it to be available for other configurations.

General note regarding certificates

You cannot use CCM for certificate storage. If a certificate-populated Contivity image exists in CCM and a certificate is deleted on the Contivity device (either manually or by applying factory defaults), exporting the CCM image does not reapply the old certificates.

Editing Group access control

Group access control entries create an association between an end-user certificate generated from the chosen CA certificate and a Group profile. If you want to edit a CA certificate with a Group access control entry, you must delete the old entry and create a new one. If you simply edit the image in CCM and then export it, Group login conflicts can occur.

Deleting Groups

Before deleting a Group (Profiles > Group), make sure that the Group is not in use in CCM or in a Contivity device. For example, if CA Certificates or RADIUS Authentication refers to a Group, CCM cannot delete this Group correctly.

Deleting scheduled re-imports

To delete a scheduled series of re-imports in CCM, select the Scheduler > Network Reimport > Properties tab. From the Properties tab, select the Schedule tab and clear the *and repeat every* check box.

Exporting

Exporting new users

CCM does not support creating users with both IPSec Username/Password and CA certificates authentication methods when internal Lightweight Directory Access Protocol (LDAP) is used.

Exporting with users using CA certificates

When users employ the CA certificate authentication method, always re-import after performing an export. If you export twice without performing any re-imports, you delete the CA certificate information for the users.

External LDAP

While the CCM 2.3 driver supports configuration of internal and external LDAP servers on Contivity devices, several caveats exist. First, you can only change the LDAP server (Internal to External, External to Internal, or one External to another External) configuration independent of any other changes in CCM. This means that an export containing LDAP server changes must not include any other configuration change.

Also, ensure that all devices using the same LDAP server are kept current in CCM. If changes are made to an LDAP server (for example, users are added), the CCM user must reimport all devices in CCM that use this server so that they all represent the current state of the network. This is true whether the LDAP was modified through CCM (by exporting to a switch that uses the LDAP) or directly through any of the embedded interfaces, such as the Web UI or CLI.

Additionally, when switching from one external LDAP server to another, you must click OK on the external LDAP server page to fully configure the new LDAP server. If you do not click OK and export the configuration, information under Profiles > Group does not reflect that of the new external LDAP server.

If the LDAP server is stopped on the switch (this can be done from the Web UI), do not toggle between the Internal and External LDAP in CCM before performing an export. Doing so can cause the switch to malfunction.

Firewalls

Invalid characters in Service Object names

In CCM, when you create or edit a Service Object in the Firewall, the name field accepts characters that are invalid on the Contivity device. This condition applies to all types of Service Objects. The only characters allowed in Service Object names are as follows:

- a-z, A-Z
- 0-9
- _ (underscore)
- : (colon)
- / (slash)
- , (comma)
- - (hyphen)
- \ (backslash)

Service Object names must start with an uppercase or lowercase alphabetic character.

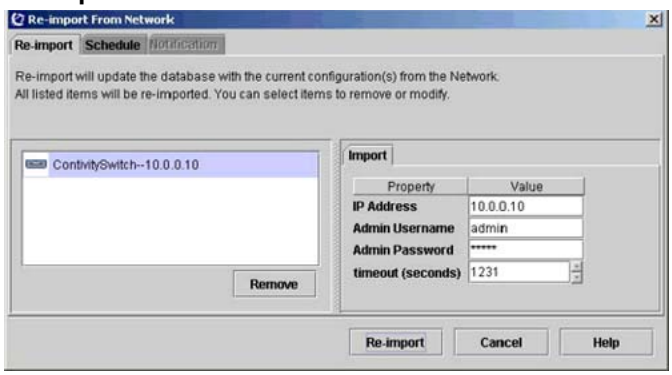
FTP or Telnet not responding

Use Contivity release V03_65.11 or later to prevent unresponsiveness with FTP or Telnet while using CCM. If you do use an earlier version, do not configure more than 100 Branch Offices with CCM.

Input to the data entry field

For data to take effect, move the focus from the data entry field (for example, move the cursor to a different field, or press the Enter key, or select a different tab, and so on). This step typically occurs during the natural flow of operations. If you change the timeout value for re-import operations, you must change the focus before clicking the re-import button (see Figure 2 "Re-import from network" (page 29)). Otherwise, the operation is performed using the old timeout value.

Figure 2
Re-import from network



License keys

CCM gets the installed status of license keys during import. If the keys are installed on the Contivity device before the import, CCM displays Key Installed in the Admin > Install Keys Status tab.

As an off-line configuration tool, CCM permits the configuration of features in the CCM database without a license key. However, for the exported configurations to take effect, you must obtain and install a license key.

Features requiring an advanced routing key can be found in the Contivity Web UI under:

- Routing > OSPF
- Routing > VRRP
- Routing > Configuration (for Equal Cost MultiPath)

Features requiring a firewall key can be found in the Contivity Web UI under:

- Services > Firewall/NAT > Contivity Stateful Firewall

Order of rules in Tunnel Filters

The way to reorder the rows in the Tunnel Filters table in CCM differs from the way it is handled in the Contivity Web UI. To change the order of the rules in the Tunnel Filters table in CCM, you must select the row, then use the Cut and Paste operation to place the rules in the proper order.

Recommended number of Groups and Users

Nortel recommends a maximum of 10 000 Users in any combination, and recommends a maximum of 600 Groups.

Timeout values for import operations

When importing Branch Office configurations, you can adjust the value of the timeout parameter.

If the timeout value is exceeded during an import operation and all the data has not been imported, the import operation fails. This import timeout value also applies to exports, because CCM performs an import behind the scenes during an export.

Tunnel Guard Wizard

On CES devices, Tunnel Guard Policy Management imposes some constraints which dictate CCM Tunnel Guard (TG) Wizard operation. They are:

- The CCM Tunnel Guard Wizard operates on devices whose rule sets are exact version matches; therefore, the rule set on the source device cannot pre-date that of the target device. You can only copy or delete rule sets if the source and target devices run the same image version
- You cannot delete a rule set if the SRS is referenced or used in a group
- You can delete a rule set whose SRS is not referenced or used in a group

For example, consider the following work flow scenario, where the source and target devices both run the image upgrade version 6_00.310:

- Copy the first rule from the source to the target device
- Set the group reference on the target device to use the first rule
- Run the TG Wizard to delete this rule: the delete operation is not allowed
- Copy a second rule from the source to the target device
- Run the TG Wizard to delete this rule: the delete is allowed because the rule is not used or referenced by a group

Using TFTP for backup

Due to reliability issues with TFTP (see "CCM—export and import to TFTP server for backup purposes does not work reliably" (page 37)), use the Backup and Restore tool (BNR) for backups and restores. To use BNR, in the CCM navigation pane, click on the Contivity device you wish to backup, and then click on the Applications tab. Double-click Launch Backup and Restore Manager. You may have to enable the Launch Applications Wizard first (see "Enabling the Execute Wizards and Launch Applications functions" (page 19)).

Resolved anomalies in CCM

The following sections describe the CCM anomalies that have been fixed for this CCM release.

CCM blank network group object

When a blank network object is exported, an error message appears that says "The name already exists". The blank network object then appears in the list of available network objects on CES. (Q01185782)

Contivity drops packets with DF and MF bits simultaneously set

Contivity drops packets that have the Don't Fragment (DF) and More Fragments (MF) bits simultaneously set when the Stateful Firewall is enabled. When the Contivity receives such a packet, it discards it and sends back an Internet Control Message Protocol (ICMP) "Destination unreachable" message. It may also send this message if the packet requires fragmentation but the DF bit is set. (Q01076568)

Copying Branch Office tunnels

If you create a new Branch Office Group under the /Base Group and then copy an existing Branch Office connection to the newly created Group and delete the old connection under the /Base Group, then the remote tunnel endpoint and the IPSec preshared secret are missing upon export of the configuration. (Q00778924)

Data Link Switching—protocol changed

The protocol is changed from Synchronous Data Link Control (SDLC) to Point-to-Point Protocol (PPP) when you enable and disable data link switching (DLSW). (Q01026746)

Default dial interface import

When you use serial mode, the Dial Interfaces should not be configurable. However, in CCM, local IP address, subnet mask, and remote IP address fields are configurable even when serial mode is used. Because of this, you see an error message upon export, but the export operation completes successfully. You may choose to do nothing regarding this issue, or you can enter 0.0.0.0 in the local IP address and remote IP address fields. This prevents the error message from displaying.

The IPSec option on L2TP is not configurable from CCM. In a Branch Office, if you have Compression disabled and the Minimal level set to anything other than Not Required, you must use the Web GUI to configure the IPSec options. (Q00767922)

Firewall considerations for off-CCM server access

When you run a server on a computer that also has a firewall, or that has a firewall installed between the Server computer and the Client computer, issues occur when connecting to the Server from the Client.

This also applies to CCM. Therefore, if you have a firewall installed on the CCM Server, or in the network path between the Server and the Client, make sure that rules on the firewall are defined to permit traffic to flow between Client and Server. (Q01164349)

FPM—firewall object naming

FPM allows you to give a network object and a service object a name that starts with a non-alphabetic character—for example: 1.2.3.4. However, the Contivity device requires that names start with alphabetic characters. Start your firewall object names and service object names with a letter, for example: ip1.2.3.4. (Q01037999)

Hide Administrator userID and password; Admin password backdoor

With a Contivity device, a "Manage Switch" or a "Manage Users" account user can change the administrator account without being the Primary Administrator. The user ID and password are visible. (Q01166718)

Inability to unlock user with administrator privileges

Contivity can be configured to lock out an account after a specified number of failed authentication attempts. An account for a Privileged user cannot be unlocked after the specified number of authentication failures. (Q01014456)

License Management wizard

If given a correctly formatted but incorrect key value, the CCM License Management wizard reports the licensing as a success and shows the key as installed. However, when you check the device, the keys are not installed. (Q00743741 and Q00776599)

Moving existing Groups

In CCM, you can move a named Group to a Group that does not have a name. When you export the configuration, the named Group is not exported. Name your unnamed Group before moving the named Group. (Q00968799)

Moving existing users

In CCM, you can move an existing user to a Group that does not have a name. When you export the configuration, the existing user is not exported. Name your unnamed Group before moving the existing user. (Q00968798)

NAT overflow

CCM erroneously allows you to define a NAT set that overflows the external IP address. Contivity devices do not allow the overflow and reject the rule upon export. (Q00770145)

QoS > Interfaces—different default values

In the QoS > Interface screen, different default values exist for some Non-Tunnel Traffic ratings than those the Contivity device shows. For example, the default value for interface LAN, Non-Tunnel Traffic Rating is 10 percent. The default value for the Public Interface (SLOT 1), Non-Tunnel Traffic Rating is 90 percent. (Q01026767)

RADIUS server public addresses

Public addresses for RADIUS servers are not importing. In addition, Profile > Group > RADIUS server entries are also not importing or exporting correctly. If you want to specify or change Profile > Group > RADIUS server information, do so through the Contivity Web GUI.

Route Policy—status disabled

A Route Policy is created with status disabled. (Q01025874)

User accounts lost on export

If you move more user accounts from one account to another account in CCM and then export the configuration to a Contivity device, the user account information is lost during the export operation. (Q00730206)

Resolved anomalies in Contivity 221

The following sections describe the Contivity 221 anomalies that have been fixed for this CCM release.

CCM and Web GUI

When you configure devices, do not switch between CCM and the Web GUI interface. Complete each configuration task using one or the other, but not both. (Q00793815)

Changing service objects

To properly make changes to service objects or service names in CCM, remove the service from all rules associated with it, make all desired changes, then add the newly changed service back to the rules. This procedure ensures that all service changes are properly accounted for within CCM. (Q00951897 and Q00951918)

Computing algorithm for DHCP pool

In CCM, the pool size is computed incorrectly when determining the last address in the DHCP pool. This is an off-by-one issue. The pool size applied by CCM is one less than the actual pool size. (Q01145086)

PPTP export

When you set the encapsulation mode to WAN > PPTP, disable the nailed-up option, and then export to a Contivity 221, the change does not export. (Q00783705)

Static route entries

With a Contivity 221 device, you can have two static route entries with the same name. However, CCM cannot have two static route table entries with the same name. When you import duplicate entries from 221 into CCM, the duplicate entry does not import and the table field is blank. Import and export operates if all static route entries have different names. (Q00817323)

Static route import

When importing a device into CCM, the static route portion fails if the route name contains a period. Either the route name or the entire route does not appear in the static routes table in CCM. Use only alphanumeric characters when naming routes. (Q00915420)

Resolved anomalies in Contivity 251

The following sections describe the Contivity 251 anomalies that have been fixed for this CCM release.

Content Filter Keyword field

In the Contivity 251 driver, the Keyword field for the content filter can be up to 127 characters in length. However, CCM displays only 19 characters at a time in that field. By moving the cursor, you can view all other characters present in the field. (Q00863194)

Range Ports in Firewall Service Objects

In CCM, you can create Custom Objects under Firewall > Firewall Service Objects. However, if you modify the Port Type to Range and do not modify the Ending Port field to reflect the change, CCM does not report an error.

Static Routes Gateway IP addresses

In CCM, you can define a static route entry with a gateway IP address that is not on a directly connected network. However, the static route entry is unusable. (Q00856261)

Static route import

When importing a device into CCM, the static route portion fails if the route name contains a period. Either the route name or the entire route does not appear in the static routes table in CCM. Use only alpha-numeric characters when naming routes. (Q00915420)

SUA/NAT address mapping

The order of the address mapping rules in the Contivity 251 device is important because they are processed in numeric order. Both CCM and Contivity 251 provide for gaps in the rules specifications so that you can insert rules between other rules in the table. CCM expands on this capability by providing the ability to Copy a rule from one place in the table and Paste it to overwrite another rule in the table. Note that when using this CCM capability, you need to write over other existing rules in the table; hence, leaving gaps within the table makes rearranging easier. (Q00857737)

Known anomalies in CCM

The following sections describe the known CCM anomalies for this CCM release.

Backup and Restore does not run on Windows 2003 Server

Backup and Restore (BNR) does not run on the Windows 2003 Server operating system. BNR runs on Windows NT, Windows 2000, Windows XP, and Solaris systems only. (Q01333785)

Basic page fields accept incorrect values

When you configure a Contivity device using CCM, ensure that the values you enter in the Basic page fields (DNS Host Name, DNS Domain Name, Primary DNS Server, Second DNS Server, Third DNS Server, Fourth DNS Server) are correct. CCM does not give an error message if these values, which should be numeric, are non-numeric. (Q01288260)

BNR—add device

You can add the same device to BNR many times if you specify the IP Address and different DNS names. Nortel does not recommend adding the same device more than once.

BNR—application does not run from CCM unless Contivity is imported

You must import the Contivity device before you can use the BNR application called from CCM. Creating a Contivity device using the Palette does not provide a means for accessing the BNR application. For the BNR application to appear on the Applications tab for that device, you must create the Contivity device by using the Import command. Command line invocation is also possible by using a patch. Contact Nortel for information about this patch. (Q01026553)

BNR—cannot be started from CCM web client

BNR cannot be started from CCM web client. (Q01002851)

BNR—Route Policy issue with duplicate policies

If your backup disk is full, BNR tries to complete as many backups as possible. In this case, BNR can report a variety of error messages in addition to disk full error messages. If a disk-full error message appears, take actions to free up disk space on the backup disk. These actions can include:

- switch backup to another disk
- reduce the number of backups that are retained
- change some backups from Full to Configuration
- use an additional machine to perform some backups
- move some Contivity backup support to a new machine (Q01032690)

Branch Office control tunnel connections

When creating a Branch Office control tunnel connection, select the control tunnel check box before entering a name for the tunnel. If you enter a name before deciding that the connection should be control, the control tunnel check box appears dimmed and unavailable for configuration. You must delete and then add the connection again to configure. (Q00779954)

Branch Office tunnel configuration incomplete

When you fail to complete a Branch Office tunnel configuration, CCM does not issue an error. You cannot export the tunnel configuration. (Q01096899)

Canceled image send operations

If you cancel an Image > Send operation in CCM, CCM lists the operation as canceled, but the FTP server remains busy and the Contivity driver still receives the image. (Q00695376)

CCM 221 WAN/Route Selection

In the WAN/Route Selection, the value for the WAN Priority changes randomly. This occurs when you use the decrement button for the Traffic Redirect Priority. (Q01144977)

CCM 2.3 displays 2.2 in on-line help

After you upgrade from CCM 2.2 or 2.2.1 to CCM 2.3, the CCM Client on-line Help About window still identifies the Product Information version as 2.2. This version corresponds to the products Server build infrastructure version, which has not changed in this release. Therefore, it is still at version 2.2 after the upgrade. To verify that you are using CCM 2.3, scroll

down in the Info tab of the Client on-line help window and you will see that the Installed Cartridges version numbers are labeled corresponding to this release. They are:

- Contivity Secure IP Services Gateway is at version 2.3.0
- Branch Access is at version 2.2.1
- Contivity 221 is at version 2.3.0
- Contivity 251 is at version 2.3.0 (Q01157666)

CCM 2.3 installation fails if directory name surrounded by quotation marks

When you install CCM 2.3, if you specify the directory name using quotation marks, the installation fails. The installation works if you do not use quotation marks. (Q01301531)

CCM 251 network group object validation

In CCM 251, a network group object Subnet Address is not validated correctly. (Q01187591)

CCM allows custom DSCP mappings, CES does not

You can use CCM to configure custom QoS DSCP 802.1 mappings for a Contivity Extranet Switch (CES). However, if you export this configuration to the CES device, the CES does not allow this option to be configured. The Egress and Ingress parameters remain in the Disabled state on the CES device. (Q01262029)

CCM—export and import to TFTP server for backup purposes does not work reliably

The export and import to TFTP server functions do not work reliably in all possible cases. TFTP export and import cannot be used as backup or restore in all possible cases. Use the Backup and Restore (BNR) tool to backup and restore CES1000 and higher CES models. (Q01157706)

CCM firewall rule issues on export to Contivity 221

Sometimes when exporting firewall rules to a Contivity 221, the rules are duplicated or exported incorrectly on the device. Repeated exports of the same rules just add duplicate rules. (Q01142226) (Q01144943)

CCM Framework—potential table index number misalignment

A table index misalignment may occur between CCM and any given device. Tables in CCM start numbering with 0, and some device-specific functional areas start numbering with 1. For example, rule numbers in the Static Routes and IPSec Policy sections on the C221 device start numbering

with 1. The CCM C221 cartridge starts rule numbers with 0. This does not cause any adverse effects on operations between CCM and Contivity devices. (Q01329357)

CCM Scheduler issue

When you shut down and then restart CCM, some operations are reported as removed from the scheduler. The operations were not removed. (Q01185797)

CCM uninstall

The uninstall program identifies itself as CCM 2.2 because this software has not changed with the upgrade to 2.2.1 or 2.3. When uninstalling CCM 2.2.1 or 2.3, you uninstall 2.2, 2.2.1, and 2.3. (Q01157651)

CES Premium Routing Key and OSPF

If you attempt to enable OSPF on an imported Contivity device which has a Premium Routing Key installed, without the Advanced Routing Key enabled, you will receive the following message: An error has occurred: Advanced Routing must be installed before enabling OSPF.

To enable OSPF, you can either:

- Install an Advanced Routing Key, and then enable OSPF from CCM
- Enable OSPF on the CES device. After you enable OSPF on the CES, use CCM to re-import the device (Q01339055)

Changes to Profiles > Network causes tunnel to bounce

When you make changes to Profiles > Network and then export, a short loss of connectivity occurs. (Q00753177)

Changes to QoS

After exporting a different classifier to an interface, even though the export appears to have been successful, you need to update the interface classifier through the GUI for the change to take effect. (Q00818588)

DHCP standard options

On rare occasions, DHCP standard options do not export to a Contivity device when Time Offset is listed before Subnet Mask. When the order of the standard options is changed, the values export correctly.

Export error messages

When the CCM client logs a failure message during an export operation, that message is not apparent on the Client Progress window. If you examine the Messages tab in the CCM client, you see messages that point to a problem with the export operation. (Q00803784)

Factory reset

When you reset the Contivity v4.75 to its factory default, and then attempt to configure its management IP address and enable the FTP server by taking an existing configuration with the Public setup and export it to the device from CCM, the Public Interface remains unchanged. Exporting a second time shows the correct values. (Q00783129)

Filter accepts incorrect addresses

In CCM you can configure incorrect IP addresses and masks in the Profiles > Filters > Interface Filters > Manage Filter Rules and the Profiles > Filters > Tunnel Filters > Manage Filter Rules nodes. CCM erroneously accepts values like 0.1.0.0 for the Address field, and 0.0.0.0 for the Mask field. No error message is given. (Q01259191)

Find in CCM toolbar

The search button on the CCM toolbar does not find all values. (Q01183644)

Find in CCM toolbar (case issue)

The search button on the CCM toolbar is case-sensitive. (Q01183630)

Firewall check box

If you have a Contivity Stateful Firewall license key installed, you can turn off the Contivity Firewall check box by clearing the Contivity Firewall check box. However, if you do not have the license key installed, you must turn off the Contivity Firewall by clearing the No Firewall check box.

Firewall Network Objects not exported

In CCM, you must create a Firewall Network Object and then use it in a rule. If you do not use the Firewall Network Object in a rule, it will not be exported. (Q01168760)

FPM—application does not run from CCM unless Contivity is imported

You must import your Contivity Device before you can use the FPM application called from CCM. Creating a Contivity device using the Palette does not provide a means for accessing the FPM application. For the FPM application to appear on the Applications tab for that device, you must create the Contivity device by using the Import command. Command line invocation is also possible using a patch. Contact Nortel for information about this patch. (Q01026553)

FPM—cannot be started from CCM web client

FPM cannot be started from CCM web client. (Q01002851)

FPM—support for Contivity devices

FPM supports only Contivity devices running version 4.80 and later. It supports only device models 1010 and later. You can use FPM to configure override rules and default rules. Interface Specific rules are not supported.

FPM—User Authentication Group

FPM restricts the User Authentication Group names field. FPM:

- Presents a list of Group names in all devices in the device list, so that you can choose the Group value
- Allows off-list entry of a Group name
- Warns you if the name entered is not a Group name in any of the devices listed in the device list

Launch Applications on Solaris: BNR and FPM—quotation marks cause launch errors

In CCM 2.3 installed on Solaris machines, the double quotation marks around the Launch Applications command syntax cause the launch of FPM or BNR to fail. Manually remove the quotation marks from the command syntax. "Using Launch Applications after installing CCM 2.3" (page 20), in the Usage Recommendations section, describes how to do this. (Q01333325)

LDAP delimiter character

When specifying the LDAP delimiter character, in CCM you can enter more than one character. Be sure to keep your input limited to a single delimiter character.

Map Class Name field accepts incorrect values

When you configure a Map class name using CCM, ensure that the name you enter in the Profiles > Map Class > Basic page Name field only contains letters and/or numbers. CCM does not give an error message if the name contains special characters (for example, ?, >, /). The name must only contain alphanumeric values. (Q01260025)

New Groups

When you create a new Group, give the Group a name before you create any users or subGroups for the Group. If you create users or subGroups in this new Group before it has a name, the user records do not export to the Contivity device, the Group name changes to default, and is not changeable unless you move the user records to another named Group. If the user record is not exported, copy the record to another Group and then export. (Q00823742)

Profiles > Client Policy name should not have special characters

In CCM you can erroneously use special characters in the Profiles > Client Policy Name field. CCM does not give an error message. (Q01301776)

Profiles—Interface Filter cannot be copied to Tunnel Filters

In CCM Profiles > Filters > Interface Filters you cannot copy Interface Filters to Tunnel Filters, or Tunnel Filters to Interface Filters. (Q01302003)

Profiles > Filters rule duplicates

In CCM you can erroneously create duplicate rules in Profiles > Filters> Interface Filters . Current Filters. Duplicate rules are not allowed. No error message is given. (Q01301964)

Known anomalies in Contivity 221

The following sections describe the Contivity 221 known anomalies for this CCM release.

Bandwidth Management—duplicate LAN or WAN classes

In CCM, in the Bandwidth Management > LAN or WAN Root Class node, you can create two or more LAN or WAN classes with the same name. No error message is given. (Q01239625)

Bandwidth Management—LAN class name accepts special characters

In CCM, you can use erroneously use special characters in the LAN or WAN Class Name field. No error message is given, and these values are exported to the Contivity 221 device. If the Name field is left blank, no error message is given. (Q01234635)

Bandwidth Management—LAN or WAN class not exported

In CCM, if you activate, then deactivate, the LAN check box on the Contivity 221 device > Bandwidth Management > Class Setup page, then export, the LAN class is not exported. This only occurs after a Restore to Factory Defaults operation has been completed. This also occurs for WAN classes. (Q01279637) (Q01298043)

Bandwidth Management—LAN or WAN classes not exported with one class

In CCM, if you attempt to export a Contivity 221 device configuration with only one LAN Class configured in the Bandwidth Management node, the export is not successful. If you add LAN classes so that there are two or more configured, the export is successful. This also applies to WAN classes. This problem only occurs after a Restore to Factory Defaults operation has been completed. (Q01243939)

DDNS User Name not required

On the CCM System > DDNS page, you can leave the User Name field empty and only enter a Password. The Contivity 221 device accepts the password without the user name. No error message is given. (Q01264632)

Maximum 40 firewall rules in GUI, 10 in CCM

A Contivity 221 device allows up to 40 firewall rules to be defined. However, CCM allows only up to 10 firewall rules to be defined. When a Contivity 221 device with more than 10 configured firewall rules is imported into CCM, the import fails. An error message that states that the maximum number of rules is 10 appears.

To prevent an import failure of a Contivity 221 device into CCM, verify that the Contivity 221 has only 10 rules or less configured. You may have to delete firewall rules to meet this criteria. (Q01244820)

Remote Management—Secured Client IP Address

Ensure that you configure correct IP addresses in the Secured Client IP Address field in the Remote Management node. If you configure an incorrect Secured Client IP Address in the Remote Management > WWW, Telnet, FTP, SNMP, DNS pages, CCM does not give an error message. In some cases, if you select the Selected button, leave the page, then return, CCM erroneously clears the Selected button and selects the All button. (Q01260165)

Static Routes destination IP address

In CCM you can erroneously configure a Static Routes Destination IP address to be 0.1.0.0 and no error message is given. If you enter an incorrect Subnet Mask, CCM changes the mask value to 255.0.0.0 and no error message is given. If you leave the Destination IP, Subnet Mask, and Gateway IP fields empty, no error message is given. (Q01276309)

SUA/NAT—incorrect IP addresses accepted in Address Mapping

In CCM, on the SUA/NAT > Address Mapping page, you can configure incorrect IP addresses in the Local IP and Global IP fields, such as 0.x.x.x or 127.x.x.x. No error message is given. (Q01264627)

SUA/NAT—incorrect IP addresses accepted in SUA Server

In CCM, on the SUA/NAT > SUA Server page, you can configure incorrect IP addresses in the Default Server and Server IP fields, such as 0.x.x.x or 127.x.x.x. No error message is given. (Q01264630)

UPnP—CCM 2.3 fails to import UPnP Ports tab

When you use CCM to import a Contivity 221, the UPnP Ports tab is missing; the information for preserving port information is not there. (Q01318240)

Known anomalies in Contivity 251

The following sections describe the Contivity 251 known anomalies for this CCM release.

Auto-detecting drivers

You must enable SNMP and FTP in the device to auto-detect and configure Contivity devices in CCM.

Bandwidth Management—Bandwidth Filter IP addresses

On the Bandwidth Management > LAN Root Class > LAN > Bandwidth Filter page, CCM allows you to configure incorrect Destination and Source IP Addresses and Destination and Source Subnet Masks, and does not give an error message. The Destination and Source IP Addresses should not begin with 0, 224, or 255. The Subnet Mask fields must begin with 128, 192, 224, 240, 248, 252, 254, 255 (with the exception of the special case 0.0.0.0). You can also configure incorrect values in the WAN Root Class > WAN > Bandwidth Filter node and CCM does not give an error message. (Q01227162)

Bandwidth Management—duplicate LAN or WAN classes

In CCM, in the Bandwidth Management > LAN or WAN Root Class node, you can create two or more LAN or WAN classes with the same name. No error message is given. (Q01239621)

Bandwidth Management—LAN or WAN Class Name

In the Bandwidth Management > LAN Root Class > LAN node, you can erroneously configure a LAN Class Name with special characters (for example, <, ?, ..) or leave the field blank. No error message is given, and the class will not be exported to the Contivity 251 device. The same applies to the WAN Class name. (Q01227135)

Bandwidth Management—LAN or WAN Class IP Addresses accept incorrect values

On the Bandwidth Management > LAN Root Class > LAN > Bandwidth Filter page, you can erroneously configure the Source IP Address and Destination IP address fields with an incorrect address, such as 0.0.0.1. No error message is given, and the class will be exported to the Contivity 251 device with the incorrect value. (Q01285720) (Q01285731)

Content Filter Keyword

In CCM, do not use trailing spaces in the Content Filter Keyword field. CCM erroneously allows you to enter trailing spaces and does not give an error message. The trailing spaces are not exported to the Contivity 251 device. (Q01290217)

Content Filter—Trusted User IP Range

In CCM, on the Content Filter > Trusted page, you can erroneously configure the From and To addresses of the Trusted User IP Range to be the same value. CCM does not give an error message. (Q01285709)

Maximum number of policies on Branch Office

CCM limits you to a maximum of 60 Branch Office policies on a given Branch Office. When you attempt to add a policy over the 60 policy maximum, the CCM progress window tracks the creation as in previous policies and reports the operation as Done instead of returning an error message. (Q00854677)

Static DHCP page appears when not supported

The Contivity 251 device does not support Static DHCP functionality, even though a Static DHCP page appears in the device. (Q00866208)

VPN—duplicate VPNs

In CCM, in the VPN > Branch Office Connections node, you can configure two connections with the same Name, My IP Address, Gateway Address, and Pre-shared Key. Although this is not allowed, CCM does not give an error message. (Q01236655)

Appendix A: Copy and Paste support for Contivity Devices

The purpose of this section is to identify supported and non-supported copy and paste functional areas in the CCM Client Configuration Data navigation tree. (Q01295034)

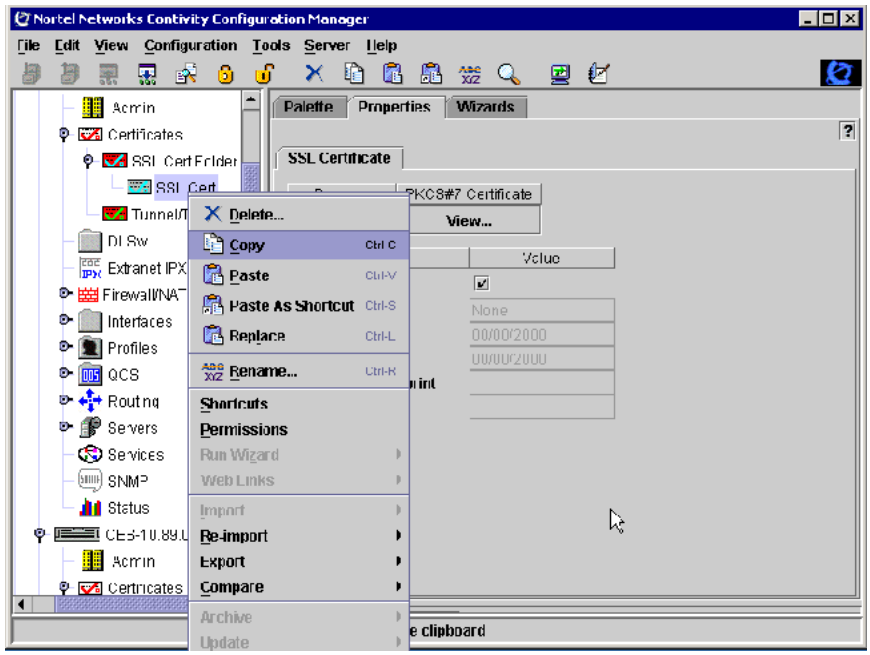
The copy and paste functionality can be categorized as either inter- or intra-device. Inter-device copy and paste means that an object from one Contivity device can be pasted into another Contivity device. Intra-device copy and paste means that an object can by copied and pasted to different elements within a single Contivity device.

Inter-device copy and paste support

CCM supports many copy and paste operations between devices. You can use the Configuration Data tree in the CCM navigation pane to copy, for example, certificates from one CES switch to another. The following example shows how to copy a certificate from one device to another.

Step	Action
1	In the CCM navigation pane, select a CES switch node and expand it.
2	In the **Certificates** node, expand the **SSL Cert** folder.
3	Select an SSL certificate and right-click. A drop-down menu appears.
4	Select **Copy**. See Figure 3 "SSL certificate copy" (page 45)

Figure 3
SSL certificate copy



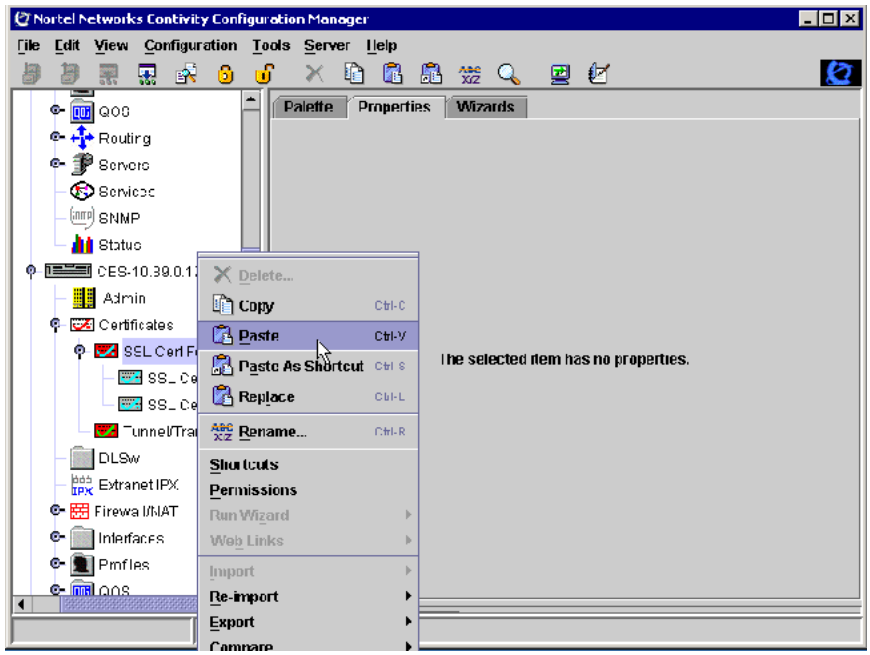
5 In the CCM navigation pane, select a new CES device and expand it.

6 In the **Certificates** node, select the **SSL Cert** node.

7 Right-click the **SSL Cert** node. A drop-down menu appears.

8 Select **Paste**. See Figure 4 "SSL certificate paste" (page 46)The certificate is added to the SSL Cert node.

Figure 4
SSL certificate paste



—End—

Supported device-to-device copy and paste operations

The following table summarizes which copy and paste operations are supported for device-to-device operations. All the objects in the table can be copied from one device and pasted into another.

Table 4
Supported inter-device copy and paste objects

Certificates > SSL Cert Folder > SSL Cert
Certificates > Tunnel/Transport > Trusted CA Certificate
Firewall/NAT > Policies > Network Objects > Network Group*
Firewall/NAT > Policies > Network Objects > New Host Definition*
Firewall/NAT > Policies > Network Objects > New IP Range Definition*
Firewall/NAT > Policies > Network Objects > New Network Definition*
Firewall/NAT > Policies > Service Objects > New ICMP Service*
Firewall/NAT > Policies > Service Objects > New IP Service*
Firewall/NAT > Policies > Service Objects > New TCP Service*

Firewall/NAT > Policies > Service Objects > New UDP Service*
Firewall/NAT > Policies > Service Objects > Service Group*
Profiles > Access Hours*
Profiles > Branch Office Connections > Groups
Profiles > Branch Office Connections > Connections
Profiles > Client Policy
Profiles > Domain Sets*
Profiles > Filters > Interface Filters > Current Filters*
Profiles > Filters > Tunnel Filters > Current Filters*
Profiles > Filters > Interface Filters > Rules
Profiles > Filters > Tunnel Filters > Rules
Profiles > Groups and Users > Groups (empty groups only)
Profiles > Map Class*
Profiles > Networks
QoS > Classifiers > Current Multi-Field Classifiers
QoS > Classifiers > Classifier Rules
Routing> Access List > Access List
Routing > BGP > Route Maps
Routing > BGP > Route Maps > Route Map
Routing > BGP > Route Reflector
Routing > BGP > Networks
Routing > BGP > Networks > Network
Routing > BGP > Neighbors
Routing > BGP > Neighbors > Neighbor
Routing > BGP > Community Lists
Routing > BGP > Community Lists > Community List
Routing > BGP > AS-Path Access Lists
Routing > BGP > AS-Path Access Lists > Access List
Routing > Interface Groups*
Routing > OSPF > OSPF Area (unless IP Address conflicts)
Routing > VRRP > VRRP
Servers > DHCP Servers > DHCP Pool

* Unless name conflicts

Supported device copy and paste operations

In the CCM navigation pane, you can copy and paste a CES device. Select the device, copy it, select Configuration data, and paste. A copy of the device appears in the navigation tree. Change the IP Address of the new device to differentiate it from the copied device..

Non-supported device-to-device copy and paste operations

The following table summarizes which copy and paste operations are not supported for device-to-device operations. For these objects, create a new object from the Palette and configure as required.

Table 5
Non-supported inter-device copy and paste objects

Profiles > Groups and Users > /Base > Users
Routing > Interfaces > Interface

Supported whole-device copy and paste operations

In the CCM navigation pane, you can copy and paste a CES device. Select the device, copy it, select Configuration Data, and paste. A copy of the device appears in the navigation tree. However, this functionality is not supported for the C221 and C251 devices.

Intra-device copy and paste support

Intra-device copy and paste refers to copying an object from a device and pasting within the same device (device-within-device). There are many objects in CCM that can be copied after changing certain parameters, such as the name or the IP address of a field.

Supported device-within-device copy and paste operations

The following table summarizes which copy and paste operations are supported for device-within-device operations.

Table 6
Supported device-within-device copy and paste

Certificates > SSL Cert Folder > SSL Cert
Certificates > Tunnel/Transport > Trusted CA Certificate
Interfaces > Backup Interface Service > Backup Interface
Interfaces > Dial on Demand > Demand > Remote Network
Interfaces > Dial on Demand > Demand (if Remote Networks are defined)
Interfaces > LAN Interface LAN > IP
Interfaces > LAN Interface Slot * Interface *
Profiles > Branch Office Connections > Groups

Profiles > Branch Office Connections > Connections
Profiles > Client Policy
Profiles > Filters > Interface Filters > Rules
Profiles > Filters > Tunnel Filters > Rules
Profiles > Groups & Users > Groups (empty groups only)
Profiles > Networks
QoS > Classifiers > Current Multi-Field Classifiers
QoS > Classifiers > Classifier Rules
Routing > Access List > Access List
Routing > BGP > Route Maps > Route Map
Routing > BGP > Networks > Network
Routing > BGP > Neighbors > Neighbor
Routing > BGP > Community Lists > Community List
Routing > BGP > AS-Path Access Lists > Access List
Routing > VRRP > VRRP
Servers > DHCP Server > DHCP Pool

Non-supported device-within-device copy and paste operations

The following table summarizes which copy and paste operations are not supported for device-within-device operations. For these objects, create a new object from the Palette and configure as required.

Table 7
Non-supported device-within-device copy and paste operations

Firewall/NAT > Policies > Network Objects > Network Group
Firewall/NAT > Policies > Network Objects > New Host Definition
Firewall/NAT > Policies > Network Objects > New IP Range Definition
Firewall/NAT > Policies > Network Objects > New Network Definition
Firewall/NAT > Policies > Service Objects > New ICMP Service
Firewall/NAT > Policies > Service Objects > New IP Service
Firewall/NAT > Policies > Service Objects > New TCP Service
Firewall/NAT > Policies > Service Objects > New UDP Service
Firewall/NAT > Policies > Service Objects > Service Group
Interfaces > Backup Interface Service > Circuitless IP
Profiles > Access Hours
Profiles > Domain Sets

Profiles > Filters > Interface Filters > Current Filters
Profiles > Filters > Tunnel Filters > Current Filters
Profiles > Groups and Users > Users
Routing > BGP > Route Maps
Routing > BGP > Route Reflector
Routing > BGP > Networks
Routing > BGP > Neighbors
Routing > BGP > Community Lists
Routing > BGP > AS-Path Access Lists
Profiles > Map Class (only for default (blank name) classes)
Routing > Interface Groups (only for default (blank name) classes)
Routing > Interfaces > Interface
Routing > OSPF > OSPF Area

CCM

Contivity Configuration Manager 2.3 Release Notes

Publication: 315768-F
Document status: Standard
Document version: 01.01
Document date: March 2006

Printed in the United States of America