2.1

Part No. 315768-C Rev 00
January 2004

600 Technology Park Drive
Billerica, MA 01821-4130

Contivity Configuration Manager v2.1 Driver Release Notes

315768-C REV 00

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

New configurable features in CCM 2.1:

- Secure HTTP—HTTP server now visible from the public network secured by SSL /TLS (Secure Sockets Layer/Transport Layer Security). A feature of Contivity 4.8.
- Rule Logging—Configures the level of detail the user wants for the logs.
- NOT—The NOT operand negates the effect of the service or network object. A feature of Contivity 4.8.
- Malicious scan detection—Enables malicious scan detection and also sets the time, the number of ports to be scanned, and the number of hosts to be scanned for malicious attacks on the CES. A feature of Contivity 4.8.
- Client PC Security Policy Association—The Contivity client checks a Software Requirement Set (SRS), guaranteeing that the required programs or DLLs are loaded and running. A feature of Contivity 4.8.
- Circuitless IP—Provides seamless access to the device in case of physical interface failure, provided there is an alternate physical path to the same circuitless IP address. A feature of Contivity 4.8.
- New Client Address Redistribution Options—Client address redistribution allows the gateway to advertise user tunnel host network routes if the private address does not belong to a locally attached gateway network. A feature of Contivity 4.8.
- New Network Address Translation Policy Generation—A feature of Contivity 4.8.
- Backup Interface Service—Allows the initial configuration of backup interface for Contivity to provide a reliable forwarding service to user traffic. A feature of Contivity 4.8.
- Serial Port—Support for asynchronous serial interfaces over the serial port allows for the support of Dial Backup scenarios and can also be used to dial into the device and manage it using the Web GUI. A feature of Contivity 4.8.
- Firewall User Authentication—Allows the administrator to enable or disable firewall user authentication on the public and private sides of the device. A feature of Contivity 4.8.
- New CERT Options—See the Contivity 4.8 documentation for more information on this feature.

- File Compression—Enables compression of core dump, syslog, account log, and LDIF files on the hard disk of the Contivity gateway, saving considerable disk space.
- Group Access List—Support for the configuration of Access Network has been added to the Connectivity section of the IP Profiles > Groups tab.
- Syslog—Enables Contivity server to forward information from the system log to different host machines via the system logging daemon.
- Wizards—Two new wizards are included in CCM 2.1
  - NAT Policy wizard - allows automatic migration of old policies to a new format
  - Tunnel Guard wizard - distributes previously created TunnelGuard rules to devices

CCM 2.1 Release

This document lists Contivity*, Contivity 221*, and Contivity Branch Access* (formerly Instant Internet*) configuration features that are not supported in Contivity Configuration Manager* release v2.1. These features should be configured by using the embedded interfaces available for these devices: Web UI and NNCLI for Contivity, Contivity Branch Access Setup/Admin Tool, or CLI. The document also recommends certain usage processes that can help users to avoid certain issues in configuring the supported devices using CCM.

Contivity Configuration Manager 2.1 supports the Contivity v3.6, v4.0, v4.07, 4.5, 4.7x, and 4.8 drivers, and the Contivity Branch Access 7.1 and 7.2 drivers (formerly Instant Internet). Models supported are Contivity 100, 400, 600, 1010, 1050, 1100, 1600, 1700, 1740, 2600, 2700, 4500, 4600, and 5000.

CCM 2.1 is compatible with v4.55 and 4.75, however it will 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 will be called out when an issue applies specifically to that model.

Executing CCM wizards

In CCM 2.1, wizards are no longer available by default. Instead, the CCM administrator must grant or deny users and groups access to use the CCM wizards. For more information, see the *Contivity Configuration Manager Administration Guide*.

➡ **Note:** If you migrate from an earlier version of CCM to CCM 2.1, the CCM administrator will still have to allow access to the wizards, even though access was already granted in a previous version.

CCM 2.1 to 2.1 migration

You can not migrate data from a pre-release version of CCM 2.1 to the release version of CCM 2.1. You will receive a message that this is not a valid migration path.

Known Anomalies in CCM 2.1

The following section lists the known anomalies in the Contivity, Contivity 221, and Contivity Branch Access in relation to CCM 2.1.

Factory reset

When you reset a Contivity device to its factory defaults, you lose all of the device’s original keys and other information. CCM treats it as a different device. You must import the device to CCM again and then make changes to the configuration.

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.

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 will have to use the Web GUI to configure the IPSec options.

CA certificates checkbox

CA certificates cannot be enabled or disabled in CCM as there is no checkbox available.

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.

DHCP lease times

CCM does not allow you to change the Specified Time Default or Maximum values. The computer will beep, but the values remain unchanged. Contivity devices do allow you to change the Specified Time values.

NAT overlap message

If you define two NAT port rules in CCM on a pre-4.80 device and specify to use public interface address, you receive an erroneous overlap error message.

WAN Interface

In the CCM Interfaces > WAN Interface > Basic tab, the Data Rate is always listed as 1536000. The Contivity device reflects the bandwidth rate that is selected in the CSU/DSU Fractional T1 field. If you change the bandwidth in CCM to some other value, the Data Rate still reads 1536000.

CCM erroneously allows you to enter larger Interface > WAN Interface values than the Contivity device supports. Values must be no larger than 1536000.

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.

L2TP branch office incorrect

To enable IPSec Data Protection in an L2TP branch office, you have to disable Compression and Encryption. However, if these are enabled, you can still choose the IPSec Data Protection level. IPSec Data Protection should be unavailable for configuration unless Compression and Encryption have been disabled.

New groups

When you create a new group, give it a name before you create any users or subgroups under it. If you create users in the new group before it has a name, the user records will not be exported to the Contivity device, unless you move the user records to another group that has a name. If you create any subgroups beneath the new group before it has a name, then the name of the new group will be set to “default” and this cannot be changed.

If the user record is not being exported, copy the record to another group and then export.

L2TP shared key missing

The L2TP IPSec Data Protection shared key field is missing. When you have anything configured in the “initiator id” field under the IPSec tab, this value overwrites any value in the UID for PPTP or L2TP. This behavior only occurs when the tunnel has been created as an IPSec tunnel first, then changed to a PPTP or L2TP tunnel. To work around this issue, delete the Initiator Setting in the IPSec tab.

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.

DHCP server options

The DHCP Standard Option > Time Offset option does not export to a Contivity device when it is listed before the Subnet Mask in the standard options list. To export Time Offset successfully, list it after the subnet mask in the standard options list in CCM.

Response Timeout Interval

On Contivity devices, the Response Timeout Interval must be 10 or less and the Maximum Transmit Attempts parameter must be five or less. However, CCM erroneously allows larger values in both cases. Upon export, the Contivity device ignores the value.

Authentication fields

When you create a new User Group in CCM and enable all encryption settings under Services > IPSec, the encryption settings under the new group’s IPSec settings will be unavailable. They should be configurable. To work around this issue, select and deselect the inheritance box for encryption under the group settings. Doing so allows you to use the IPSec boxes once more.

Enabling anti-spoofing

Under Firewall/NAT, the Basic tab has the ability to enable all of the Firewall features. The Basic tab also allows you to enable Anti-spoofing without enabling the Contivity Stateful firewall. However, when you export a configuration with Anti-spoofing enabled without enabling the firewall, anti-spoofing remains disabled on the device. In order to export an anti-spoofing configuration successfully, you must have the firewall enabled as well.

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.

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.

User accounts lost on export

If you move 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.

Adding users before naming group

If you create a group in CCM and do not name it, and then add users to the group, the user will not be configured in the driver after an export operation. You must first name the group, then add the users for the configuration to export.

SUA NAT address mapping

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

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.

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.

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.

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.

Reporting feature in CBA Multi-Device wizard

The reporting feature is currently unavailable in the Multi-Device Configuration wizard.

User IP address pool contains option for default pool

CCM allows you to configure a default IP address pool, but you must name the pool “default” rather than simply checking a box as you would in the device.

Syslog Filter Facility has 2 “All” entries

The drop down list for Syslog Filter Facility contains two choices for “All.”

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.

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.

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.

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.

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, this should be done via the Contivity Web GUI.

WAN Interface

CCM offers data rates for the LMC 1000 WAN card that are larger than the maximum accepted by the card: 2048000. When specifying data rates for the LMC 1000 in CCM, be careful to limit your choices to 2048000 or smaller.

On the WAN Interface > PPP Settings page, you can specify an illegal value for the Interface mask. When entering a mask value in this field, make sure that the value is a legal mask.

The WAN Interface Description does not import or export for the four types of WAN cards available. When you set descriptions for each WAN interface and then export to a Contivity device, the interface description is blank. Also, the PPP Description does not import or export for the Wanic 700 or the LMC 1200 cards.

DHCP IP Address Inclusion

CCM will let you specify that a DHCP IP Address Inclusion or Exclusion pool range is outside the pool itself. When specifying either of these, make sure that the range is within the DHCP pool.

Hours rename

If you create a new Profiles > Access Hours entry, the name will appear under the Backup Interface Service > Hours drop-down menu. However, if you rename the Access Hours profile, the name does not update in the drop-down menu.

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.

Duplicated NAS UID and LAC UID

CCM erroneously allows duplicate NAS UID and LAC UID entries even though Contivity devices do not allow the duplication.

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.

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.

Dropdown for MAC

The dropdown menu for the MAC Pause Free Receive FIFO Threshold has some values that are not available on the CES and lacks values that are present on the device. When selecting values, limit your choices to 50%, 60%, 65%, 75%, and 85%.

IPSec Data Protection key export

When you enter an IPSec Data Protection key password for an L2TP branch office tunnel in CCM and then export the configuration to a Contivity device, the IPSec key does not get exported. For the IPSec key to work properly, configure the tunnel using the Web GUI.

IP addresses on different subnets

In CCM, the local and remote IP addresses for virtual circuits can be on different subnets. However, Contivity devices do not allow the IP addresses to be on different subnets, unless the subnet mask is 255.255.255.255. You must either specify a subnet mask of 255.255.255.255 or modify the IP addresses to be on the same subnet.

MAC Pause

When you are specifying values for MAC Pause Ticks, be sure that your value is 31 or greater.

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.

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.

Server start

When starting the CCM server for the first time after installation, the server must be running and 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, FTP should be enabled 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 so 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” / “Key Not Installed” under the Admin > Install Keys Status tab.

As an off-line configuration tool, CCM permits the configuration of these features in CCM database without a license key. But 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 email. This PKCS#7 Base-64 Certificate encoding will have to 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 email. This PKCS#7 Base-64 Certificate encoding will have to 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, you should 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 from the Web UI.

3 Send this information to the CA Authority using their web site or email.

CA Authority generates PKCS#7 Base-64 Certificate encoding based on the data that they receive.

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 which use CA certificate authentication method, always re-import after doing an export. If you export twice without doing any re-imports, you may wipe out the CA certificate information for the users.

Firewalls

Invalid characters in naming definitions

In CCM, the Firewall > Stateful Firewall Policies > Network Objects allows you to use invalid characters when you add a new definition to an imported configuration. When you paste a new Network Object or Service Object in CCM, the name field accepts characters that are invalid on the Contivity device. This is true for Network Group, New Host Definition, New IP Range Definition, and New Network Definition under Network Objects, and for New ICMP Service, New IP Service, New TCP Service, New UDP Service, and Service Group under Service Objects. The invalid characters are:

- +
- =
- [ ]
- ,
- ;
- “
- \
- < >
- {}
- #

Your naming conventions for objects must not include any of the above characters or the Contivity device will not recognize the object upon export of the configuration.

Deletable rule

A firewall rule should be deleted only from the tree under the firewall policy. The rules show up as part of the table under the properties section. For example, they can be seen under Firewall > Stateful Firewall Policies > User Defined Policy > Interface Specific Rules > LAN > Source Interface Rules. These are only for changing the order of rules in a policy. Even if a rule is deleted from this table, it will still exist in CCM and in the Contivity after export.

Missing options in Rules field

When you import a Contivity switch into CCM, some firewall rules options are unavailable for configuration. Under Firewall > Stateful Firewall Policies > *User Defined Policy* > Interface Specific Rules > LAN > Source Interface Rules > Rule 1 > Properties, the Dst Interface drop down list does not include the Slot1 Interface1 option.

To configure this feature from the Web UI, select Services > Firewall/NAT > Manage Policies > User Defined Policy > Edit > Interface Specific Rules > LAN > Source Interface Rules > Rule 1 > Dst Interface and select Slot1 Interface1.

Network Mask format

In CCM, the Network Mask format under Firewall > Stateful Firewall Policies > Network Objects > New Network Definition > Properties differs from that on the Contivity device. You can enter any number for the Network Mask in CCM rather than in dotted decimal notation found in Contivity.

The value would not get exported to the network but it would show up in the CCM database.

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)

IPX

When you import a Contivity switch into CCM, there are several instances where the ranges given for a particular field under Extranet IPX are incorrect. The ranges in the IPX Maximum SAP Entries field and the IPX Maximum Route Entries field are listed as 0-5000. The correct value that the Contivity switch takes is 10-10,000.

The Extranet IPX should not allow modifications to the number of interfaces. However, this is not the case in CCM. CCM allows you to delete rows from the interface table even though it does not allow you to add interfaces. If you delete the interface row, you will not be able to configure the device.

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.

Secondly, 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 via any of the embedded interfaces, such as the Web UI or CLI.

Thirdly, 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. Should you 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 doing an export. Doing so can cause the switch to malfunction.

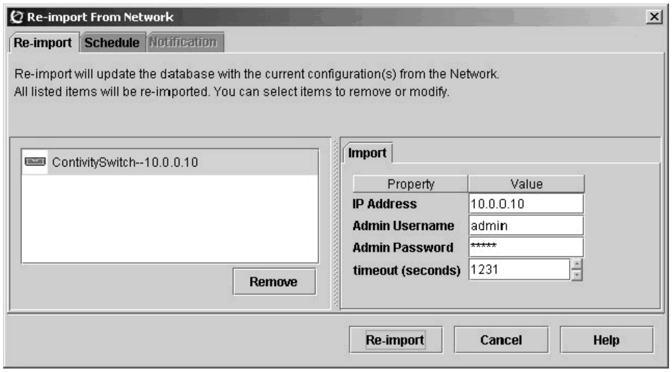
Timeout values for import operations

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 hit, a different tab selected, etc.). This step typically occurs during the natural flow of operations. However, there is one operation where, if you change the timeout value for re-import operations, you must change the focus before clicking the re-import button. Otherwise, the operation is performed using the old timeout value.



Re-import will update the database with the current configuration(s) from the Network.
All listed items will be re-imported. You can select items to remove or modify.

ContivitySwitch--10.0.0.10

Property	Value
IP Address	10.0.0.10
Admin Username	admin
Admin Password	*****
timeout (seconds)	1231

Order of rules in Tunnel Filters

The way to re-order the rows in the Tunnel Filters table in CCM differs from how 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 uncheck the “and repeat every” checkbox.

Contivity 221 Known Anomalies

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.

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.

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 can be configured.

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.

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 dropdown will be disabled. To re-enable the Encryption dropdown, disable NAT Traversal and set protocol to AH. Then set protocol to ESP and enable NAT Traveral.

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.

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.

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.

New network objects

Newly created network objects must be assigned to a rule prior to export or they will be lost during the operation.

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.

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.

Contivity Branch Access Known Anomalies

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 routes are 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.