2.2.1

Part No. 315768-E Rev 00
August 2005

600 Technology Park Drive
Billerica, MA 01821-4130

Contivity Configuration Manager v2.2.1 Release Notes

NORTEL

Copyright © 2005 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

CCM 2.2.1 Release Notes

This document does the following:

- lists the books without changes for the CCM 2.2.1 Release
- lists the books with changes for the CCM 2.2.1 Release
- describes the new features for the CCM 2.2.1 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*
- describes document corrections for the next release of CCM

This document also lists Contivity, Contivity 221*, Contivity 251*, and Contivity Branch Access* (formerly Instant Internet*) configuration features that are not supported in Contivity Configuration Manager release v2.2.1. Configure these features by using the embedded interfaces available for these devices: Web User Interface (UI) and Command Line Interface (CLI) for Contivity, Contivity Branch Access Setup/Admin Tool, or CLI.

Contivity Configuration Manager supports the Contivity CES version 4.90 and 5.00, and the Contivity Branch Access version 7.20 device (formerly Instant Internet), the Contivity 221 version 2.1, and the Contivity 251 version 2.1.

CCM 2.2.1 is compatible with Contivity v4.55 and Contivity 4.75. However, CCM 2.2.1 does not provision the following features:

- Configure OSPF Area Ranges for the backbone area
- Critical Interface Group
- Open Shortest Path First (OSPF) totally stubby areas
- Support for Remote Authentication Dial-In User Service (RADIUS) Accounting Messages over public interface
- UDP Port as RADIUS Message Source

Note: Some issues apply to a single device model.

Books included in this release

The following books are not changed for the CCM 2.2.1 Release:

- Installing Contivity Configuration Manager (314789-E)
- Contivity Configuration Manager 2.2 User Guide (314790-D)
- Contivity Configuration Manager Administration Guide 2.2 (314792-D)
- Using Contivity Configuration Manager to Configure Contivity Branch Access (315769-B)
- Contivity Configuration Manager Tool Set 318759-A
- Using Contivity Configuration Manager to Configure Contivity 221 317747-A
- Using Contivity Configuration Manager to Configure Contivity 251 318128-A

The following books are updated for the CCM 2.2.1 Release:

- Using Contivity Configuration Manager to Configure Contivity (315227-E)
- Contivity Configuration Manager Wizards (320517-A)
- Installing Contivity Configuration Manager 2.2.1 (31828-B)
- Contivity Configuration Manager v2.2.1 Release Notes (315768-E)
- Contivity Configuration Manager 2.2.1 License (314906-F)

Note: The on-line Help system does not contain the new feature information for the 2.2.1 release. The updated books in the list above cover the new feature support that was added for this release (2.2.1).

New features in CCM 2.2.1 release

The following are the new features for this release:

- Asymmetric Digital Subscriber Line (ADSL)

ADSL is a technology that allows more data to be sent over existing copper telephone lines. ADSL supports data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate). ADSL requires a special ADSL modem.

CCM 2.2.1 provides support for the ADSL card through the addition of the ATM Interface-Slot, and the ATM Virtual Circuit elements added to the Configuration Data tree. This feature is supported in CES V5.00 and later.

- Asynchronous Branch Office Tunnel (ABOT) DNS

  The Asynchronous Branch Office Tunnel (ABOT) Domain Name Server (DNS) feature allows the user to insert a DNS name instead of an IP address on an IPsec tunnel for an Initiator tunnel type. This feature is supported in CES release V5.00. This feature is not supported for Responder or Peer-to-Peer tunnel, and L2TP or PPTB ABOTs. This feature is supported in CES V5.00.

- Configuration option for Link Control Protocol (LCP) echo

  The Link Control Protocol (LCP) is used to automatically agree upon the encapsulation format options, handle varying limits on sizes of packets, detect a looped-back link and other common configuration errors, and terminate the link. This feature allows the PPTP user to manage and debug a link. It is supported in CES V5.00 and later.

- Entrust Key Update

  This feature provides support for Certificate Authority (CA) certificates. The start and end dates are now displayed for the CA certificates. This feature is supported in CES V5.00 and later.

- Firewall/NAT Session Initiation Protocol (SIP) Application Level Gateway (ALG) enhancement

  The Firewall folder has the NAT enhancement added in order to support the NAT ALG for SIP. This feature is supported in CES V5.00.

- IP Address Release Time

  The IP Address Release Time feature enables you to set a blackout interval for remote users. You can apply the blackout interval to DHCP and/or the address pool. This feature is supported in CES V5.00.

- Quad T1/E1

This CCM feature supports the four-port T1/E1 card interface with the integrated Channel Service Unit/Data Service Unit (CSU/DSU). This feature is supported in CES V4.9.

- Tunnel Guard Agent Minimum Version

  The Tunnel Guard Agent Minimum Version Field feature allows you to specify a required minimum version of the tunnel guard agent. This feature is supported by V 4.9. For Groups other than /Base, a Use Inherited checkbox is available.

Usage recommendations

This Usage Recommendations section provides steps that help you avoid issues when configuring the supported devices of CCM. The following is a list of the usage recommendations:

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 the following devices:

For Contivity configurations using any access mode

Since 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 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 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 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 Contivity Web UI.

For information on SNMP for Contivity Branch Access, see page 38.

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 through the Web GUI, see Profiles > Filters > Allow Management Traffic > For These Local Services.

CCM 221 SUA/NAT

In the 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 are making any changes to a device configuration, if you leave any required fields without good values, the fields appear Yellow or Red. This means that the information related to that incomplete field will not be exported to the device.

Certificates

The following presents information on configuring various certificates.

Configuring a CA certificate

CCM supports the Certificate Authority (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 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 Secure Sockets Layer (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 their web site or through an e-mail. This PKCS#7 Base-64 Certificate encoding 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 retrieve the encrypted string generated by the Web UI.
3. Send this information to the CA Authority using the 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 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, there may be Group login conflicts.

Deleting Groups

Before deleting a Group (Profiles > Group), make sure that the Group is not in use in CCM or in the Contivity box. For example, if CA certificates or RADIUS Authentication is referring 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.

Exports

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 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 will 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)

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

FTP or Telnet not responding

Use Contivity release V03_65.11or 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.

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, take great care 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.

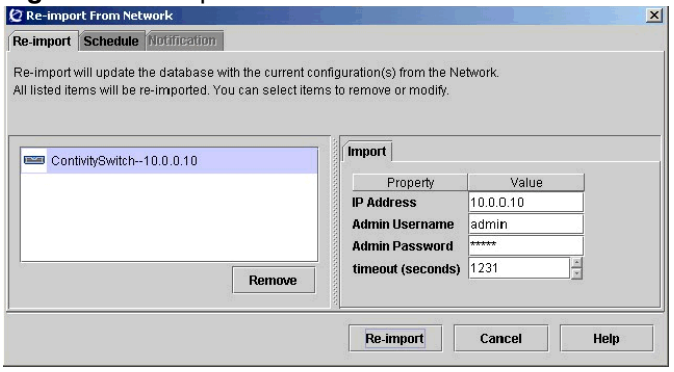
Additionally, when switching from one external LDAP server to another, you must click OK on the external LDAP server page to fully configure the new LDAP server. If you do not click OK and export the configuration, information under Profiles > Group will not reflect that of the new external LDAP server.

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 performing an export. Doing so can cause the switch to malfunction.

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 19). Otherwise, the operation is performed using the old timeout value.

Figure 1 Re-import from network



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 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

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.

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.

Resolved Anomalies in CCM

The following is a list of the resolved known anomalies in CCM:

Alpha-numeric password required

Users must enter the alpha-numeric password even when PasswManagement is disabled. When a Group connectivity parameter 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)

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)

Subject DN Type import

When you import a Contivity device 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)

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)

Resolved Anomalies in Contivity 221

The following is a list of the resolved known anomalies in Contivity 221:

Failsafe for locked processes

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

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)

Importing VPN policies

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

Parameters for VPN Branch Office

If NAT Traversal is enabled and AH protocol is selected when you set parameters for a Virtual Private Network (VPN) Branch Office, the Encryption selection drop-down list is disabled. To re-enable the Encryption drop-down list, disable NAT Traversal and set the protocol to AH. Then set protocol to Encapsulating Security Payload (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)

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)

SUA NAT address mapping

Importing or exporting SUA NAT address rule mapping can cause an error log 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)

Resolved Anomalies in Contivity 251

The following is a list of the resolved known anomalies for Contivity 251:

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 are met. If this operation fails, simply export a second time, and the operation will succeed. However, if you make only one of the changes described in this section, the export is successful on the first attempt. (CR Q00952560)

Special characters and Firewall Service Objects

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

Known Anomalies in CCM

This section lists the known anomalies related to CCM 2.2:

- Power tools
  - — Backup and Restore (BNR)
  - — Firewall Policy Manager (FPM)
- Contivity
- Contivity 221
- Contivity 251
- Contivity Branch Access

Backup and Restore (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 — Application does not run from CCM unless Contivity is imported

You must import your Contivity Device 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 — Cannot be started from CCM web client

BNR cannot be started from CCM web client. (CR 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:

- 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)

Branch Office control tunnel connections

When creating a Branch Office control tunnel connection, check 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. (CR 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. (Q1096899)

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. (CR Q00695376)

CCM 221 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. (Q01145086)

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 2.2.1 displays 2.2 in on-line help

After you upgrade from CCM 2.2 to CCM 2.2.1, 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 2.2.1, 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 2.2.1 (was at 2.2.0 in previous release)
- Branch Access is at version 2.2.1 (was at 2.2.0 in previous release)
- Contivity 221 is at version 1.2.0 (was at 1.1.0 in previous release)
- Contivity 251 is at version 1.2.0 (was at 1.1.0 in previous release) (Q1157666)

CCM 2.2.1 Installers do not support Upgrade for Oracle-based installations

The CCM 2.2.1 Installers do not support the installation and migration of Oracle-based CCM sites. Nortel does support installation and migration of Cloudscape-based CCM sites. Users who currently have CCM installed with an Oracle database can either; remain at the CCM 2.2 release until the next release, or users can call Nortel Customer Support for a manual upgrade procedure to step through the installation and migration from CCM 2.2 to CCM 2.2.1 (Q1164231)

CCM 251 network group object validation

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

CCM blank network group object

When a blank network object is exported, an error shows that says “The name already exists”. The blank network object then appears in the list of available network objects on CES. (Q1185782)

CCM duplicate any rule

CCM lets you create duplicate 'Any' rules. These rules are not exported. (Q1188400)

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 install/migrate Server over Oracle

When you setup the Net Service Name in Oracle on an Operating System registered to a domain, Oracle adds the domain name to the name you entered. This can affect database connectivity. (Q01164375)

CCM migration: some solaris systems migration freeze, if the database is not empty

There is an intermittent problem with the Solaris Installer. Cloudscape-based installations can hang during migration, and then the user must cancel from the installer. Therefore, the upgrade to v2.2.1 is unsuccessful.

In order to avoid Cloudscape-based installations from hanging during migration, do the following:

Log in as root, and enter the following command:

```
PATH=$PATH:.
export PATH
```

Note: This is a temporary setting. Do not retain the :. in your PATH variable by either exiting the shell, or logging off when you have completed the installation.

If you continue to have problems during the migration process, contact Nortel Customer Support for assistance. Nortel will provide a script and procedure for migration and upgrade for Cloudscape-based users. (Q01191638)

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. (Q1185797)

CCM Server installed-as-Service considerations

When you install the CCM Server as a service on your computer, store the CCM software on the same drive as your operation system. This is usually the C drive. If you put the software on a different drive, the service may not run. (Q01164311)

CCM uninstall

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

Changes to Profiles > Network causes tunnel to bounce

When you make changes to Profiles > Network and then export, there is a short loss of contivity. (CR Q00753177)

Changes to Quality of Service (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. (CR Q00818588)

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. (CR Q00778924)

Data Link Switching (DLSW) — Protocol changed

The Protocol is changed from SDLC to PPP when you enable and disable DLSW. (CR 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 will prevent 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. (CR Q00767922)

Dynamic Host Control Protocol (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.

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. (CR 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 will show the correct values. (CR Q00783129)

Find in CCM toolbar

Search button on the CCM toolbar does not find all values. (Q1183644)

Find in CCM toolbar (case issue)

Search button on the CCM toolbar is case sensitive. (Q1183630)

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 considerations for off-CCM server access

Anytime you run a server on a computer that also has a firewall, or for which there is 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(s) are defined to permit traffic to flow between Client and Server. (Q01164349)

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 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 an 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

FPM only supports Contivity devices running version 4.80 and higher. It only supports device models 1010 and higher. 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 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

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.

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. (CRs 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. (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)

NAT overflow

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

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 do not export to the Contivity device and the Group name changes to “default” and does 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)

QoS > Interfaces — different default values

In the QoS > Interface there are different default values for some Non-Tunnel Traffic ratings than those the Contivity shows. For example: The default value for interface LAN, Non-Tunnel Traffic Rating is 10 percent. The default value for public interface (SLOT 1), Non-Tunnel Traffic Rating is 90 percent.
(CR 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. (CR Q01025874)

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)

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 operations. (CR Q00730206)

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 check box clears itself without giving an error message to the user. (CR Q00739993)

Known Anomalies in Contivity 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. (CR Q793815)

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. (CRs Q00951897 and Q00951918)

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)

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 alphanumeric characters when naming routes. (CR Q00915420)

Known Anomalies in Contivity 251

The following are the known anomalies in Contivity 251.

Auto-detecting drivers

You must enable Simple Network Management Protocol (SNMP) and FTP in the device in order to auto-detect and configure Contivity devices in CCM.

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)

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)

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 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)

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. (CR 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.(CR 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, allowing you to 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)

Known Anomalies in Contivity Branch Access

The following are the known anomalies in the Contivity Branch Access.

Default routes

CCM supports one default route. If more than one default route is configured, only the first one is 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 need to enter a password for the device or the operation fails. For example, if the Contivity Branch Access device does not have a password, you can import from Add List. However, if the device has a password and you attempt to import from Add List without entering the password, the operation fails.

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

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, enable SNMP 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. Activate Telnet 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.

Document corrections

The following are the document correction for this release.

License versions

There are three license versions for CCM:

1 50 network elements

DM0021052-2.2 Contivity Configuration Manager 2.2, manages from 1 to 50 devices including the Contivity 2xx. This license version includes media kit and license. It supports Windows, NT, Solaris and includes an embedded database.

DM0021053-2.2 License to upgrade Contivity Configuration Manager 2.2 from maximum of 50 devices up to 250 devices.

2 250 network elements

DM0021017-2.2 Contivity Configuration Manager 2.2, manages from 1 to 250 devices including the Contivity 2xx. This license version includes a media kit and license. It supports Windows, NT, Solaris and it includes an embedded database.

3 2500 network elements

DM0021018-2.2 Contivity Configuration Manager 2.2, manages from 1 to 2500 devices including the Contivity 2xx. This license version includes a media kit and license. It supports Windows, NT, Solaris, and it includes an embedded database.

DM0021019-2.2 License to upgrade Contivity Configuration Manager 2.2 from maximum of 250 devices up to 2500 devices.

The section on License Versions will be updated in the next release of *Contivity Configuration Manager Administration Guide* (314792-D Rev 00).