Nortel Unified Communications Management

Fundamentals

Release: 1.0
Document Revision: 01.02

www.nortel.com

NN48014-100

Nortel Unified Communications Management
Release: 1.0
Publication: NN48014-100
Document release date: 2 February 2009

Printed in Canada

Contents

New in this release

The following sections detail what's new in *Nortel Unified Communications Management* (NN48014-100) for 1.0:

Features

See the following sections for information about feature changes:

- "Device and Server Credentials Editor" (page 5)
- "Security Administration" (page 5)

Device and Server Credentials Editor

You can use the Device Credential Editor, part of UCM Common Services, to set passwords, SNMP options, and other credentials for network devices. These configurations will be common to all installed UCM applications, including VPFM (or VPFM Lite), EPM, and NRM. For more information, see "Device and Server Credentials Editor configuration" (page 15).

Security Administration

You can configure security protocols for network elements, set user access parameters, and set security policies across the network using Security Administration, part of UCM Common Services. These configurations will be common to all installed UCM applications, including VPFM (or VPFM Lite), EPM, and NRM. From more information, see "Security Administration configuration" (page 13).

Other information

See the following section for information about changes that are not feature related:

Multimedia content

Some conceptual and procedural topics covered in the documentation are now available in a multimedia format. Links to the multimedia content are provided contextually in the documentation.

"WATCH THE VIDEO" identifies a link to multimedia content.

Introduction

Nortel Unified Communications Management (UCM) provides the common platform for integrating network management products, such as Network Resource Manager (NRM), Enterprise Policy Manager (EPM), and Visualization Performance and Fault Manager (VPFM), as well as VPFM-Lite. UCM contains administrative services for all of these products through Common Services (UCM-CS), which includes Security Administration and Device Credentials Editor. It also provides a home page from which to access any of these installed products.

Navigation

UCM login

The following chapter describes how to launch and log onto Unified Communications Management.

Navigation

- "Logging onto UCM" (page 9)

Logging onto UCM

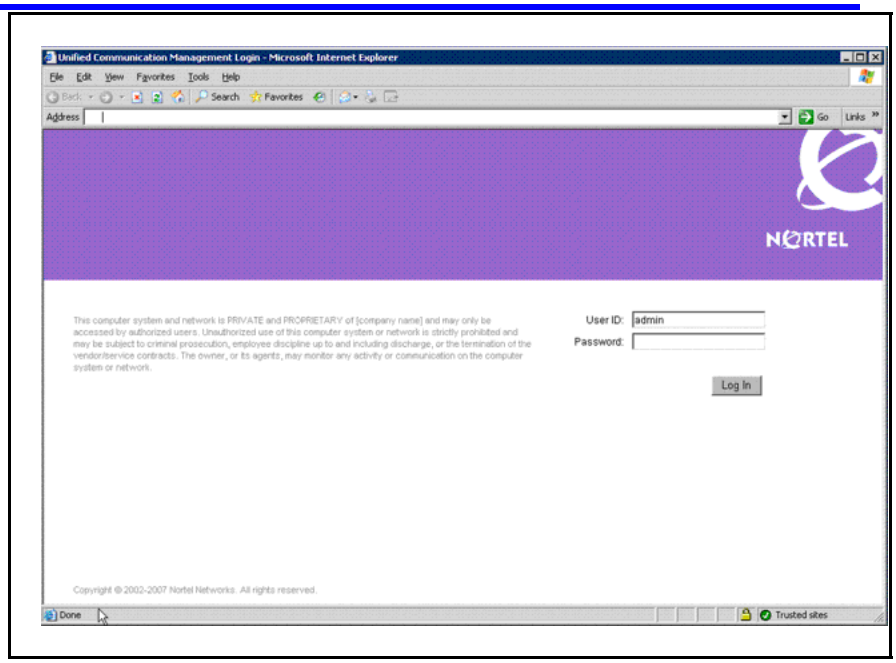
Use the following procedure to log onto UCM.

Prerequisites

- You must install UCM
- Internet Explorer 7, or Firefox 2 if logging in with a client PC.

Procedure Steps

Step	Action
1	On the server where UCM is installed, choose **Start>Programs>Nortel>UCM>Unified Communications Management**. **Or** On a client PC, point an internet browser to the FQDN of the server where UCM is installed.
2	Click **Ok** if a message appears telling you to select a security certificate. This certificate is pre-installed and cannot be changed.
3	When the dialog box appears, select the option to accept the certificate. This will differ depending on the browser you are using. The UCM login screen appears.

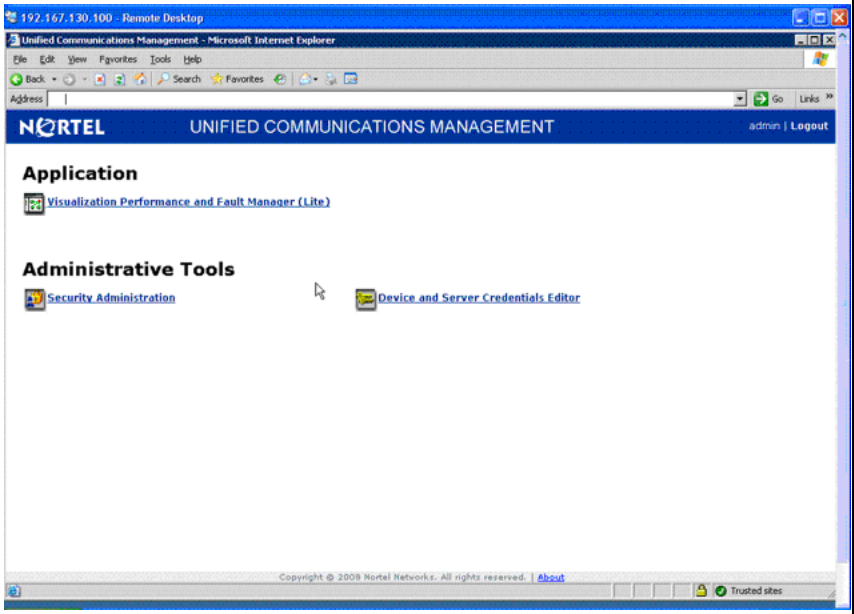


4 Enter the User ID.
The default is admin.

5 Enter the password.
This is set during the installation of NRM, EPM, VPFM, or VPFM-Lite.

6 Click **Log in**.

The Unified Communications Management home page appears.



--End--

Security Administration configuration

For information about Security Administration in Unified Communications Management (UCM), see *Nortel Communications Server 1000—Enterprise Common Manager Fundamentals* (NN43001-116).

Device and Server Credentials Editor configuration

This chapter provides information on configuring device credentials using the Device and Server Credentials Editor.

Nortel Unified Communication Management (UCM) applications use SNMP v1/v2/v3, Telnet, CIM/XML, SSH, FTP, RLogin, or SSH protocols for communication with network infrastructure devices such as routers. The protocol required depends on the type of device. Communication to a windows server is done using the WMI protocol. Each set of credential information is referred to as a credential set. These credential sets allow UCM applications to retrieve information from the network elements and devices. The Device and Server Credentials Editor service maintains a list of credential sets for the devices that make up a network. Credentials can be enter for every device (IP address) or for a range of IP addresses. Refer to the documentation for your network devices to determine which protocols they use for authentication.

When using Network Discovery in VPFM, the application uses these credentials to discover network devices and servers. For more information about network discovery, refer to *Nortel Visualization Performance and Fault Manager—Configuration* (NN48014-500).

The following table lists the categories of credential information that can be managed in the Device and Server Credentials Editor.

Table 1
Device and Server Credentials Editor fields

Credential information	Attributes
Name	Credential Set Name
IP Address or Range	Device/Server IP Address or Address Range
SNMPv1/v2	Read Community Write Community

Table 1
Device and Server Credentials Editor fields (cont'd.)

SNMPv3	SNMPv3 User Authorization Protocol (MD5, SHA1, None) Authorization Key Privacy Protocol (AES128, DES, 3DES, None) Privacy Key
Telnet	Telnet Username Telnet Password Telnet Port
FTP	FTP Username FTP Password FTP Port
SSH	SSH Username SSH Password SSH Port
CIM-XML	CIM Username CIM Password
RLogin	RLogin Username RLogin Password
Windows Server	Windows Username Windows Password Windows Domain

Navigation

- "Adding a credential set" (page 16)
- "Editing a credential set" (page 18)
- "Deleting a credential set" (page 19)
- "Refreshing the credential set list" (page 20)

Click here to view a multimedia presentation about setting device credentials
http://www31.nortel.com/webcast.cgi?id=8006

Adding a credential set

Use the following procedure to add a new credential set to the Unified Communications Management. You must add a credential set for each device you want to manage.

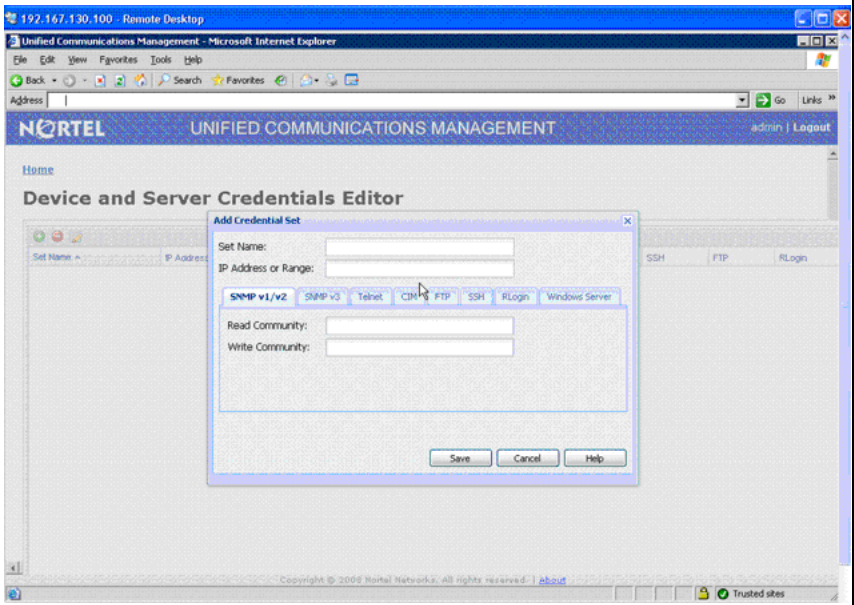
The Set Name should contain printable ASCII characters, but no special characters (&^%(!/\)^, and so on). The Space ( ), Dash (-), and Underscore (_) characters are allowed.

The Set name must be unique. If you add a new entry or rename an existing one with a Set Name already used in another entry, a warning message is displayed.

Prerequisites

- You must install UCM. UCM is installed when you install a UCM application (VPFM, VPFM Lite, EPM, or NRM). For more information, refer to the installation guide for your UCM application.
- Ensure that you are logged on to UCM.

Procedure Steps

Step	Action
1	Select **Device and Server Credentials Editor** from the main UCM page.
2	Click the **Add Credential Set** button. The Add Credential Set dialog box appears. 
3	Enter the **Set Name**.
4	In the **IP Address/Range** field, specify the IP address information for the credential. For a list of valid IP addresses and ranges, see "IP addresses and ranges reference" (page 25).

5 Add device credential information on the appropriate tab(s). For information about the available tabs, see Table 1 " Device and Server Credentials Editor fields" (page 15).

Each tab corresponds to an authentication protocol. The tab that needs to be entered will depend on the type of authentication your device uses.

6 Click **Save**. The credential set will appear in the pane.

--End--

Editing a credential set

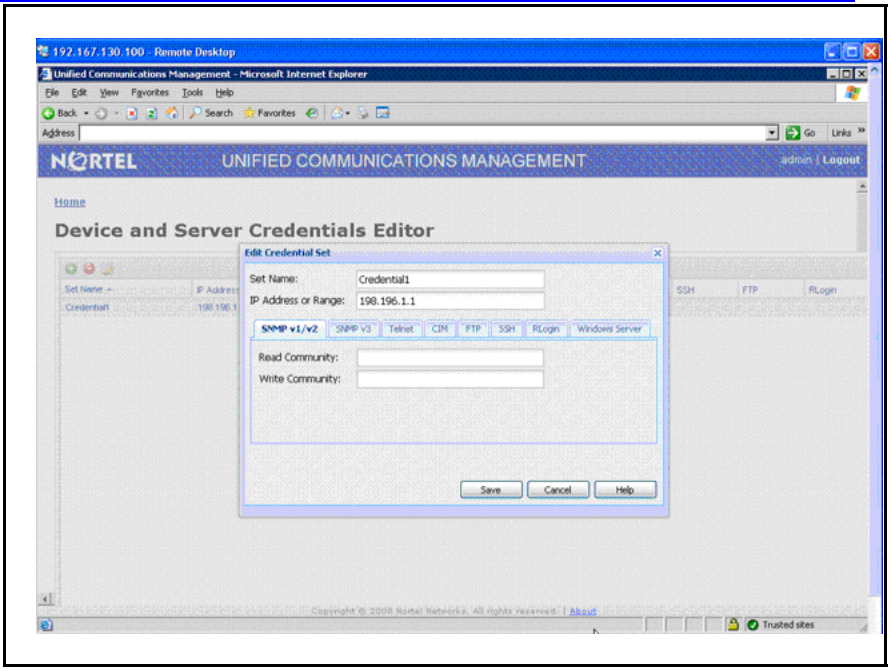
Edit a credential set to change the set name, IP address, and device credential information for a credential set.

Prerequisites

- Ensure that you are logged on to UCM.

Procedure Steps

Step	Action
1	Select **Device and Server Credentials Editor** from the main UCM page.
2	In the Device and Server Credentials Editor, click on the credential set you want to change.
3	Click the **Edit Credential Set** button. The **Edit Credential Set** dialog box appears.



4 Make changes to the credential set as required.

5 If you want to specify a different type of device credential information, click the **Show All** tab, and then type the new device credential information in the appropriate tab.

6 Click **Save**.

All specified IP addresses are validated after saving the changes.

--End--

Deleting a credential set

Delete a credential set to remove it from the Device and Server Credentials Editor.

Prerequisites

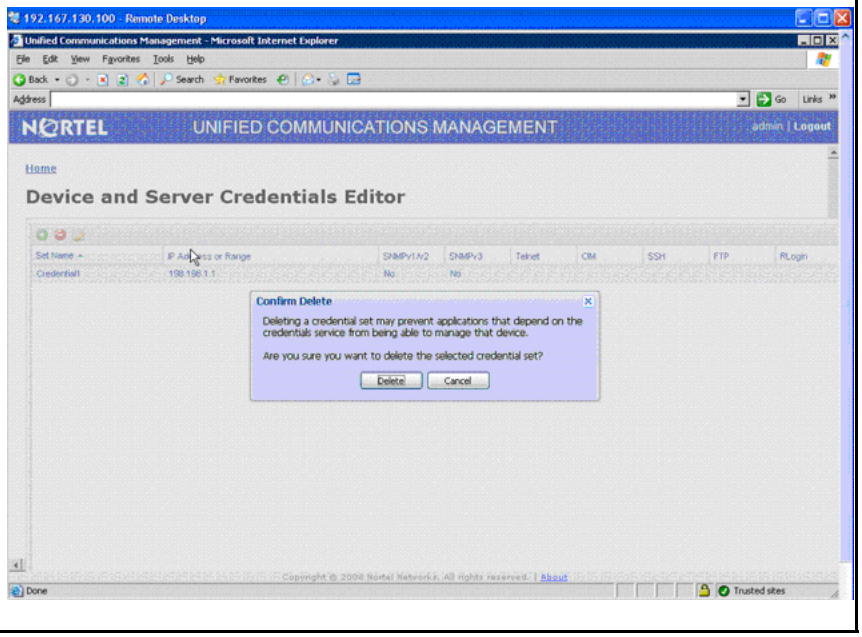
- Ensure that you are logged on to UCM.

Procedure Steps

Step	Action
1	Select **Device and Server Credentials Editor** from the main UCM page.
2	Click on the credential set you want to remove. You can select several credential sets at once by holding down the CTRL key and clicking on the credential sets.

3 Click the **Delete Credential Set(s)** button.

You are prompted to confirm the deletion.



4 Click **Delete** to continue.

--End--

Refreshing the credential set list

Use the manual Refresh command to ensure that the information that appears in the Device and Server Credentials Editor is up-to-date. Updates to the credential sets list may not immediately be reflected in the Device and Server Credentials Editor until it is refreshed. Credential sets update automatically every 10 seconds.

Procedure Steps

Step	Action
1	In the Device and Server Credentials Editor, click the **Refresh** button, located at the bottom of the page. The list of available credential sets is refreshed from the UCM database.

--End--

Backup and Restore

All data within Unified Communications Management applications, including licenses can be backed up and restored on demand. Backup and Restore functionality is accessed from the command line.

All backup files are stored in a folder named backups under UCM_HOME directory. Backup files are stored in JAR format. The application writes debug information of its operations into log files located in common services installation folder: UCM_HOME. Backup archives are stored in [YY]-[MM]-[DD]_[HH].[mm].jar format (for example, 2008-06-09_15.33.jar).

Within common services, the following data are being backup up:

- jbossdb database in MySQL (for Device and Server Credentials data)
- users and roles data
- license files
- profiles / device attributes xml file (located in [UCM_JBOSS_HOME]/server/default/conf)

Stopping services (JBoss, MySQL, and license server) is not necessary to run the backup process.

The following sections describe backup and restore procedures:

- "Backing up UCM files" (page 21)
- "Restoring UCM files" (page 22)

Click here to view a multimedia presentation about backup and restore operations http://www31.nortel.com/webcast.cgi?id=8007

Backing up UCM files

Use the following procedure to backup UCM files.

Prerequisites

- You must be logged into the UCM server as and "Administrator" (in a Windows environment), or as "root" (in Linux).
- You can only backup and restore the same major application version. Differences between minor versions are supported. For example, you can backup and restore from version 1.0 to 1.1, but not from 1.0 to 2.0.

Attention: Do not abort the backup or restore in the middle of the process (for example by pressing Ctrl-C). Doing so my compromise system stability.

Procedure Steps

Step	Action
1	From the command prompt, run the following script:**`C:\Program Files\Nortel\UCM\backupAllData.bat`** **OR** If using Linus, run the following script from the command shell: **`/opt/nortel/ucm/backupAllData.sh`**
2	Enter the database administrator password when prompted. The system backs up all UCM data.

--End--

Restoring UCM files

Use the following procedure to restore a previously backed up archive.

Prerequisites

- You must be logged into the UCM server as and "Administrator" (in a Windows environment), or as "root" (in Linux).
- You can only backup and restore the same major application version. Differences between minor versions are supported. For example, you can backup and restore from version 1.0 to 1.1, but not from 1.0 to 2.0.

Attention: Do not abort the backup or restore in the middle of the process (for example by pressing Ctrl-C). Doing so my compromise system stability.

Procedure Steps

Step	Action
1	From the command prompt, run the following script:**C:\Program Files\Nortel\UCM\restoreAllData.bat** **OR** If using Linux, run the following script from the command shell: **/opt/nortel/ucm/restoreAllData.sh**
2	Enter the database administrator password when prompted.
3	Enter the name of the archive you wish to restore. The system restores the selected archive. You may be required to restart services after the restore is complete.

--End--

IP addresses and ranges reference

This chapter provides detail about the valid IP addresses and IP ranges used by the Device and Server Credentials Editor.

Valid IP addresses and ranges

The following section describes the valid IP addresses and ranges used for device credentials.

Navigation

Valid IP addresses

IPv4 addresses must conform to the following format: [1-255].[0-255].[0-255].[0.255].

IPv6 addresses must conform to IPv6 rules:

- IPv6 addresses must contain eight groups of four hexadecimal digits.
- Each group must be separated by a colon (:).
- If one or more four-digit group or groups appears as 0000, the zeros may be omitted and replaced with two colons (::). For example, the following are valid IPv6 addresses:
  - 2001:0db8:85a3:08d3:1319:8a2e:0370:7334
  - 2001:0db8::1428:57ab

Valid IP address ranges

When specifying IP address ranges, only consecutive wild cards starting from the last octet of an address are supported. This guarantees one continuous range. For example, only the following combinations are valid:

- IPv4:
  - 17.0.9.* (same as 17.0.9.0-17.0.9.255)

  - 17.0.*.* (same as 17.0.0.0-17.0.255.255)
  - 17.*.*.* (same as 17.0.0.0-17.255.255.255)
  - *.*.*.* (same as 0.0.0.0-255.255.255.255)
  - 17.*.9.9 is invalid
  - 0.0.0.0 and 255.255.255.255 are considered to be valid IPs only if they are given within a range. For example, 0.0.0.0 as single IP is invalid, but 0.0.0.0-2.3.4.5 is a valid range.
- IPv6:
  - 2001:0db8:85a3:08d3:1319:8a2e:0370:* (same as 2001:0db8:85a3:08d3:1319:8a2e:0370:0000-2001:0db8:85a3:08d3:1319:8a2e:0370:ffff)
  - 2001:0db8:85a3:08d3:1319:8a2e:*:*
  - 2001::8a2e:0370:*
- IPs contained in a range cannot have wild cards. For example, 192.168.4.*-192.168.5.245 is an invalid range.

IP address format limitations

The following formats are not supported by Device and Server Credentials Editor:

- An address/subnet mask pair (for example, 10.127.100.0/255.255.255.0)
- Network prefix (CIDR) notation (for example, 10.127.100.0/24)

Nortel Unified Communications Management

Fundamentals

Printed in Canada
Release: 1.0
Publication: NN48014-100
Document revision: 01.02
Document release date: 2 February 2009

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com

NORTEL