Digi Connectware Manager Operator's Guide

Making DEVICE NETWORKING *easy*™

Digi Connectware Manager Operator's Guide

Part number/version: 90000770_A
Release date: February 2006
www.digi.com

Contents

Using This Guide

Review this section for basic information about this guide, as well as for general support contact information.

About this guide

This guide describes the tasks operators, network managers, and others perform to configure, update, manage and monitor groups of devices across remote networks using Digi Connectware Manager.

Software release

This guide supports Digi Connectware Manager version 3.1.

Who should read this guide

This guide is for operators who use Digi Connectware Manager to access, configure, and manage devices.

To complete the tasks described in this guide, you must:

- Be familiar with installing and configuring software.
- Have administrative privileges.

Conventions used in this guide

This table describes the typographic conventions used in this guide:

This convention	Is used for
italic type	Emphasis, new terms, variables, and document titles.
bold, sans serif type	Menu commands, dialog box components, and other items that appear on-screen.
Select **menu name→ menu selection name**	Menu commands. The first word is the menu name; the words that follow are menu selections.
`monospaced type`	File names, pathnames, and code examples.

Related documentation

Digi Connectware Manager Getting Started Guide provides installation instructions.

Customer support

To get help with a question or technical problem with this product, or to make comments and recommendations about our products or documentation, use this contact information:

For	Contact information
Technical support	Telephone: ■ United States: 1 877 912-3444 ■ Other locations: 1 952 912-3456
	Fax: 1 952 912-4960
Digi home page	www.digi.com
Online problem reporting	www.digi.com/support/eservice/eservicelogin.jsp

Introduction

CHAPTER 1

This chapter provides an overview of Digi Connectware Manager.

About Digi Connectware Manager

Digi Connectware Manager, part of the Digi Connectware Suite, provides enterprise class configuration, management, and administration of its remote site management class of products, including:

- Digi Connect Remote Gateway GSM
- Digi Connect WAN, WAN GSM, VPN, VPN GSM, ME, SP, and EM
- Connect Port Display
- Connect Port WAN

Two components, the Server Management application and the Device Management application, make up Digi Connectware Manager; this document primarily addresses the Device Management application.

By providing a central point of access to remote devices or groups of devices, Digi Connectware Manager makes it easier for you to manage many devices. Using a standard Web browser, you securely make configuration changes to a device or to groups of devices, manage devices, and monitor device status and statistics. Because you can diagnose and solve problems from a central site, resulting in fewer maintenance trips to remote locations, Digi Connectware Manager helps you reduce maintenance costs.

Digi Connectware Manager can be hosted at a customer's central data center or through a Digi ASP partner and can be accessed securely from anywhere across a wired or wireless IP network, including the Internet.

In addition to Digi Connectware Manager, the Digi Connectware Suite also includes a connection manager that provides a means of seamless connections to remote devices, including devices on private or dynamic IP networks.

Features

Features of Digi Connectware Manager include:

- **Device configuration**. Digi Connectware Manager makes it easy for you to define and update, for example, network, serial port, security, and alarm, and other device configuration.
- **Device management**. You can perform management and administrative tasks such as backing up, restoring, importing, and exporting device configuration settings. You also easily can update firmware and redirect devices to different destinations.
- **Device and connection monitoring**. With the device and connection monitoring features, you can get up-to-date information and statistics about a device's mobile signal strength, network activity, and more. You also can view connection status and history information
- **Alerting and notification**. This real-time stream of messages associated with error conditions and status indications provides device and connection information.
- **Secure communications**. Digi Connectware Manager provides up to 256-bit AES encryption and authentication for communication with remote devices.
- **Alarm generation and alerting**. Digi Connectware Manager provides an alarm action to allow notifications to be sent to a SNMP Network Management Station (NMS) from the Connectware Manager in response to the supported trigger conditions.
- **Grouping**. When you create groups of devices, you can efficiently apply device settings or perform maintenance tasks on multiple devices at one time. Although devices are often grouped by location, you can group them in the way that's useful to you and your environment.

Terms to know

This section provides brief descriptions of terms used throughout this guide.

Management Console

The *Management Console* is a Web-based interface through which you gain access to Digi Connectware Manager and the Device Management and Server Management applications.

Provisioning and autoprovisioning

Provisioning is the process of adding a device. By default, *auto-provisioning* is enabled in Connectware Manager; when a device connects, the server automatically retrieves the device's serial number and firmware version and associates the device ID with known device types.

If you disable auto-provisioning, you add devices manually, using the Device Management application.

Device configuration

Device configuration is the process by which you attribute characteristics to devices. The characteristics, which define many aspects of a device's behavior, include settings associated with, for example, a device's security capabilities, network connection, mobile connection, alarm notification capability, and others.

Device maintenance

Device maintenance consists of managing deployed devices by such tasks as monitoring and controlling their status, editing configuration information, and setting up for automatic firmware downloads.

Network administration

Network administration consists of the tasks you do to maintain the best performance level of devices, such as performance and load balancing.

Exploring Digi Connectware Manager Device Management

CHAPTER 2

This chapter describes how to log into Digi Connectware Manager and start the Device Management application. This chapter also gets you acquainted with the **Connectware Device Management** page and describes how to do basic tasks from this page.

Logging in to Digi Connectware Manager and starting Device Management

If you are using Digi Connectware Manager for the first time, during the installation you may see a prompt to install Java Runtime Environment (JRE) version 1.5, which is supplied with Digi Connectware Manager. Respond to this prompt by clicking **Yes**.

In addition, depending on the way your system is set up, you also may see a series of Windows security messages. To continue with the installation, click **Yes**.

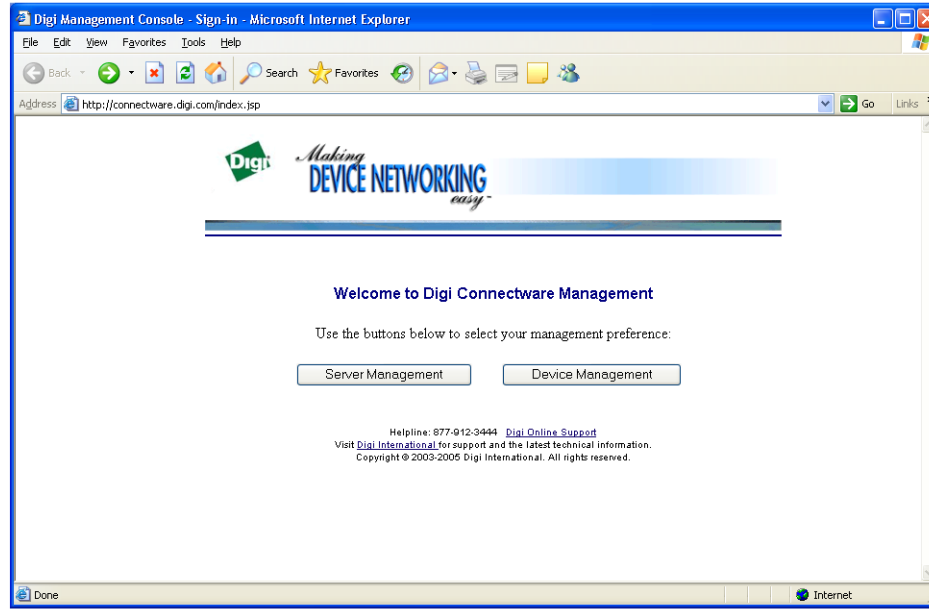
To log into Digi Connectware Manager:

1 Start a Web browser.

2 In the **Address** input box, enter `http://connectware server`

where you replace `connectware server` with the name or address of your Connectware server; for example: `http://connectware.digi.com`

The **Digi Connectware Management Welcome** page opens:



3 To start the Device Management application, click **Device Management**.

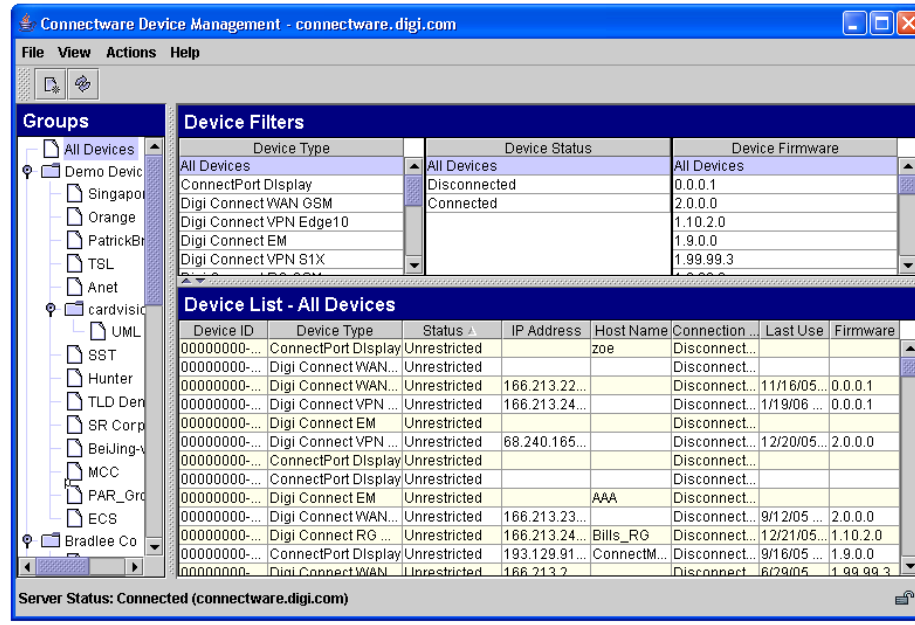
A dialog box opens and prompts you to log in:

4 Enter the default username and password:

- **Username:** `admin`
- **Password:** `changeme`

and then click **Login**.

The **Connectware Device Management** page opens:



If this is the first time you are using Digi Connectware Manager, be aware that the list of groups in the left pane and the **Device List** will be empty because you haven't yet added any groups or devices.

From this page, you can:

- Filter and sort the information in the **Device List**.
- Refresh the information
- View messages from the Device Management application.
- Select one or more devices to configure, manage, and monitor.
- Add and remove devices and groups

Filtering and sorting information

This section describes ways in which you can change the display of the information that appears in the **Device List**.

Filtering

If you are managing hundreds of devices, the **Device List** can be very long. Going through the list to locate a particular device among all the others can be inconvenient and time-consuming.

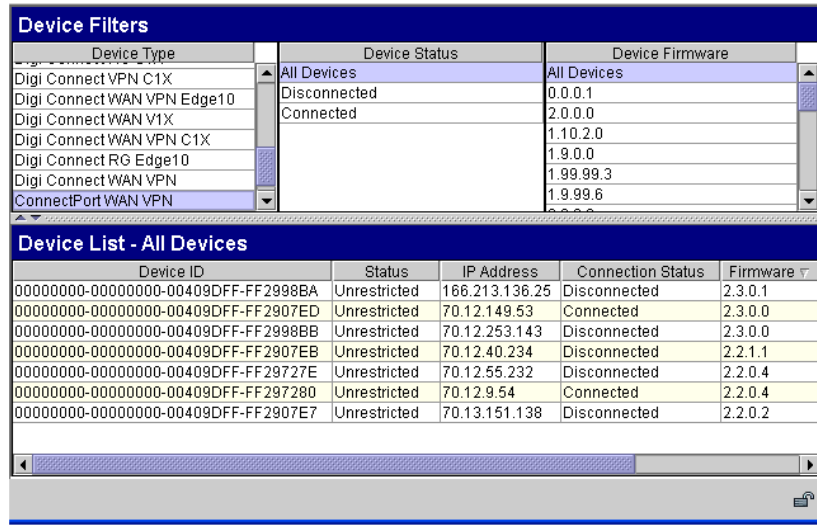
By using filters, however, you can limit the number of devices that appear in the list by specifying filter criteria; only devices that meet the criteria will appear on the list. With fewer devices in the list, you can more easily find the one you want.

This table describes the filters, which are located at the top of the **Connectware Device Management** page:

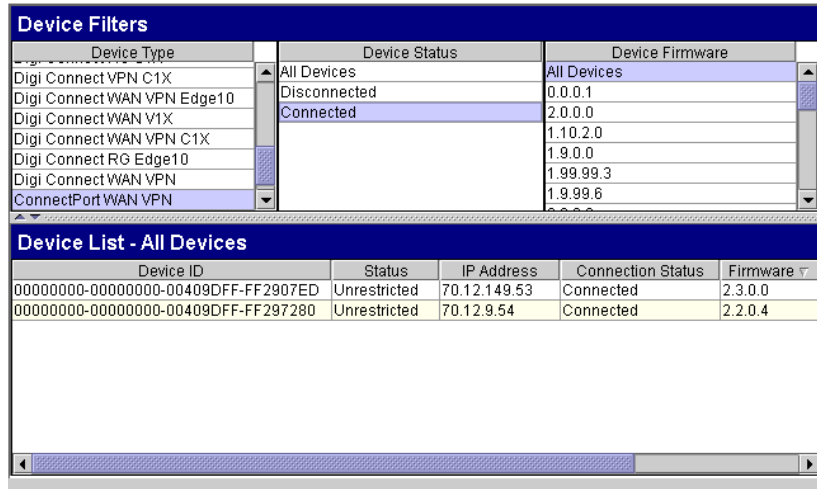
Filter	What it does
Device Type	Limits the devices in the list to the specific device type you select; for example, ConnectPort Display
Device Status	Limits the devices in the list according to whether they are connected or disconnected
Device Firmware	Limits the devices in the list by firmware version

After you use one filter, you can further limit the devices in the list by using another filter. For example, you could filter first by device type, and then filter to see which devices of that type are currently connected, as shown in the next two examples.

Here, the list is filtered by device type — in this case, ConnectPort VPN WAN — which limited the number of devices in the **Device List** to seven:



In this example, the list that was previously filtered by **Device Type** was then filtered by **Device Status** — in this case, **Connected** — which further limited the number of devices in the **Device List**:



Displaying or hiding columns

The **Device List** provides information about each device, arranged in columns. The default columns are **Device ID**, **Device Type**, **Status**, **IP Address**, **Host Name**, **Connection Status**, **Last Use**, and **Firmware**, but you can choose the columns you want to display or hide.

▶ **To display or hide a column:**

1 Right-click a column heading.

This pop up menu opens:

2 From the pop up menu, either check an item you want to display or uncheck one you don't want to display.

You can make only one selection at a time.

Your current settings (such as columns, window sizes, and so on) are stored in a file on your PC. On Windows 2000 and Windows XP systems, the file is in this location:

`C:\Documents and Settings\<<your-user-name>>\Data\config.ini`

▶ **To return to all the defaults:**

1 Close the Device Management application.

2 Delete the file.

3 Restart the Device Management application.

Sorting information within columns

The information in a column can be in one of three states: none, ascending, and descending. To sort the information in a column, click its header.

Refreshing information

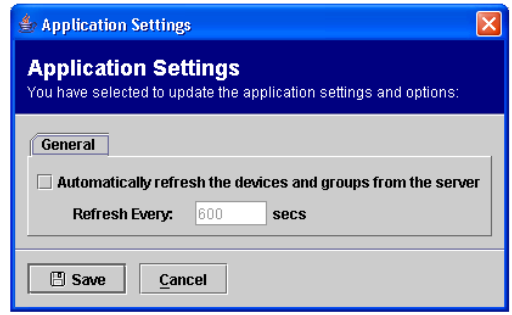
To refresh, or update, device and group information at any time, select **File → Refresh**.

By default, automatic refreshing of device and group information is disabled. You can specify whether you want device and group information to be refreshed automatically and how frequently you want the refresh to occur.

▶ **To specify how often to refresh the screen:**

1 Select **View → Options**.

The **Application Settings** dialog box opens:



2 Check **Automatically refresh the devices and groups from the server.**

3 In the **Refresh every** input box, enter the number of seconds you want between refreshes.

4 Click **Save**.

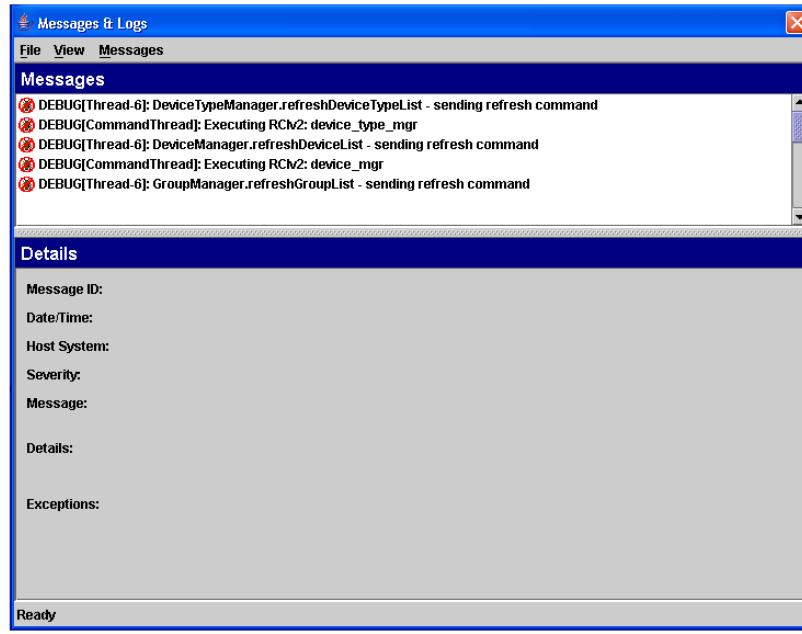
Several messages scroll on your screen to tell you that the list of device types, devices, and groups is being refreshed.

Viewing messages and logs

You can view a real-time stream of messages associated with error conditions and status indications and that provide information. The messages, which are from the Device Management application, are useful for troubleshooting.

To view messages, select **View → Messages & Logs**.

The **Messages & Logs** window opens:



You can leave the **Messages & Logs** window open while you perform other tasks and functions.

You can specify how you want to view the messages and details in the **Messages & Logs** window and the types of messages, based on the severity level, that you want to receive.

- To specify the way the information is arranged, select either **View → Side by Side** or **View → Stacked**.
- To specify the severity level of messages you want to receive, select **Messages → Message Severity Level**, and from the sub menu, select the icon that represents the severity level you want.

  The messages will be at the severity level you selected and higher.
- To refresh the message information, select **Messages → Refresh**.

Adding and removing devices and groups

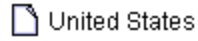
When you add a device, by default it goes in the **All Devices** group and is displayed in the **Device List**. From there, you can either move or copy the device into another group at any time:

- **Moving a device.** The device exists *only* in the group to which you moved it.
- **Copying a device.** The device exists in both groups.

You can create any number of groups and use them to organize your devices in a way that makes sense for your organization. You could, for example, create groups based on their geographical locations, or device type, or by firmware release.

After you create groups and move or copy devices into them, you can perform tasks on all the devices in the group, rather than on each individual device. For example, you could configure the devices, perform administrative tasks, or view statistics.

When you create a group, its name — in this case, United States — and this icon appear in the left pane:



You can create nested groups. The names of the group and its subgroup or subgroups appear in the left pane with these icons:

Adding a device

When you add a device, by default it is added to **All Devices** group. You can then either move or copy the device to a group.

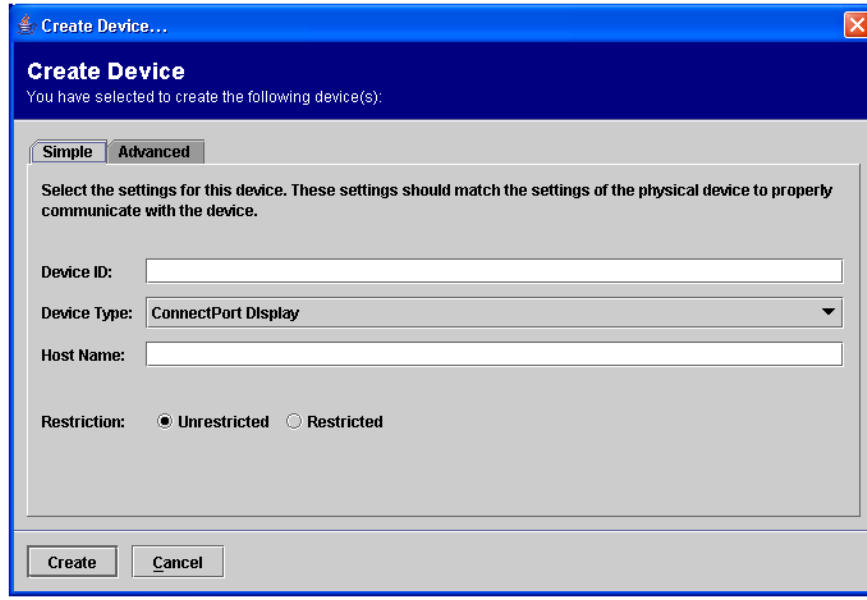
A device can be in either of these states:

- **Restricted**. Connectware Manager does not allow the device to connect. This state is useful if, for example, you want to bring many devices online at some future time; you can add the devices in the restricted state, and change them to the unrestricted state when you are ready to do so.
- **Unrestricted**. Connectware Manager allows the device to connect.

▶ **To add a device:**

1 Select **File → New Device**.

The **Create Device** dialog box opens:



2 Enter the device ID and name by which the device will be known on the network. Then, from the **Device Type** pulldown menu, select the type of device.

3 Under **Restriction**, click one:

- **Unrestricted**
- **Restricted**

4 Click **Create**.

The new device is added to the **Device List**.

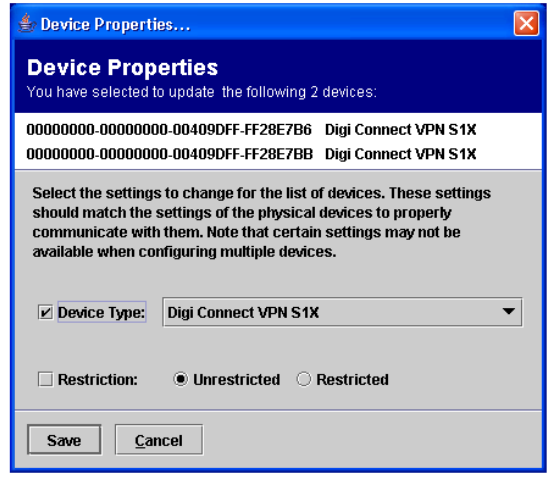
To see the updated information, select **File** → **Refresh**.

▶ **To change the restriction state of an existing device:**

1 Select the device in the **Device List**.

2 Right-click, and from the menu that opens, select **Device Properties**.

The **Device Properties** dialog box opens:



3 Click the restriction state you want for the device, and then click **Save**.

Selecting devices or groups

You can select either a group, a device, or multiple devices to configure, manage, or monitor.

- **Selecting a group**. In the navigation pane at the left of the **Connectware Device Management** page, right-click the group, and from the menu that opens, select an option.

  Any settings or actions you select will apply to all devices in the group.

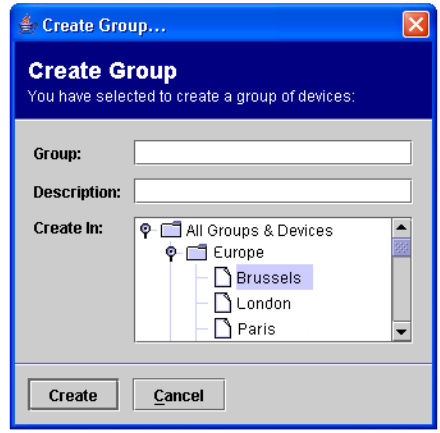
- **Selecting one device from the Device List**. Right-click the device, and from the menu that opens, select an option.
- **Selecting multiple devices from the Device List**. Shift-click the devices, right-click, and from the menu that opens, select an option. Any settings or actions you select will apply to all the selected devices.

Creating a group

▶ **To create a group:**

1. Select **File → New Group**.

   The **Create Group** dialog box opens:



2. Enter a name and brief description, and then select the location for the new group.
3. Click **Create**.

   The new group appears in the left pane.

Copying or moving devices to a group

At any time, you can add devices to a group by either:

- **Copying.** When you copy a device, it exists in both the original group and the group to which you copy it.
- **Moving.** When you move a device to a group, it exists only in the group to which you move it.

▶ **To copy a device to a group:**

1. In the **Device List**, select one or more devices to add to a group.
2. Right-click, and from the menu that opens, select **Copy To**. Then select the group to which to copy the device.

   You see a message that the device is being added to the group.

▶ **To move a device from one group to another:**

1. Select the group that contains the device you want to move.
2. From the **Device List**, select the device.
3. Right-click, and from the menu that opens, click **Move To**. Then select the group to which to move the device.

   You see a message that the device is being removed from the group, followed by another message that the device is being added to the new group.

Removing a group

When you remove a group, the group and all its subgroups are removed from the server.

▶ **To remove a group:**

1. In the left pane, select the group you want to remove.
2. Right-click, and from the menu that opens, select **Remove Group**.

   The **Remove Group** dialog box opens and prompts you for confirmation:

3. Click **Remove Group**.

Removing devices from a group

You can remove a device from a group; by default, the device remains in the **All Devices** group and any other group to which it belongs. Then you can either keep the device there or move it to another group.

▶ **To remove a device from a group:**

1. Select the group from which you want to remove one or more devices.
2. In the **Device List**, select the device or devices you want to remove.

   The **Remove Device** dialog box opens and prompts you to specify how you want to remove the device or devices:

3. Select one:
   - To remove the device from the group but keep it on the server, click **Remove device from *groupname***
   - To remove the device from the server and all groups to which it belongs, click **Remove device from the server and all associated groups.**
4. Click **Remove**.

Removing devices from the Device List

When you remove a device from the **All Devices**, the device is permanently removed from the server.

1 In the **All Devices**, select the device or device you want to remove from the server.

2 Right-click, and from the menu that opens, select **Remove Device**.

The **Remove Device** dialog box opens and prompts you to confirm the removal of this device:

3 Click **Remove**.

Configuring Devices

CHAPTER 3

This chapter provides an overview of device configuration.

Overview

When you configure a device, you define its characteristics. These characteristics control many aspects of the device's behavior. This table lists the types of configuration data you can define and provides some examples of each:

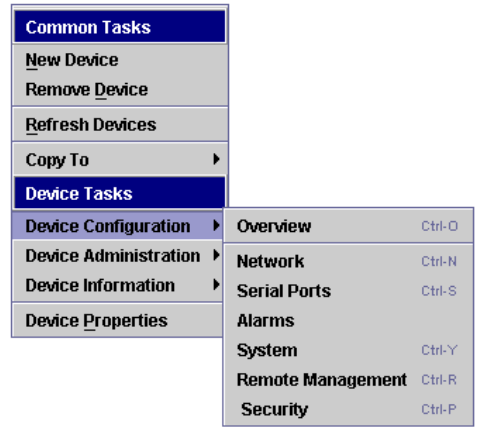
Type of data	Examples
Network	■ The method to use to assign the IP address ■ DHCP server settings ■ The global network services to run on the device ■ IP routing and forwarding ■ VPN security policies, tunnels, Diffie-Hellman group
Mobile	■ Provider settings ■ Service plan ■ Connection settings
Serial ports	■ Port services ■ Network services ■ TCP and UDP settings
Alarms	■ Alarm type ■ Type of notification
System	Device identity: ■ Description ■ Location ■ Device ID
Remote management	■ The Connectware server to which to connect ■ The method to use to connect to the server ■ The security setting required to connect to the server ■ Keep-alive settings
Security	■ Authentication credentials ■ Password authentication ■ SSH public key authentication

You can configure one device, multiple devices, or a group at one time.

Accessing configuration information

▶ **To access the configuration pages so you can set up or edit settings:**

1. Select the device, devices, or groups you want to configure.
2. Right-click, and from the menu that opens, select **Device Configuration** and an option from the submenu:



   This step opens the Web UI for the device you selected.

3. From this point, see the documentation for your device.

Note that configuring alarms is included in this document because it requires using both the Device Management and Server Management applications.

Configuring Alarm Actions

CHAPTER 4

This chapter describes how to configure alarm notifications to be sent from Digi Connectware Manager.

Overview

You can configure your device server to generate an alarm based on the occurrence of specific events and send notification of the alarm to a SNMP Network Management Station (NMS) or an email recipient. You can configure an email notice, a SNMP trap, or both to be sent in response to any of the four supported trigger conditions.

Configuring alarm notifications involves using both the Server Management application and a per-device setup using the Device Management application.

This chapter describes how to create a condition alarm and configure notification.

About alarms and trigger conditions

An alarm consists of a trigger condition and the resulting action. Each alarm can have one or more actions. You configure trigger conditions definitions and alarm actions independently for a device or group of devices.

This list describes the supported alarm trigger conditions:

- Low RSSI (*rssi)*. You configure the RSSI level and the minimum period of time the average RSSI is allowed to stay below that level. When the average RSSI level drops below the configured RSSI level and stays below it for a configured time, an alarm is fired.
- Excessive cellular data (*cell_data*). You specify the amount of data (in bytes) and the interval of time (in minutes) in which that amount of data can be exchanged. When the exchange exceeds the values you configured, an action is fired.
- Management link down (*disconnected*). You specify the length of time a device is allowed to be down. When the disconnect time exceeds the value you configured, the server fires an action.
- Serial data pattern match (*pattern_match*). You specify a string of serial data, and when matching data is identified, an alarm is fired.

Configuring with the Server Management application

This section describes the tasks for setting up notification of a device alarm that can be sent to either SNMP Network Management Station (NMS) or an email recipient

Some of the configuration is saved to the physical device, so make sure the device has an active connection to the Connectware Manager before you save the configuration information.

This version of Connectware Manager supports a single SNMP NMS target.

Configuring SNMP trap notification

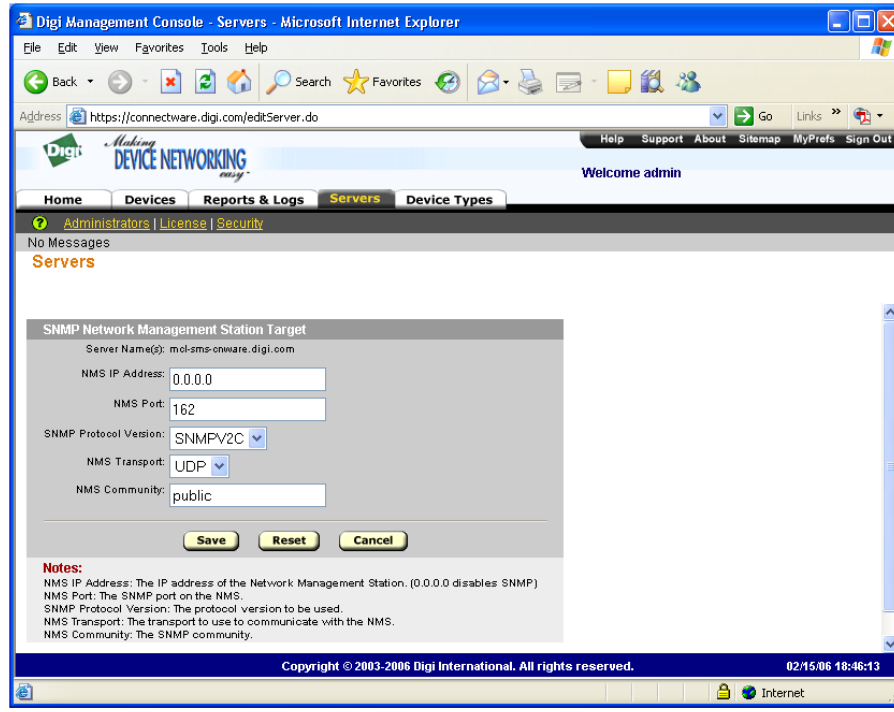
To send notifications from Connectware Manager to an NMS in response to the alarm trigger conditions, you need to configure the NMS target using the Server Management application. You also need to configure the device identity; this information is sent as part of the notificaiton

All alarm notifications you configure to be sent using the Connectware Manager is directed to this target.

▶ **To configure SNMP trap notification:**

1. Log in to the **Server Management** application.
2. Click the **Servers** tab.
3. On the gray selection bar, hover over **Advanced Settings** and select **SNMP NMS Target** from the drop-down menu.

The **NMS Target configuration** page opens:



4 Enter this information:

- The IP address of the NMS
- The port number the NMS is using to listen for SNMP trap/notification
- The SNMP protocol version

  (Note that Connectware Manager v3.1 currently supports only SNMP Version 2) and the transport TCP or UDP to be used
- The SNMP community to which the trap/notification should be sent

Then, to save your settings to the Connectware Manager database, click **Save**.

Note that setting the IP address to 0.0.0.0 disables all SNMP communications from the Connectware Manager. You might want to do this to prevent the NMS from receiving an unmanageable amount of notifications in some cases.

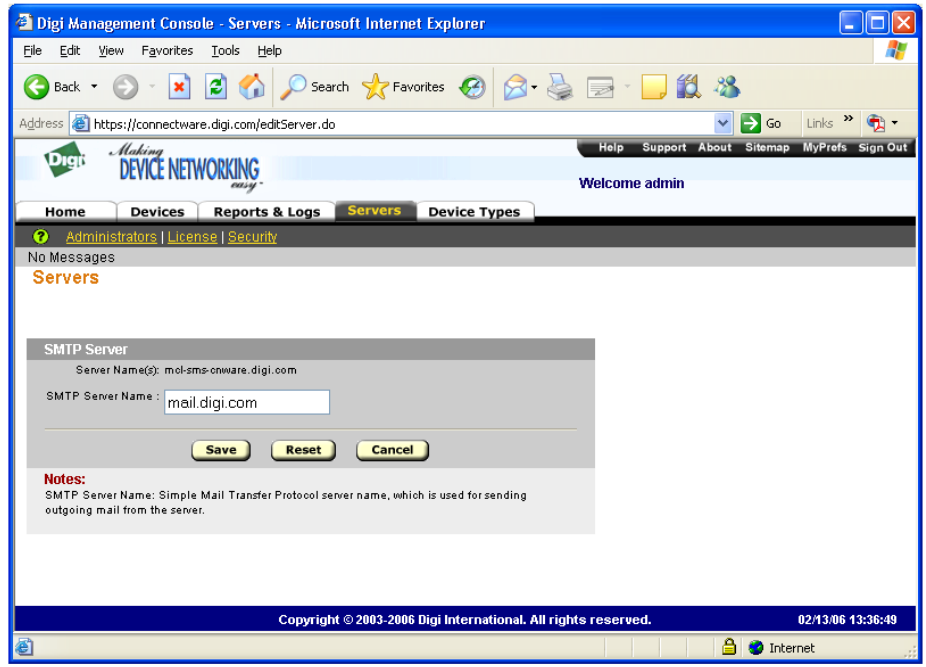
For example, suppose you have hundreds of devices configured to send a management link down notification, and you are a planning a network outage that would meet the trigger condition. Instead of reconfiguring all the devices, you can temporarily disable the notification at the server.

Configuring SMTP notification

▶ **To configure SMTP notification:**

1. Log in to the **Server Management** application.
2. Click the **Servers** tab.
3. On the gray selection bar, hover over **General Settings**, and from the drop-down menu, select **SMTP Server**.

   The **Servers** page opens:



4. In the **SMTP Server Name** input box, enter the name of the SMPT server that will send mail messages.
5. Click **Save**.

Configuring with the Device Management application

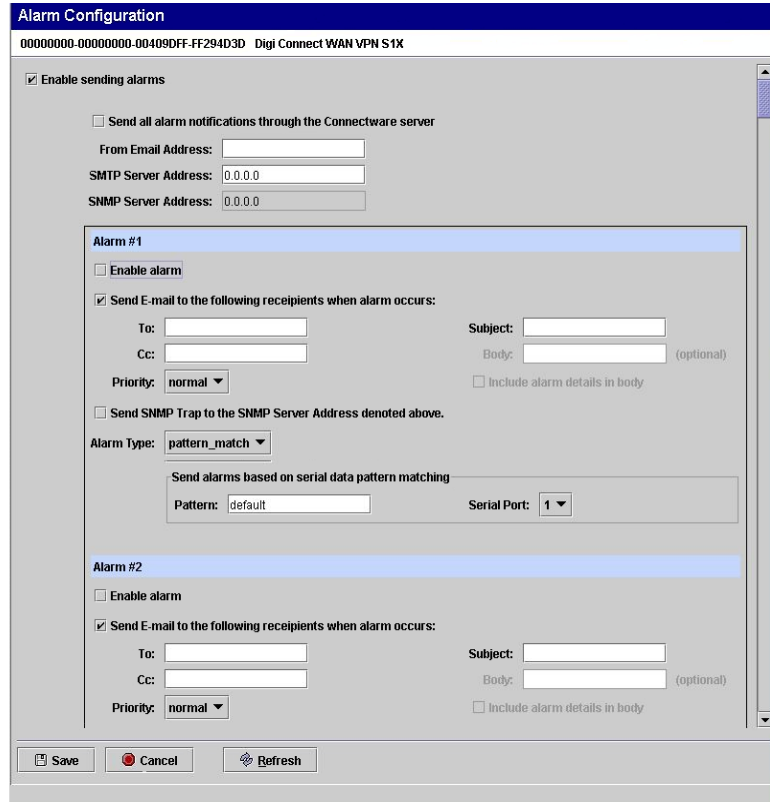
To configure the device alarm, you use the Device Management application. This section provides instruction for both SNMP and SMPT.

Configuring a device alarm (SNMP)

▶ **To configure a device alarm:**

1. Log in to the **Device Management** application.
2. From the **Device List**, select the device you want to configure.
3. Right-click the device you selected, and from the drop-down menu, select **Device Configuration → Alarms**.

   The **Alarm Configuration** page opens:



4 Do these steps:

- Check **Enable sending alarms** and **Send all notifications through the Connectware server.**

  (The trap will be sent through the Connectware server you specified in "Configuring SNMP trap notification.")
- Under the settings that are specific to **Alarm #1**, check **Enable alarm** and **Send SNMP trap to the SNMP Server Address denoted above.**
- From the **Alarm Type** drop-down menu, select the alarm trigger condition. (See the section "Examples of trigger notification," later in this chapter.)

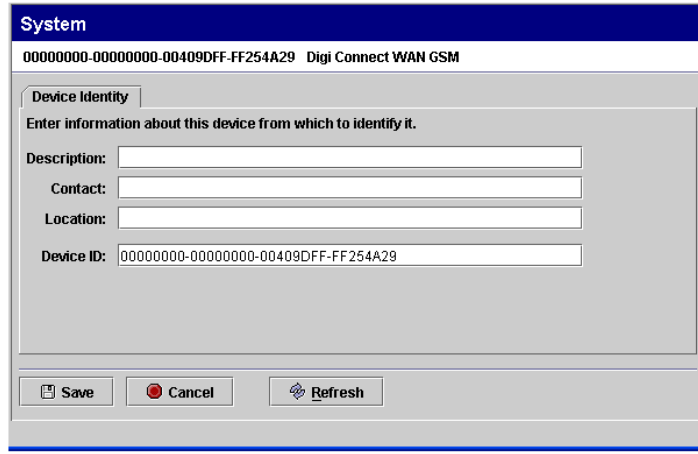
Then click **Save.**

In addition to configuring the device alarm, you need to configure the device identity. This information is sent as part of the SNMP notification.

▶ To configure the device identity:

1 From the **Device Configuration Navigation** bar, select **System.**

The **System** page opens:



2 Populate the **Description**, **Contact**, and **Location information** fields that are specific to the device.

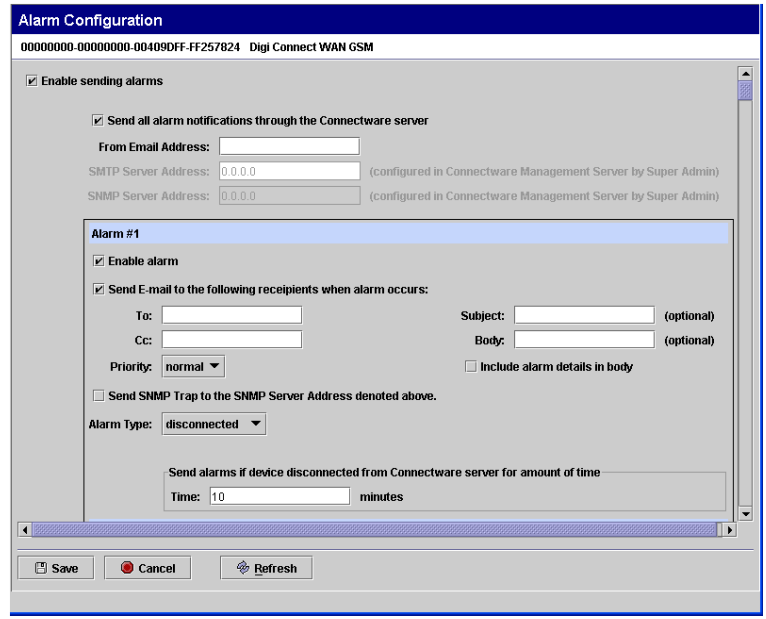
To save the information, click **Save.**

Configuring a device alarm (SMTP)

▶ **To configure a device alarm:**

1. Log into the **Device Management** application.
2. From the **Device List**, select the device you want to configure.
3. Right-click, and from the menu that opens, select **Device Administration → Alarms**.

   The **Alarm Configuration** page opens:



4. Do these steps:
   - Check **Enable sending alarms** and **Send all notifications through the Connectware server.** (These are global alarm settings.)
   - In the **From Email Address** input box, enter the address from which the email will come; for example:

     `connectware@yourdomain.com`
   - Under the settings that are specific for Alarm #1, in the **Subject** input box, enter text for the subject (optional).

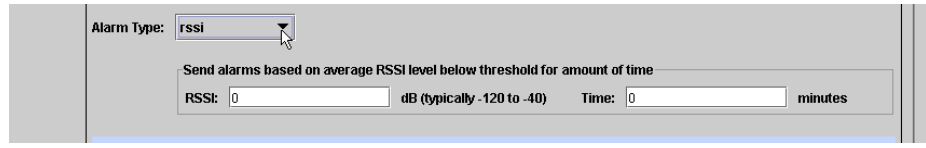
- In the **Body** input box, enter text for the body (optional).
- Check **Include alarm details in body.**
- From the **Alarm Type** drop-down menu, select the alarm trigger condition. (See the section "Examples of trigger notification," later in this chapter.)

Then click **Save**.

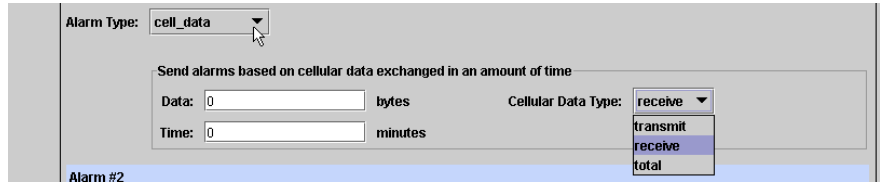
Examples of trigger condition configurations

You can configure other trigger conditions to send SNMP notification as well. The next three figures show the configuration of those trigger conditions.

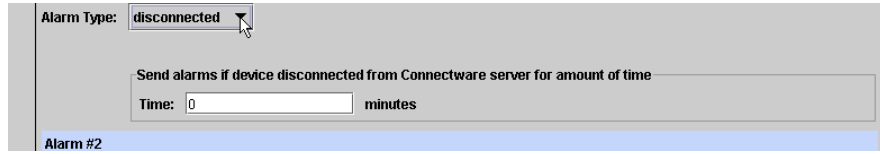
- Low RSSI trigger condition:



- Excessive cellular data trigger condition:



- Management link down trigger condition:



The next section, "SNMP notification/trap content", provides details about the contents of the SNMP notification and a sample trace of the notification resulting from the alarm configuration shown in "Configuring a device alarm."

SNMP notification/trap content

With the exception of the `SnmpTrapOID` variable, the information in each of the SNMP Trap/Notifications is same for each of the four alarm trigger. You can use the `SnmpTrapOID` variable, which contains an SNMP OID, to determine the trigger condition that caused the notification to be sent.

This table describes the Protocol Data Unit (PDU) used to transmit the notification information:

Offset	OID	Value	Description
1	1.3.6.1.2.1.1.3.0 (SNMPv2-MIB::sysUpTime.0)	Device up time	The device up time.
2	1.3.6.1.6.3.1.1.4.1.0 (SNMPv2-MIB::snmpTrapOID.0)	Trigger Condition OID	The OID that identifies the trigger condition. See the next table.
3	1.3.6.1.4.1.332.11.6.2.4	Device ID	The device identifier
4	1.3.6.1.4.1.332.11.6.2.2	Device Contact	The device contact field
5	1.3.6.1.4.1.332.11.6.2.3	Device Location	The device location field
6	1.3.6.1.4.1.332.11.6.2.1	Device Description	The device description field

This table describes the trigger conditions:

Notification	OID
Management Link Down	1.3.6.1.4.1.332.11.6.100.1
Low RSSI	1.3.6.1.4.1.332.11.6.100.2
Serial Data Pattern	1.3.6.1.4.1.332.11.6.100.3
Excessive Cellular Data	1.3.6.1.4.1.332.11.6.100.4

Here is a sample trace of a serial data pattern alarm:

```
Red Hat Linux release 8.0 (Psyche)
Kernel 2.4.18-14 on an i586
login: xxxxxx
Password: xxxxxxx
[root@linux]# snmptrapd -P -d tcp:1162
Error: Failed to connect to the agentx master agent: Unknown host (No such
file or directory)
2005-11-16 10:32:07 NET-SNMP version 5.0.1 Started.

Received 233 bytes from tcp:192.168.0.6:6942
0000: 30 81 E6 02  01 01 04 06  70 75 62 6C  69 63 A7 81    0.......public..
0016: D8 02 04 52  4B D7 61 02  01 00 02 01  00 30 81 C9    ...RK.a......0..
0032: 30 10 06 08  2B 06 01 02  01 01 03 00  43 04 04 05    0...+.......C...
0048: FD BC 30 19  06 0A 2B 06  01 06 03 01  01 04 01 00    ..0...+.........
0064: 06 0B 2B 06  01 04 01 82  4C 0B 06 64  03 30 32 06    ..+.....L..d.02.
0080: 0B 2B 06 01  04 01 82 4C  0B 06 02 04  04 23 30 30    .+.....L.....#00
0096: 30 30 30 30  30 30 2D 30  30 30 30 30  30 30 30 2D    000000-00000000-
0112: 30 30 34 30  39 44 46 46  2D 46 46 32  35 37 30 31    00409DFF-FF25701
0128: 43 30 1F 06  0B 2B 06 01  04 01 82 4C  0B 06 02 02    C0...+.....L....
0144: 04 10 4D 79  44 65 76 69  63 65 20 43  6F 6E 74 61    ..MyDevice Conta
0160: 63 74 30 20  06 0B 2B 06  01 04 01 82  4C 0B 06 02    ct0 ..+.....L...
0176: 03 04 11 4D  79 44 65 76  69 63 65 20  4C 6F 63 61    ...MyDevice Loca
0192: 74 69 6F 6E  30 23 06 0B  2B 06 01 04  01 82 4C 0B    tion0#..+.....L.
0208: 06 02 01 04  14 4D 79 44  65 76 69 63  65 20 44 65    .....MyDevice De
0224: 73 63 72 69  70 74 69 6F  6E                         scription

2005-11-16 10:33:10 192.168.0.6 [tcp:192.168.0.6:6942]:
  SNMPv2-MIB::sysUpTime.0 = Timeticks: (67501500) 7 days, 19:30:15.00
  SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.332.11.6.100.3
  SNMPv2-SMI::enterprises.332.11.6.2.4 = STRING: "00000000-00000000-
00409DFF-FF25701C"
  SNMPv2-SMI::enterprises.332.11.6.2.2 = STRING: "MyDevice Contact"
  SNMPv2-SMI::enterprises.332.11.6.2.3 = STRING: "MyDevice Location"
  SNMPv2-SMI::enterprises.332.11.6.2.1 = STRING: "MyDevice Description"
```

Managing Devices

CHAPTER 5

This chapter describes how to perform administrative tasks associated with managing devices.

Overview

This chapter describes how to perform administrative tasks such as:

- Backing up and restoring device settings
- Exporting and importing device settings
- Temporarily redirecting a device to a different destination
- Disconnecting devices
- Removing devices
- Restoring a device's factory default settings
- Rebooting a device
- Updating a device's firmware

Backing up and restoring device settings

It's a good practice to back up device configuration information so you'll have it if you need to restore settings. The information is maintained on the server.

Be aware that you can restore the settings *only* to the device you backed up, and not to any other devices.

Backing up device settings

▶ **To back up device settings (server):**

1. In the **Device List**, select the device you want to back up.
2. Select **Actions → Device Administration → Backup**.

The **Backup Device Settings** dialog box opens:

3 Click **Backup**.

You see a message that the settings are being backed up to the server.

Restoring device settings

▶ **To restore device settings (server):**

1 In the **Device List**, select the device to which you want to restore device settings.

2 Select **Actions → Device Administration → Restore**.

The **Restore Device Settings** dialog box opens:

3 Click **Restore**.

You see a message that the settings are being restored from the server.

Exporting and importing device settings

You can save a copy of a device's configuration information by *exporting* it. You specify a directory on your PC, and a file with the configuration settings is created there. The file is named with the device ID; if you export settings from multiple devices, a file is created for each device.

If you later want to use the exported settings on the same device, or on one or more other devices, you *import* them.

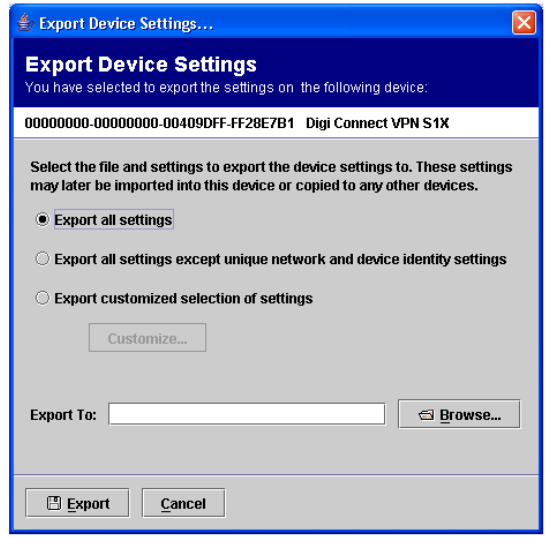
Exporting device settings

You can either export all the device settings or select the ones you want.

▶ **To export device settings:**

1. In the **Device List**, select one or more devices whose settings you want to export.
2. Select **Actions → Device Administration → Export**.

   The **Export Device Settings** dialog box opens:



3 Select the settings to export by clicking one of these:
   - **Export all settings**
   - **Export all settings except unique network and device identity settings**
   - **Export customized selection of settings**. If you select this option, click **Customize**, and select the settings you want to export.

4 To specify the directory to which to export the settings, do either of these steps:
   - Type the path name to the file in the input box next to **Export to**.
   - Click **Browse**, and navigate to the file.

5 Click **Export**.

Importing device settings

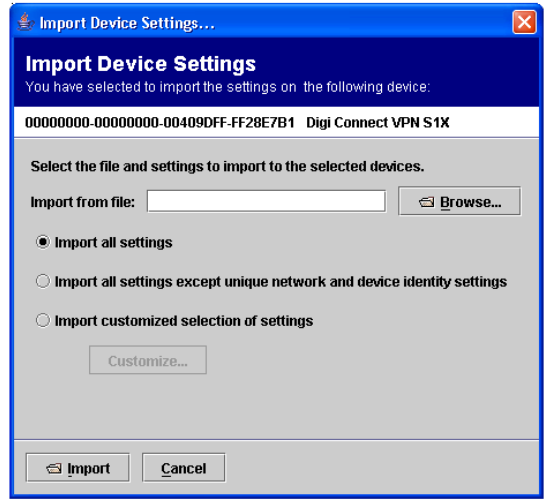
You can either import all the device settings or select the ones you want.

▶ **To import device settings:**

1 In the **Device List**, select one or more devices to which to import device settings.

2 Select **Actions → Device Administration → Import**.

3 The **Import Device Settings** dialog box opens:



4 To select the file with the settings you want to import, do either of these steps:
   - Type its name next to **Import from file**.
   - Click **Browse** and navigate to the file.

5 Select the settings to import by clicking either:
   - **Import all settings**
   - **Import all settings except unique network and device identity settings.**
   - **Import customized selection of settings**. If you select this option, click **Customize**, and select the settings you want to import.

6 Click **Import**.

Redirecting devices

Sometimes it's useful to direct a device to another destination temporarily.

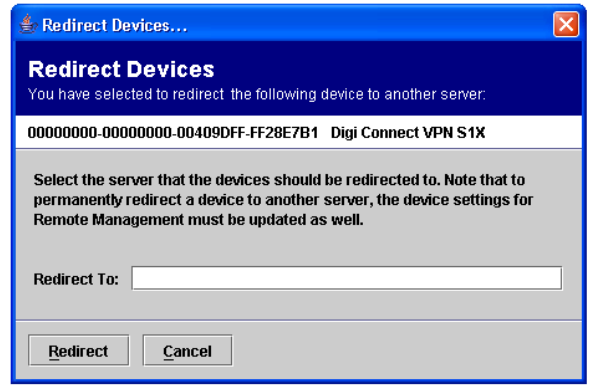
When you redirect a device, it remains active until it is disconnected. If you previously configured the device to automatically reconnect, it reconnects to its normal destination after the number of seconds you specified.

▶ **To redirect devices to a different destination:**

1 In the **Device List**, select one or more devices to redirect.

2 Select **Actions → Device Administration → Redirect**.

The **Redirect Devices** dialog box opens:



3 In the **Redirect To** input box, enter the destination server name.

4 Click **Redirect**.

Disconnecting and removing devices

When you *disconnect* a device, its name remains in the **Device List**, but its status changes to Disconnected.

When you *remove* a device, all the information that's stored on the server for that device is permanently deleted. If, however, the server is configured to auto provision a device when it reconnects, the device is automatically added back.

Disconnecting devices

▶ **To disconnect one or more devices from the server:**

1 In the **Device List**, select one or more devices.

2 Select **Actions → Device Administration → Disconnect**.

The **Disconnect Devices** dialog box opens:

3 Click **Disconnect**.

To see the updated connection status, refresh the page.

Removing devices

▶ **To remove devices:**

1. In the **Device List**, select one or more devices to remove.
2. Right-click, and from the menu that opens, select **Remove**.

   The **Remove Device** dialog box opens:

3. Click **Remove**.

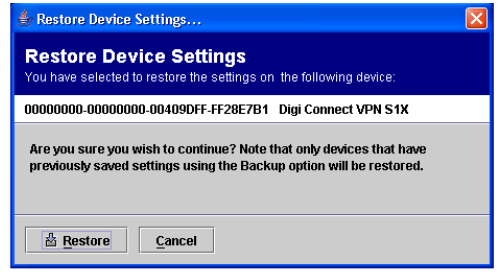
Restoring factory defaults

Device manufacturers ship devices with some configuration settings already defined. If it becomes necessary, you can easily restore a device's factory defaults.

▶ **To restore factory defaults:**

1. In the **Device List**, select one or more devices.

   The **Restore Factory Defaults** dialog box opens:



2 Select the settings to restore by clicking either:

- **Reset all settings to the factory defaults**
- **Reset all settings except unique network and device identity settings**
- **Reset customized selection of settings to the factory defaults.** If you click this option, click **Customize**, and then select the settings you want to restore to factory defaults.

3 Click **Restore**.

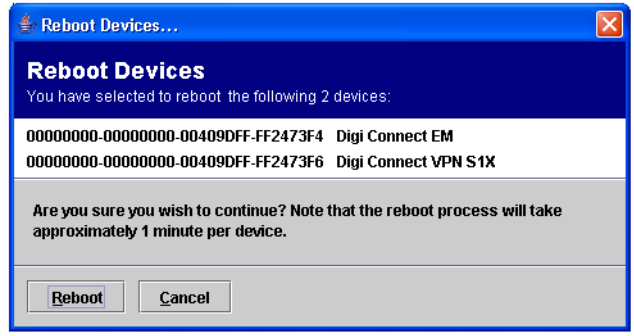
Rebooting a device

To reboot a device:

1 Select the device or devices to reboot.

2 Right-click, and from the menu that opens, select **Reboot**.

The **Reboot Device** dialog box opens:



3 Click **Reboot**.

Updating firmware

When a new firmware version becomes available, download it to a file on your PC. You'll use this file to update one or more devices.

▶ **To update a device's firmware version:**

1. In the **Device List**, select one or more devices to update.
2. Right-click, and from the menu that opens, select **Device Administration → Update Firmware**.

   The **Update Firmware** page opens:

3. To specify the firmware version to which you want to update, do either of these steps:
   - In the **Select Firmware** input box, enter the path name to the file in which you saved the new firmware.
   - Click **Open**, and navigate to the file in which you saved the new firmware.
4. Click **Update**.

Monitoring Device Statistics and Status

CHAPTER 6

This chapter describes how to monitor information about a device's settings and connections.

Overview

The Device Management application gives you quick access to detailed state and statistics about a device, such as:

- Device up time
- Amount of used and free memory
- Network settings
- Mobile settings

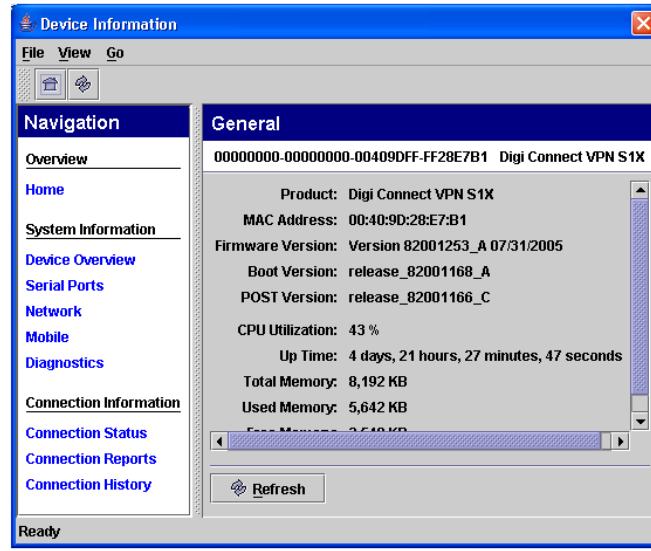
You also can monitor the state of the device's connection and see a connection report and connection history statistics.

Viewing device statistics

▶ **To view an overview of statistics about a device:**

1. In the **Device List**, select a device.
2. Right-click, and from the menu that opens, select **Device Information → Device Overview.**

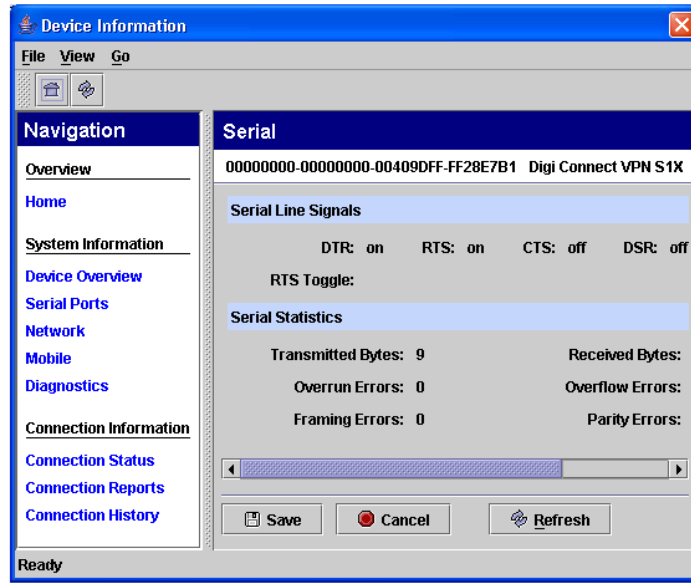
   The **General** page opens:



▶ **To view a device's serial port state:**

1. In the **Device List**, select a device.
2. Right-click, and from the menu that opens, select **Device Information → Serial**.

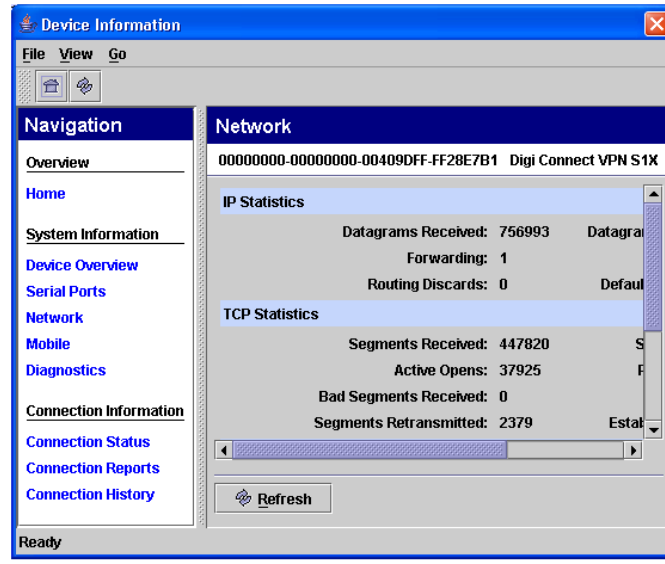
   The **Serial** page opens:



▶ **To view a device's network state:**

1. In the **Device List**, select a device.
2. Right-click, and from the menu that opens, select **Device Information → Network**.

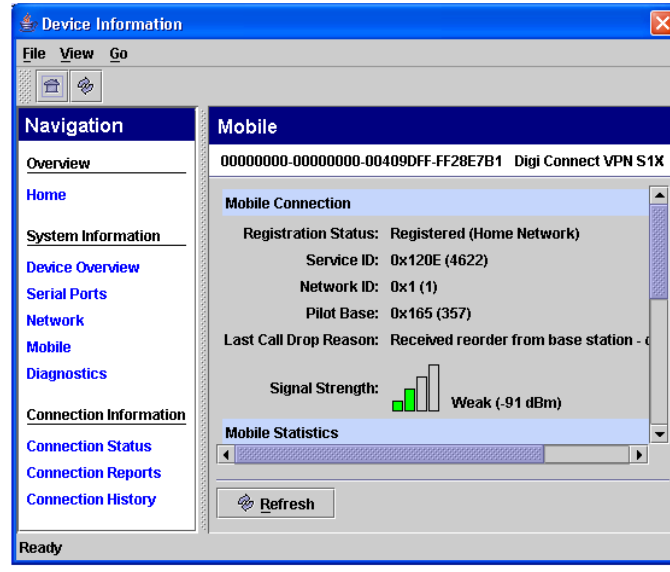
The **Network** page opens:



▶ **To view a device's mobile state:**

1. In the **Device List**, select a device.
2. Right-click, and from the menu that opens, select **Device Information → Mobile**.

   The **Mobile** page opens:



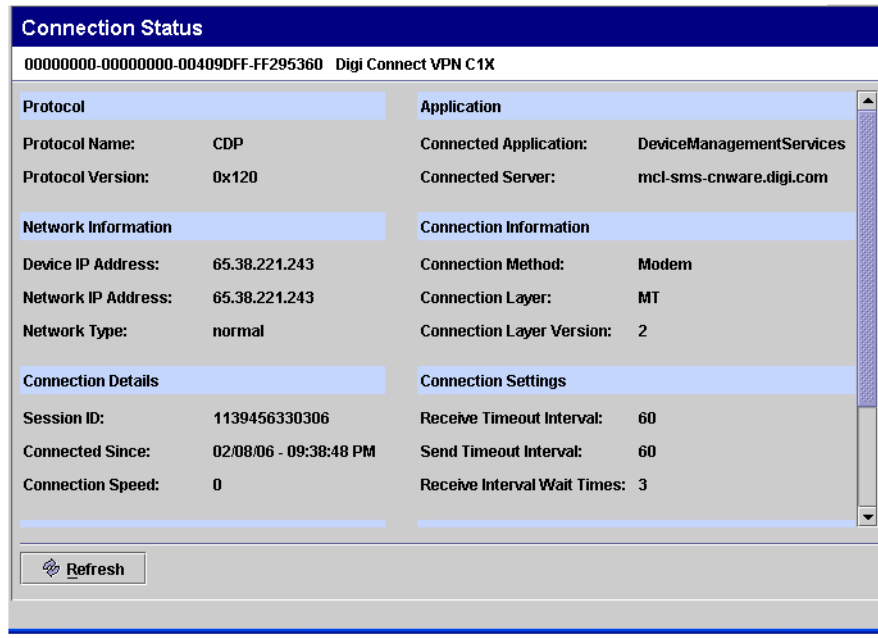
Viewing device status

When you monitor a device's state, you have quick access to information about the device's connection status and connection history. You also can view a report about the device's connections.

▶ **To view a device's connection status:**

1. In the **Device List**, select a device.
2. Right-click, and from the menu that opens, select **Device Information → Connection Status**.

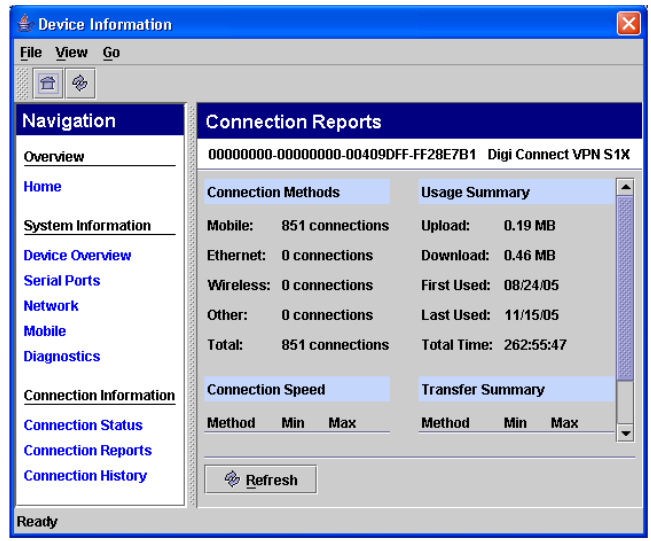
   The **Connection Status** page opens:



▶ **To view a device's connection reports:**

1. In the **Device List**, select a device.
2. Right-click, and from the menu that opens, select **Device Information → Connection Reports**.

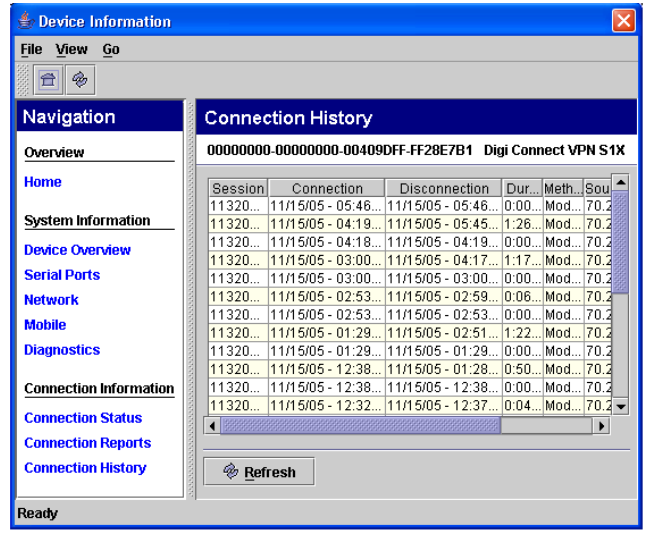
The **Connection Reports** page opens:



▶ **To view a device's connection history:**

1. In the **Device List**, select a device.
2. Right-click, and from the menu that opens, select **Device Information → Connection History**.

   The **Connection History** page opens:



Index

T

U

V


Digi®