2.2

Part No. 315768-D Rev 00
December 2004

600 Technology Park Drive
Billerica, MA 01821-4130

Contivity Configuration Manager v2.2 Driver Release Notes

NORTEL NETWORKS™

Copyright © 2004 Nortel Networks

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, Contivity, Contivity 221, Contivity Branch Access, Instant Internet, and Contivity Configuration Manager are trademarks of Nortel Networks.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

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

New features in this release

CCM 2.2 v. 4.9

New features in CCM 2.2 v.4.9 include:

- Contivity Security Accelerator Card — A card supported by Contivity 5000. Support includes increased encryption throughput, improved compression performance, 3DES and AES-128 support in hardware, ISAKMP and IPsec encryption key generation for Group 1, 2, and 5, and True Random number generation. You can find card configuration information on the Properties > Accelerator tab.
- Advanced Encryption Standard (AES) for User Tunnels — An enhancement to the Contivity Advanced Encryption Standard feature. Contivity has supported AES-128 for Branch Office tunnels, and the Contivity VPN Client (CVC) has supported DES and 3DES. This enhancement adds AES-128 and AES-256 support for Client Tunnels in Contivity and CVC. Use of AES-128 for IPsec encryption and IKE Encryption with Diffie-Hellman Group8, Group5, and Group2 is now allowed. In addition, use of AES-256 for IPsec encryption and for IKE Encryption with Diffie-Hellman Group8, Group5, and Group2 is now allowed.
- Gigabit Ethernet Fiber & Copper — Provides configuration support for the Contivity 5000 onboard LAN ports, the 1000 BASE-SX PCI interface card, and the 1000 BASE-T PCI interface card.
- 802.1Q Interface VLAN — Routes traffic between Virtual Local Area Networks.
- Configurable MTU and TCP MSS Clamping — Supports configurable Physical Interface MTU, configurable effective tunnel MTU for IPsec, configurable effective MTU PPP for L2TP, L2F, and PPTP, ICMP RFC compliance, TCP MSS Clamping per interface, and DF Bit behavior compliance with RFC 2401.
- QoS Guarantee Bandwidth for each Application — An enhancement to Contivity QoS, which provides the option of dropping data that exceeds configured Traffic Conditioning Assured Forwarding rates. With this enhancement, Contivity now supplies guaranteed bandwidth based on Diffserv code points, enabling the customer to offer a service that guarantees a fixed percentage of total bandwidth to each of several applications.
- Internal DHCP for IP Address Pools — A default pool can be used to provide addresses when the preferred pool is exhausted or unavailable. The default fail

over control enables/disables use of the default pool. Named pools are also supported. The pool name for the user/group profile can be used to select which of the internal DHCP Server's pools a local address comes from.

CCM 2.2 v. 5.0

New features in CCM 2.2 v.5.0 include:

- 1750 platform supported
- Inverse Split Tunneling — Provides capability to enable or disable Inverse Split Tunneling on a per-group basis, and to control the networks to which the inverse split tunneling allows access to outside of the tunnel.
- LDAP special character—Provides configuration support needed for allowing certificate subject DNs to be created that include previously not allowed special characters, such as a comma.
- IPsec Mobility—Provides configuration support for enabling and disabling IPsec Mobile. Also provides configuration for enabling and disabling Mobile IPsec Persistence as well as configuration for Roaming Time and Session Persistence Time parameters.
- Data Link SWitching (DLSW) — Provides a standards-based mechanism for reliably transporting connection-oriented Systems Network Architecture (SNA) and Network Basic Input/Output System (NetBIOS) data across a network. DLSW can be accessed only if a valid key is installed.
- LDAP proxy enhancement — Provides configuration support for advanced setup for User Certificate Access.
- Dynamic Administrator Password Authentication — Provides dynamic password support for administrative users. When enabled, administrative users are forced to authenticate via RADIUS which, if configured, can then forward authentication credentials to a dynamic password authentication system. The Administrative Privileges tab under Profiles > Users contains the enabling checkbox.

CCM 2.2 Release

This document lists Contivity, Contivity 221*, Contivity 251*, and Contivity Branch Access* (formerly Instant Internet*) configuration features that are not supported in Contivity Configuration Manager release v2.2. Configure these

features by using the embedded interfaces available for these devices: Web UI and CLI for Contivity, Contivity Branch Access Setup/Admin Tool, or CLI.

This document also recommends usage processes that help users to avoid issues in configuring the supported devices using CCM.

Contivity Configuration Manager supports the Contivity 4.9x (partial features), Contivity 5.0x (partial features), and the Contivity Branch Access 7.2 device (formerly Instant Internet), the Contivity 221 device and the Contivity 251 device. The version is 2.1 for Contivity 221 and 251.

CCM 2.2 is compatible with Contivity v4.55 and Contivity 4.75. However, it does not provision the following features added in these releases:

- Critical Interface Group
- OSPF totally stubby areas
- Configure OSPF Area Ranges for the backbone area
- Support for RADIUS Accounting Messages over public interface
- UDP Port as RADIUS Message Source

Note: When referencing a device, the device model is called out when an issue applies specifically to that model.

CCM 2.2 is compatible with Contivity v4.9 and Contivity 5.0. However, it does not provision the following features added in these releases:

- 4.9 features not supported:
  - ABOT with DNS
  - ADSL
  - ADSL RIP /OSPF Enhancement
- 5.0 features not supported:
  - QUAD T1/E1
  - FW/NAT SIP AGL Enhancement
  - Entrust Key Update for Bell Canada

Power Tools Summary

Backup and Restore Tool

The Backup and Restore tool (BNR) provides a central place for the storage and full control of the backup and restore operations for each of your Contivity devices.

Before BNR, you configured the backup of each of your Contivity devices individually. You specified backup server information and set up the schedule device by device. It was difficult to monitor the progress of backups, and to verify that backups were completed.

BNR gives you control, storage, and monitoring capability for your Contivity device backups from a convenient location. You can also restore select machine configurations easily.

Most people run BNR from a single PC that can connect to all of their Contivity devices. This PC (or more than one PC, as multiple BNR PCs can be used for redundancy) is usually located at the Network Operations Center (NOC). In BNR you do the following:

- define your devices (IP and Login information)
- create one or more backup plans
- place each of your VPNs into one or more of these backup plans

Each backup plan defines the backup type and schedule for each Contivity device it backs up. Backups can be scheduled every hour, day, week, or month. A backup can save either configuration data or it can be a full system backup.

For instance, you can have one backup plan that backs up configuration data every morning at 2am, and another backup plan that performs full system backups at 6pm on the first of every month. You can reduce the network load by staggering backup plans. If, for example, you have 1000 Contivity devices to back up, you could break the backups into smaller groups of 100 that are scheduled to run every hour overnight.

BNR provides a means to restore Contivity device configurations. The restore can occur immediately or according to schedule. For instance, you may specify that a VPN in Miami and another in Huntsville need their configurations restored on

Thursday night at 11:15pm. The restore operation will complete automatically at that time.

Firewall Policy Manager

The Firewall Policy Manager (FPM) tool for Contivity provides a way to configure all the firewall policies of your Contivity devices from a central location. If you need to add a rule to permit, prevent, or control a certain type of communication on a large number of your Contivity devices, you can do that from a single location in one step.

In the past, you managed each of your Contivity devices individually and separately. By using FPM you can:

- import (get) policies from select Contivity devices
- modify these policies and use them as model firewall policies that you can export (send) to many Contivity devices in a single action
- group your devices so that certain devices get certain firewall policies while others can be given a different set of firewall policies

You can specify the order that the policies are to be applied and all particulars of the rules in the policies, just like you can on a Contivity device. As you identify more vulnerabilities and dangers, you can use FPM to define and protect your intranet from them easily, logically, and rapidly.

Usage Recommendations

Enabling wizards

In order to run wizards, the network administrator must grant users access to the wizards by setting the functional security tab. For more information on functional security, see the Contivity Configuration Manager Administration Guide.

Start server

When starting the CCM server for the first time after installation, the server must be running and the database fully initialized before you can run any operations from the server menu.

Before using CCM

Certain features of devices should be activated before using CCM to configure these devices:

For Contivity configurations using any access mode

Since CCM relies on FTP to send configuration instructions and to collect the results, enable FTP on the Contivity before using CCM. This is applicable to any access mode (private network, branch tunnel, control tunnel) you may use. Note that by default FTP is disabled for Contivity devices. To enable this protocol, use the Services > Available menu options from Contivity Web UI.

For Contivity configurations using Branch Office access mode

In this access mode, FTP Management should be enabled on the appropriate tunnel filter. To configure this feature from the Web UI, select Profiles > Filters > Edit Tunnel Filter (choose 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, SNMP should be enabled before using CCM. To enable this protocol, use the Service > Available menu options from 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. You can do this by using the Admin > SNMP menu options from Contivity Web UI.

For information on SNMP for Contivity Branch Access, see page 27.

FIPS (applicable to FIPS-certified products only)

CCM can manage products running in FIPS mode as long as management is through a tunnel. To configure via the Web GUI, see Profiles > Filters > Allow Management Traffic > For These Local Services.

License Keys

CCM gets the installed status of the keys during import. Depending on whether the keys are installed on the Contivity before the import, CCM displays “Key Installed” or “Key Not Installed” under the Admin > Install Keys Status tab.

As an off-line configuration tool, CCM permits the configuration of these features in the CCM database without a license key. However, in order for the exported configurations to take effect, a license key must be obtained and installed on the box.

Features requiring 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

Certificates

Configuring a CA certificate

CCM supports the CA certificate configuration in the following form: to configure a CA certificate, you should first obtain a PKCS#7 Base-64 Certificate encoding from the CA Authority either using their web site or through an e-mail. This PKCS#7 Base-64 Certificate encoding will must be pasted 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 encoding, 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 the SSL certificate configuration in the following form: To configure an SSL certificate, you should first obtain a PKCS#7 Base-64 Certificate encoding from the CA Authority either using their web site or through an e-mail. This PKCS#7 Base-64 Certificate encoding will must be pasted 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 encoding, you must import the certificate into CCM. You can use the same string for any number of devices.

Operations with server certificates

CCM, being an off-line configuration tool, 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. CCM enables you to delete the Server certificates from CCM when they are no longer needed. To generate a Server certificate using Web/GUI, do the following:

1. On the Web UI, under System > Certificates, click the PKCS#10 Certificate Request tab.
2. Enter the required information and get the encrypted string generated by the Web UI.
3. Send this information to the CA Authority using Authority web site or e-mail.

   CA Authority generates PKCS#7 Base-64 Certificate encoding based on the data that is received.
4. On the Web UI, navigate to the Import Tunnel or Transport Certificate tab and select Server Certificate. Paste the encoding in the window.
5. Click OK to get the Server certificate.

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

General note regarding certificates

CCM cannot be used for certificates storage. If a certificate-populated Contivity image exists in CCM and the certificates are deleted on the Contivity either manually or by applying factory defaults, exporting the CCM image will 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, there may be group login conflicts.

Exports

Exporting new users

CCM does not support creating users with both IPSec Username/Password and CA certificates authentication methods when internal LDAP is being used.

Exports with users using CA certificates

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

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 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)

In addition, Service Object names must start with an upper- or lower-case alphabetic character."

Wizards

When you cancel the CCM Version Management wizard during an upgrade operation, the server may take several minutes to process the cancellation. During this time, the server does not respond to any requests. (CR Q00809277)

External LDAP

While the CCM 2.1 driver supports configuration of internal and external LDAP servers on Contivity devices, there are several caveats. First, any change of the LDAP server (Internal to External, External to Internal, or one External to another External) must be made independent of any other changes in CCM. This means that an export containing LDAP server changes must not include any other configuration change.

Also, great care must be taken to ensure that all boxes using the same LDAP server are kept current in CCM. If changes are made to an LDAP server (for example, Users are added), all devices in CCM that use this server must be re-imported 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 will 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 preforming an export. Doing so can cause the switch to malfunction.

Timeout values for import operations

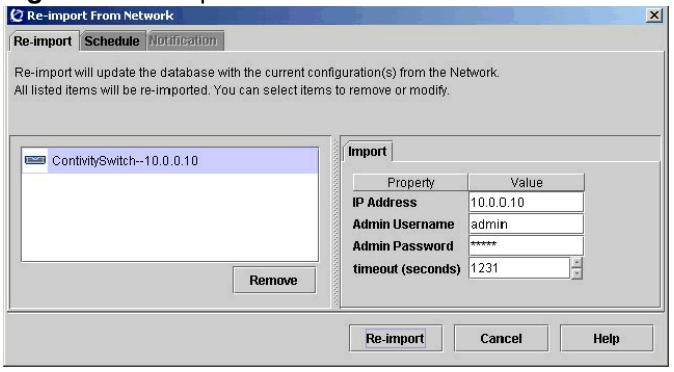
When importing branch office configurations, you can adjust the value of the timeout parameter. The current default is 20 minutes (1200 seconds), which should be sufficient for importing 200 branch offices. However, if you have more than 200 branch offices, you should increase this number. If you have fewer than 200 branch offices in your configurations, you can decrease this number since you will not need such a long timeout interval.

The timeout value is the total time allowed for sending and executing all import instructions and retrieving the results off the box. If the timeout value is exceeded during an operation and the all of the results have not been found, the operation fails. If all results are found before the timeout, the operation may continue past the timeout value. This value does not cover the time it may take to negotiate the FTP session, parse the result files, or populate the database. This value does apply partially to exports, as an import is currently required for export. You must ensure the timeout specified on the import tab is valid for the configuration before exporting.

Input to the data entry field

In order for data to take effect, the focus should be moved from the data entry field (the cursor moved to a different field, the enter key pressed, a different tab selected, and so on). This step typically occurs during the natural flow of operations. However, there is one operation in which, if you change the timeout value for re-import operations, you must change the focus before clicking the re-import button (see Figure 1 on page 20). Otherwise, the operation is performed using the old timeout value.

Figure 1 Re-import from network



Order of rules in Tunnel Filters

The way to re-order 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.

FTP or Telnet not responding

If you are using a Contivity version earlier than 3.65 and the device has more than 100 branch offices, FTP or Telnet on the Contivity device may become unresponsive when you are using CCM. The solution for this issue is implemented in Contivity release V03_65.11. If you are using an earlier version, you should not configure more than 100 branch offices with CCM. Contivity versions 3.65 and higher do not exhibit this problem.

Deleting Groups

To delete a group (Profiles > Group), you must make sure that it is not in use in CCM or on the Contivity box itself. For example, if CA certificates or Radius Authentication were to refer to a group, CCM would not be able to delete this group correctly.

Recommended number of Groups and Users

Nortel Networks has verified that up to 10 000 users in any combination up to 600 groups will work as expected.

Deleting scheduled re-imports

In order to delete a scheduled series of re-imports in CCM, select Scheduler > Network Reimport > Properties tab. From the Properties tab, select the Schedule tab and deselect the “and repeat every” checkbox.

Known Anomalies in CCM 2.2

The following section lists the known anomalies related to CCM 2.2:

- Power tools
  - — FPM
  - — BNR
- Contivity
- Contivity 221
- Contivity 251
- Contivity Branch Access

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

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

FPM — Cannot be started from CCM web client

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

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” is a FPM permitted name. The Contivity 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”. (CR Q01037999)

FPM — Support for Contivity devices

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

FPM — User Authentication Group

Currently FPM restricts the User Authentication Group names field. FPM allows the following:

- Present a list of group names in all devices in the device list, so that you can choose the group value
- Allow off-list entry of a group name
- Warn you if the name entered is not a group name in any of the devices listed in the device list

FPM — Add device

You can add the same device to FPM many times, if you specify the IP Address and different DNS names. This is not recommended.

BNR — Add device

You can add the same device to BNR many times, if you specify the IP Address and different DNS names. This is not recommended.

BNR — Cannot be started from CCM web client

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

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

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

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:

- switching backup to another disk
- reducing the number of backups that are retained
- changing some backups from Full to Configuration
- using an additional machine to perform some backups
- moving some Contivity backup support to a new machine (CR Q1032690)

Alpha-numeric password required

Users must enter the alpha-numeric password even when PasswManagement is disabled. When a group's connectivity parameters has the Alpha-Numeric Password Required: switch set Enabled, CCM requires alphanumeric passwords, even if the Password Management switch is Disabled. To bypass this issue, set the Alpha-Numeric Password Required switch to Disabled when the Password Management switch is Disabled. (CR Q01034999)

Data Link SWitching (DLSW) — Protocol changed

The Protocol is changed from SDLC to PPP when you enable and disable DLSW. (CR Q01026746)

Firewall checkbox

If you have a Contivity Stateful Firewall license key installed, you can turn off the Contivity Firewall checkbox by deselecting the Contivity Firewall checkbox. However, if you do not have the license key installed, the only way to turn off the Contivity Firewall is to check the No Firewall checkbox.

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. (CR 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. (CR Q00968798)

Route Policy — Status disabled

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

Third administration authentication server not exported

If you have defined a third server for administration authentication on a Contivity device and then choose a different value for the third server under CCM, the third server is not exported. When you attempt to export the configuration from CCM to the device, the value does not export. (CR Q00992850)

Factory reset

When you reset the Contivity v4.75 to its factory defaults 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 will show the correct values. (CR Q00783129)

Default dial interface import

When using 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 will 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 will prevent the error message from being displayed.

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. (CR Q00767922)

Export error messages

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

Subject DN Type import

When you import a Contivity device's branch office connection with a defined DNS Name type Subject DN to CCM, the type does not import correctly. The type that appears in CCM following an import is different than what is on the Contivity device. (CR Q00772580)

Syslog forwarding error

When you use CCM to configure syslog forwarding, and change the UDP port to an out of range value, CCM resets the port number back to the old value, but does not send an error message. (CR Q00749229)

New groups

When you create a new group, give the group a name before you create any users or subgroups under it. If you create users or subgroups in this new group before it has a name, the user records will not export to the Contivity device and the group name will change to "default" and will not be changeable unless you move the user records to another named group. If the user record is not being exported, copy the record to another group and then export. (CR Q00823742)

Copying Branch Office Tunnels

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

Private interface IP address changed when VRRP configured

If VRRP is configured and enabled on an interface, you should be unable to change the private interface IP address. However, CCM allows the change to take place without generating an error message. (CR Q00733856)

Tunnelguard wizard

The Tunnelguard wizard cannot copy policies with rule expressions containing "and/or." All of the rules in the expression must be defined on the target device for the wizard to copy rules with "and/or" expressions. (CR Q00778311)

User accounts lost on export

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

Branch Office control tunnel connections

When creating a Branch Office control tunnel connection, check the control tunnel checkbox before entering a name for the tunnel. If you enter a name before deciding that the connection should be "control", the control tunnel checkbox will be greyed out and unavailable for configuration. You will have to delete and then add the connection again to configure. (CR Q00779954)

Report wizard

When you use the Report wizard to generate System reports in CCM, CCM displays and logs an erroneous fatal error message. The wizard completes the report, but displays the message anyway. (CR Q00758266)

Canceled image send operations

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

Reporting feature in CBA Multi-Device wizard

The reporting feature is currently unavailable in the Multi-Device Configuration wizard. (CR Q00663455)

Syslog Filter Facility has two “All” entries

The drop-down list for Syslog Filter Facility contains two choices for “All.” (CR Q00741399)

Changing QoS

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

Changes to Profiles > Network causes tunnel to bounce

When you make a change to Profiles > Network, the tunnel is bounced when the new configuration is exported. (CR Q00753177)

QoS>Interfaces — different default values

In the QoS>Interfaces there are different default values for some Non-Tunnel Traffic ratings than the Contivity shows. (CR Q01026767)

Optimized 4.8

If you attempt to use the Version Management wizard to load an optimized version of Contivity 4_80.124, you will not be able to select the file. Instead, expand the non-optimized version of 4_80.124 and then point the Version Management wizard to the directory that contains all of the files. (CR Q00819518)

License Key wizard

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

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.

LDAP delimiter character

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

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 rejects the rule upon export. (CR Q00770145)

DHCP standard options

On rare occasions, DHCP standard options will 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.

Web Server enabling error

The CCM Web Server cannot be enabled against a port that is already enabled. However, CCM does not display an error message when this occurs. Should you attempt to enable the Web Server against a port that is already enabled, the Web Server Enabled checkbox unchecks itself without giving an error message to the user. (CR Q00739993)

Known Anomalies in Contivity 221

Static Route entries

Contivity 221 allows you to have two static route entries with the same name. However, CCM 2.1 does not allow two static route table entries to have 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 work without problems if all static route entries have different names.(CR 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 alpha-numeric characters when naming routes.(CR Q00915420)

Static DHCP addresses

CCM accepts static DHCP addresses that are not in the range of the DHCP pool, despite displaying a warning message containing pool ranges. (CR Q00783772)

Importing VPN policies

CCM 2.1 only imports the first 10 IP policies configured for a particular VPN Branch Office connection, even though up to 60 policies can be configured. (CR Q00809419)

Failsafe for locked processes

When a CCM process locks at a certain percentage during an operation, a timeout message should appear that would allow the hung process to automatically finish. (CR Q00806392)

Parameters for VPN Branch Office

When setting parameters for a VPN Branch Office, if NAT Traversal is enabled and AH protocol is selected, the Encryption selection drop-down will be disabled. To re-enable the Encryption drop-down, disable NAT Traversal and set protocol to AH. Then set protocol to ESP and enable NAT Traversal. (CR Q00820465)

When defining parameters for a VPN Branch Office Connection, do not specify Null encryption for Phase 1 on the Advanced tab for the branch office. Although this option is offered in CCM, Contivity 221 does not allow it. (CR Q00820458)

Gateway

CCM erroneously allows you to enter a gateway that is not located on a directly connected network. The Contivity 221 device does not allow this and disallows the entry. (CR Q00798965)

SUA NAT address mapping

Importing or exporting SUA NAT address rule mapping can cause an error to be generated. However, the configuration functions properly despite an error log being generated. (CR Q00820463)

SUA Server

Do not specify a port mapping for port 1026 in the SUA Server table. If you map to this port or have a port map range that includes port 1026, the Contivity 221 device disallows this port and reports a “server ports duplicate” error. (CR Q00794401)

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. (CR Q00783705)

CCM and Web GUI

When configuring devices it is not advisable to switch between CCM and the Web GUI interface. Complete each configuration tasks using one or the other, but not both. (CR Q793815)

Changing service objects

To properly make changes to service objects or service names in CCM, you should 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. (CRs Q00951897 and Q00951918)

Known Anomalies in Contivity 251

Auto-detecting drivers

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

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, allowing you to effectively 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 re-arranging easier. (CR Q00857737)

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.(CR Q00915420)

Special characters and Firewall Service Objects

In CCM, the Name field in Firewall > Service Objects erroneously accepts special characters such as (), Â, ¶, ¥, §, ®, µ, ¹, etc. Do not enter a name containing any of these characters, as the Contivity 251 does not support them. Use only alpha-numeric characters when naming service objects. (CR Q00948684)

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. (CR Q00948855)

Static Routes Gateway IP Addresses

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

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. (CR 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. (CR Q00866208)

Content Filter Keyword field

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

Changing firewall service object

If you remove a service object from a rule AND delete a service object from a device and then export your changes from CCM, the export operation fails. The operation fails when both criteria above are met. If this operation fails, simply export a second time and the operation should succeed. However, if you make only one of the changes above, the export is successful on the first attempt. (CR Q00952560)

Known Anomalies in Contivity Branch Access

SNMP for Contivity Branch Access Auto-detect

Since auto-detect in CCM relies on SNMP to discover Contivity Branch Access devices before importing their configurations from the network, SNMP should be enabled before using CCM.

Two SNMP parameters regulate the SNMP behavior of Contivity Branch Access: *snmpd* deals with SNMP proper and *snmp* handles SNMP traps. For auto-detect to work properly, *snmpd* must be enabled.

Telnet for Contivity Branch Access configurations

CCM relies on Telnet to configure Contivity Branch Access devices. For that reason, Telnet should be activated in the devices before trying to configure them using CCM. To enable Telnet from the Contivity Branch Access Setup/Admin Tool, select Support > Service. Enable “Telnet” and restart Contivity Branch Access for the change to take effect.

Default routes

CCM supports one default route. If more than one default route is configured, only the first one will be imported by CCM. To configure more routes, use the static routes option.

Importing from Add List

If you want to import a Contivity Branch Access device using the Add List functionality in CCM, you may need to enter a password for the device or the operation may fail. For example, if the Contivity Branch Access device does not have a password, you can import from Add List with no problems. However, if the device has a password and you attempt to import from Add List without entering the password, the operation will fail.

In order to import from Add List, enter the information (IP address, community string, timeout) in the Add to List box as normal. Before you click the Import button, specify a password for each device in the list in the left-hand pane. Click Import when finished.