

## Digi Connectware Manager Operator's Guide



# Digi Connectware Manager Operator's Guide

Part number/version: 90000770\_A Release date: February 2006 www.digi.com ©2005 Digi International Inc.

Printed in the United States of America. All rights reserved.

Digi, Digi International, the Digi logo, the Making Device Networking Easy logo, NetSilicon, a Digi International Company, NET+, NET+OS and NET+Works are trademarks or registered trademarks of Digi International, Inc. in the United States and other countries worldwide. All other trademarks are the property of their respective owners.

Information is this document is subject to change without notice and does not represent a commitment on the part of Digi International.

Digi provides this document "as is," without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of, fitness or merchantability for a particular purpose. Digi may make improvements and/or changes in this manual or in the product(s) and/or the program(s) described in this manual at any time.

This product could include technical inaccuracies or typographical errors. Changes are made periodically to the information herein; these changes may be incorporated in new editions of the publication.

## Contents

1
2
3
5
6
8
8
10
11
11
12
13
14
15
16
17

Chapter 3: Configuring Devices	21
Overview	22
Accessing configuration information	23
Chapter 4: Configuring Alarm Actions	25
Overview	26
About alarms and trigger conditions	26
Configuring with the Server Management application	27
Configuring SNMP trap notification	27
Configuring SMTP notification	29
Configuring with the Device Management application	30
Configuring a device alarm (SNMP)	30
Configuring a device alarm (SMTP)	32
Examples of trigger condition configurations	33
SNMP notification/trap content	34
Chapter 5: Managing Devices	37
Overview	38
Backing up and restoring device settings	38
Backing up device settings	38
Restoring device settings	39
Exporting and importing device settings	40
Exporting device settings	40
Importing device settings	41
Redirecting devices	42
Disconnecting and removing devices	43
Disconnecting devices	43
Removing devices	44
Restoring factory defaults	44
Rebooting a device	45
Updating firmware	45

Chapter	6:	Monitoring	Device	Statistics	a n d	Status	47
Overvi	ew			•••••			48
Viewin	ng d	evice statistic	s				48
Viewin	ng de	evice status					

# Using This Guide

 ${f R}$  eview 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 convention	ls 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 <b>menu name→ menu</b> 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.

This table describes the typographic conventions used in this guide:

#### **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

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 <a href="http://connectware">http://connectware</a> 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:

Digi Management Console - Sign-in - Microsoft Internet Explorer		
Elle Edit View Favorites Tools Help		- 🥂
🕝 Back 🔹 🌍 🔹 📓 🏠 🔎 Search 🤺 Favorites 🤣 🔗 - 🖕 🔂 🛄 🦓		
Address 🕘 http://connectware.digi.com/index.jsp	💌 🔁 Go	Links »
DEVICE NETWORKING		2
Welcome to Digi Connectware Management		
Use the buttons below to select your management preference:		
Server Management Device Management		
Helpline: 877-912-3444 <u>Dial Online Support</u> Visit <u>Dial International</u> for support and the latest technical information. Copyright © 2003-2005 Digi International. All rights reserved.		
2.		~
Cone 4	🥑 Internet	

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

A dialog box opens and prompts you to log in:

👙 Connectware Device Management 🛛 🛛 🔀								
	Welcome to	Connectware Device Management						
Digit	Username: Password:							
Login	<u>C</u> ancel	Logs						

- 4 Enter the default username and password:
  - Username: admin
  - **Password:** changeme

and then click Login.

The Connectware Device Management page opens:

👙 Connectware Devi	ce Management - connectware.d	ligi.com						×
File View Actions	Help							
G. 🗇								
Groups	Device Filters							
- 🗋 All Devices 🔺	Device Type		Device Status	3	Dev	ice Firmwa	re	
🗣 🗂 Demo Devic	All Devices	All Devices	;		All Devices			
	ConnectPort Display	Disconnec	ted		0.0.0.1			
	Digi Connect WAN GSM	Connected			2.0.0.0			-
	Digi Connect VPN Edge10				1.10.2.0			
- 🗋 PatrickBr	Digi Connect EM				1.9.0.0			-
- 🗋 TSL	Digi Connect VPN S1X	. 🕶			1.99.99.3			
- 🗋 Anet				******				00000
o cardvisic −	Device List - All Devices							
L - 🗋 UML	Device ID Device Type	Status ∆	IP Address	Host Name	Connection	Last Use	Firmware	
- Disst	00000000 ConnectPort Display	Unrestricted		zoe	Disconnect			
	00000000 Digi Connect WAN	Unrestricted			Disconnect			33
	00000000 Digi Connect WAN	Unrestricted	166.213.22		Disconnect	11/16/05	0.0.0.1	
TLD Den	00000000 Digi Connect VPN	Unrestricted	166.213.24		Disconnect	1/19/06	0.0.0.1	
- 🗋 SR Corp	00000000 Digi Connect EM	Unrestricted			Disconnect			-
- 🗅 BeiJing-	00000000 Digi Connect VPN	Unrestricted	68.240.165		Disconnect	12/20/05	2.0.0.0	-
-Бмсс	00000000 ConnectPort Display	Unrestricted			Disconnect			-
	00000000 ConnectPort Display	Unrestricted			Disconnect			-
PAR_Gr	00000000 Digi Connect EM	Unrestricted	100.010.00	AAA	Disconnect	0.11 0.10 5		-
L D ECS	UUUUUUUU Digi Connect WAN	Unrestricted	166.213.23	D.11 D.0	Disconnect	9/12/05	2.0.0.0	-
🕈 📑 Bradlee Co 🥃	DUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU	Unrestricted	166.213.24	BIIIS_RG	Disconnect	12/21/05	1.10.2.0	-
	Doctore ConnectPort Display	Unrestricted	193.129.91	ConnectM	Disconnect	9/10/05	1.9.0.0	-
	quantanting and connectionary	unresidded	11nn 7137		usconnect	INL/MILLS	<u></u>	
Server Status: Connect	ted (connectware.digi.com)							f

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.

7

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:

Device Filters								
Device Type			Device Status Device Firmware					
Digi Connect VPN C1X		All Dev	ices		All	Devices		
Digi Connect WAN VPN Edge10		Discon	inected		0.0	).0.1		
Digi Connect WAN V1X		Conne	cted		2.0	).0.0		
Digi Connect WAN VPN C1X					1.1	0.2.0		
Digi Connect RG Edge10					1.9	3.0.0		
Digi Connect WAN VPN					1.9	99.99.3		
ConnectPort WAN VPN	-				1.9	9.99.6		-
▲ ▼	00007				00000			000007
Device List - All Devices								
Device ID			Status	IP Address		Connection Status	Firmware	7
00000000-00000000-00409DFF-F	F29	998BA	Unrestricted	166.213.136.2	5 [	Disconnected	2.3.0.1	
00000000-00000000-00409DFF-F	F29	907ED	Unrestricted	70.12.149.53	(	Connected	2.3.0.0	
00000000-00000000-00409DFF-F	F29	998BB	Unrestricted	70.12.253.143	0	Disconnected	2.3.0.0	
00000000-00000000-00409DFF-F	F29	907EB	Unrestricted	70.12.40.234	[	Disconnected	2.2.1.1	
00000000-00000000-00409DFF-F	F29	3727E	Unrestricted	70.12.55.232	[	Disconnected	2.2.0.4	
00000000-00000000-00409DFF-F	F29	37280	Unrestricted	70.12.9.54	(	Connected	2.2.0.4	
00000000-00000000-00409DFF-F	F29	907E7	Unrestricted	70.13.151.138	0	Disconnected	2.2.0.2	
								•
								ſ

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**:

Device Filters								
Device Type			Device Sta	tus	Device Firmware			
Digi Connect VPN C1X	🔺 A	All Devi	ces		All Devices			
Digi Connect WAN VPN Edge10		Discon	nected		0.0.0.1			
Digi Connect WAN V1X		Connei	oted		2.0.0.	.0		
Digi Connect WAN VPN C1X					1.10.2	2.0		
Digi Connect RG Edge10	333				1.9.0.	.0		
Digi Connect WAN VPN					1.99.9	99.3		
ConnectPort WAN VPN	-				1.9.99	9.6		•
▲ ▼ ***********************************	000000	******						00007
Device List - All Devices								
Device ID			Status	IP Address	C	Connection Status	Firmware	$\nabla$
00000000-0000000-00409DFF-F	F290	)7ED	Unrestricted	70.12.149.53	Col	nnected	2.3.0.0	
00000000-00000000-00409DFF-F	F297	280	Unrestricted	70.12.9.54	Cor	nnected	2.2.0.4	
								_
						89999999		•

. . . . . . .

#### 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:

Device ID
☑ Device Type
☑ Status
🗹 Host Name
🗹 Firmware
☑ IP Address
Connection Status
☑ Last Use
🗆 Contact
Description
Location

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  $\rightarrow$  **Befresh**.

. . . . . . .

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  $\rightarrow$  Options.

The Application Settings dialog box opens:

🛓 Application Settings 🛛 🔀
Application Settings You have selected to update the application settings and options:
General Automatically refresh the devices and groups from the server Refresh Every: 600 secs
Save <u>C</u> ancel

- 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  $\rightarrow$  Messages & Logs.

The **Messages & Logs** window opens:

🔹 Messages ft Logs	×
<u>File View M</u> essages	
Messages	
DEBUG[Thread-6]: DeviceTypeManager.refreshDeviceTypeList - sending refresh command     DEBUG[CommandThread]: Executing RCM2: device_type_mgr     DEBUG[Thread-6]: DeviceManager.refreshDeviceList - sending refresh command     DEBUG[CommandThread]: Executing RCM2: device_mgr     DEBUG[CommandThread]: Executing RCM2: device_mgr	
Details	222
Message ID:	
Date/Time:	
Host System:	
Severity:	
Message:	
Details:	
Exceptions:	
Ready	

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  $\rightarrow$  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:

🗋 United States

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

- 🗣 📑 United States
  - 🗋 Atlanta
  - 🗋 Boston
  - 🗋 Chicado
  - 🗋 Detroit

#### 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  $\rightarrow$  New Device.

The Create Device dialog box opens:

🍰 Create Devic	e	×
Create De You have select	vice ed to create the following device(s):	
Simple Ad	vanced	
Select the set communicate	tings for this device. These settings should match the settings of the physical device to properly with the device.	
Device ID:	[	
Device Type:	ConnectPort Display	-
Host Name:		
Restriction:	Unrestricted      Restricted	
Create	<u>C</u> ancel	

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  $\rightarrow$  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:

🌢 Device Properties		
Device Properties You have selected to update the following 2 devices:		
00000000-0000000-00409DFF-FF28E7B6 Digi Connect VPN S13 00000000-00000000-00409DFF-FF28E7BB Digi Connect VPN S13	( (	
Select the settings to change for the list of devices. These settings should match the settings of the physical devices to properly communicate with them. Note that certain settings may not be available when configuring multiple devices.		
Device Type: Digi Connect VPN S1X	•	
Restriction: <ul> <li>Unrestricted</li> <li>Restricted</li> </ul>		
Save Cancel		

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  $\rightarrow$  New Group.

The Create Group dialog box opens:

👙 Create Gro	ир	$\mathbf{X}$	
Create Group You have selected to create a group of devices:			
Group: Description:			
Create In:	P     All Groups & Devices       P     Europe	•	
	- D Brussels - D London - D Paris	•	
Create	<u>C</u> ancel		

- 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:

🛓 Remove Group 🛛 🔀
Remove Group You have selected to remove a group of devices:
Are you sure you wish to continue? Note that the group and all subgroups will be permanantly removed from the server and no longer accessible.
Remove Group

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:

👙 Remove Device 🔀		
Remove Device You have selected to remove the following device:		
0000000-0000000-00409DFF-FF28D739 Digi Connect WAN Edge10		
Select how to remove the devices. Devices may be removed from the current group only or may be permanently removed from the server and all associated groups.		
Remove device from Server2		
$\bigcirc$ Remove device from the server and all associated groups		
<u>R</u> emove <u>C</u> ancel		

- **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:

🛓 Remove Device	×
Remove Device You have selected to remove the following device:	
0000000-0000000-0000000-00000044 ConnectPort Display	
Are you sure you wish to continue? Note that the devices will be permanantly removed from the server and no longer accessible.	
Remove Cancel	

3 Click Remove.

#### 

# Configuring Devices

CHAPTER 3

This chapter provides an overview of device configuration.

. . . . . . .

**1** 

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

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:

Common Tasks		
New Device		
Remove <u>D</u> evice		
Refresh Devices		
Copy To		
Device Tasks		
Device Configuration 🔸	Overview	Ctrl-O
Device Administration 🕨	Network	Ctrl-N
Device Information	Serial Ports	Ctrl-S
Device Properties	Alarms	
	System	Ctrl-Y
	Remote Management	Ctrl-R
	Security	Ctrl-P

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

 $T_{\rm his}$  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.

🗿 Digi Management Co	nsale - Servers - Microsoft Internet Explor	or	
File Edit View Favori	es Tools Help		
	🖸 🖻 🕡 🎤 Search 🏋 Pavorites 🍖		
Address 🕘 https://connect	ware.digi.com/editServer.do	<b></b> 🔁 Go	)Links » 📆 🕶
Digit Making	EWORKING	Help Support About Sitema	ap MyPrefs Sign Out
	LINUMINU asy	Welcome admin	
Home Device	s Reports & Logs Servers Device	e Types	
Administrators   Li	cense   Security		
Servers			
			^
SNMP Network Mana	gement Station Target		
Server Name(s):	mol-sms-onware.digi.com		
NMS IP Address:	0.0.0.0		
NMS Port:	162		
SNMP Protocol Version:	SNMPV2C V		
NMS Transport:			
NMS Community:	public		
	,		
	Save Reset Cancel		
Notes:			
NMS IP Address: The IP NMS Port: The SNMP po	address of the Network Management Station. (0.0.0.0 t on the NMS.	J disables SNMPJ	
NMP Protocol Version: NMS Transport: The tran	The protocol version to be used. sport to use to communicate with the NMS.		
NMS Community: The SM	IMP community.		~
	Copyright © 2003-2006 Digi Ir	nternational. All rights reserved.	02/15/06 18:46:13
é		🔒 🔮 Ir	iternet ,

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 dropdown menu, select **SMTP Server**.

The Servers page opens:

Digi Management Console - Servers - Microsoft Internet Explorer	
File Edit View Favorites Tools Help	
🕞 Back 🔹 ⊘ 🔹 📓 🏠 🔎 Search 🤺 Favorites 🤣 🔗 - چ 🚍 - 📴 鑬 🦓	
Address 🕘 https://connectware.digi.com/editServer.do	» 🔁 -
Help Support About Sitemap MyPre	fs Sign Out
Home Devices Reports & Logs Servers Device Types	
Administrators   License   Security	
No Messages	
SMTP Server	
Server Name(s): mol-sms-onware.digi.com SMTP Server Name : mail.digi.com	
Save Reset Cancel	
Notes: SMTP Server Name: Simple Mail Transfer Protocol server name, which is used for sending outgoing mail from the server.	
Copyright © 2003-2006 Digi International. All rights reserved. 02/13/	06 13:36:49
😂 🔷 Internet	

- 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**  $\rightarrow$  Alarms.

The Alarm Configuration page opens:

	0000-00403011	-11254D3D Digi C	JUNIECU YYAN VEN .			
Enable send	ling alarms					
	Send all alarm	notifications throu	ugh the Connectwa	re server		
F	rom Email Addı	ress:				
SM	ITP Server Add	ress: 0.0.0.0				
SN	MP Server Add	ress: 0.0.0.0				
Ala	arm #1					
	Enable alarm					
Ľ	Send E-mail to	the following rece	eipients when alarr	n occurs:		
	To:			Subje	ect:	
	Cc:			Bo	ndy:	(optional)
	Priority: nor	mal 🔻		🗆 Ir	nclude alarm details in bo	dy
	Send SNMP T	rap to the SNMP Se	erver Address deno	oted above.		
□ Ala	Send SNMP Ti irm Type: pat	rap to the SNMP Se tern_match ▼	erver Address deno	oted above.		
Ala	Send SNMP Ti irm Type: pat	rap to the SNMP Se tern_match 💌 nd alarms based o	erver Address deno on serial data patte	nted above. rn matching		
Ala	Send SNMP Tr Irm Type: pat Se Pa	rap to the SNMP Se tern_match ▼ nd alarms based o attern: default	erver Address deno on serial data patte	nted above. rn matching Seria	il Port: 1 💌	
Ala	Send SNMP Ti nrm Type: pat Se Pa	rap to the SNMP Se tern_match nd alarms based o attern: default	erver Address dend on serial data patte	nted above. rn matching Seria	I Port: 1 💌	
Ala	Send SNMP Tr nrm Type: pat Se Pa arm #2	rap to the SNMP Se tern_match ▼ nd alarms based o attern: default	erver Address deno	nted above. rn matching Seria	il Port: 1 💌	
Ala	Send SNMP Tr nrm Type: pat Se Pa arm #2 Enable alarm	rap to the SNMP Se tern_match nd alarms based o attern: default	erver Address deno	nted above. rn matching Seria	il Port: 1 V	
Ala Ala	Send SNMP Tr arm Type: pat Se Pa arm #2 Enable alarm Send E-mail to	rap to the SNMP Se tern_match nd alarms based o attern: default o the following rece	erver Address deno on serial data patte	nted above. rn matching Seria n occurs:	i Port: 1	
Ala Ala	Send SNMP Tr nrm Type: pat Se Pa arm #2 Enable alarm Send E-mail to To:	rap to the SNMP Se tern_match ▼ Ind alarms based of attern: default	erver Address dend	nted above. nn matching Seria n occurs: Subje	I Port: 1	
Ala Ala	Send SNMP Ti rm Type: pat Se Pa arm #2 Enable alarm Send E-mail to To: Cc:	rap to the SNMP Se tern_match ▼ Ind alarms based of attern: default	erver Address dend	nted above. nn matching Seria n occurs: Subje	I Port: 1	(optional)

- 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:

System	
0000000-000	00000-00409DFF-FF254A29 Digi Connect WAN GSM
Device Identi Enter informa	ity tion about this device from which to identify it.
Description:	
Contact:	
Location:	
Device ID:	0000000-0000000-00409DFF-FF254A29
🗄 Save	Cancel

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**  $\rightarrow$  Alarms.

The Alarm Configuration page opens:

unn o	onfiguration		
000000	-00000000-00409DFF-FF2	257824 Digi Conne	ect WAN GSM
Enable	e sending alarms		
	V Sond all alarm pati	fications through t	ha Cannortuiara capar
	From Email Address		
	SMTP Server Address	•	(configured in Connectware Management Server by Super Admin)
	SNMP Server Address	: 0.0.0.0	(configured in Connectware Management Server by Super Admin)
	Alarm #1		
	Enable alarm		
	Send E-mail to the	following receipier	nts when alarm occurs:
	To:		Subject: (optional)
	To:		Subject: (optional) Body: (optional)
	To: Cc: Priority: normal		Subject:
	To: Cc: Priority: normal	▼ o the SNMP Server	Subject:
	To: Cc: Priority: normal Send SNMP Trap t Alarm Type: discom	the SNMP Server	Subject:(optional) Body:(optional) Include alarm details in body Address denoted above.
	To: CC: Priority: normal Send SNMP Trap t Alarm Type: discom	othe SNMP Server     nected      r	Subject:
	To: CC: Priority: normal Send SNMP Trap t Alarm Type: discom Send a Time:	the SNMP Server     nected      r     larms if device disc	Subject:
	To: Cc: Priority: normal Send SNMP Trap t Alarm Type: discom Send a Time:	o the SNMP Server nected     find device disc	Subject:
	To: Cc: Priority: normal Send SNMP Trap t Alarm Type: discom Send a Time:	o the SNMP Server nected      r	Subject:
P San	To: Cc: Priority: normal Send SNMP Trap t Alarm Type: discont Send a Time: Priority: normal	othe SNMP Server nected     r	Subject:

- 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:

Alarm Ty	pe: rssi	
	Send alarms based on average RSSI level below threshold for amount of time	
	RSSI: 0 dB (typically -120 to -40) Time: 0 minutes	

Excessive cellular data trigger condition:

Alarm Type:	cell_data v	
	Send alarms based on cellular data exchanged in an amount of time	
	Data: 0 bytes Cellular Data Type:	receive 🔻
	Time: 0 minutes	transmit
		receive
Alarm #2		lutai

Management link down trigger condition:

Alarm Type:	disconnected 12
	Send alarms if device disconnected from Connectware server for amount of time
	Time: 0 minutes
Alarm #2	

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: xxxxxx [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.

Receiv	ved	233	3 by	/tes	fro	om 1	tcp:	:192.	. 168	3.0.	.6:6	5942					
0000:	30	81	E6	02	01	01	04	06	70	75	62	6C	69	63	Α7	81	0public
0016:	D8	02	04	52	4B	D7	61	02	01	00	02	01	00	30	81	С9	RK.a0
0032:	30	10	06	80	2B	06	01	02	01	01	03	00	43	04	04	05	0+C
0048:	FD	ВC	30	19	06	0 A 0	2B	06	01	06	03	01	01	04	01	00	0+
0064:	06	ОB	2B	06	01	04	01	82	4C	OВ	06	64	03	30	32	06	+Ld.02.
0080:	ОB	2B	06	01	04	01	82	4C	OВ	06	02	04	04	23	30	30	.+#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	OВ	2B	06	01	04	01	82	4C	ОB	06	02	02	CO+L
0144:	04	10	4D	79	44	65	76	69	63	65	20	43	6F	6 E	74	61	MyDevice Conta
0160:	63	74	30	20	06	ОB	2B	06	01	04	01	82	4C	ОB	06	02	ct0+L
0176:	03	04	11	4D	79	44	65	76	69	63	65	20	4C	6 F	63	61	MyDevice Loca
0192:	74	69	6F	6E	30	23	06	0 B	2B	06	01	04	01	82	4C	0 B	tionO#+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	6 F	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: "00000000-0000000-
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"
```

#### н. . . . . . . **F H** н. . . .

## Managing Devices . . . . . . . . . . . .

CHAPTER 5

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

**H H** 

### 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  $\rightarrow$  Device Administration  $\rightarrow$  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  $\rightarrow$  Device Administration  $\rightarrow$  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  $\rightarrow$  Device Administration  $\rightarrow$  Export.

The Export Device Settings dialog box opens:

👙 Export Device Settings	X
Export Device Settings You have selected to export the settings on the following device:	
00000000-0000000-00409DFF-FF28E7B1 Digi Connect VPN S1X	
Select the file and settings to export the device settings to. These setting: may later be imported into this device or copied to any other devices. Export all settings	;
O Export all settings except unique network and device identity settings	
O Export customized selection of settings	
Customize	_
Export To:	
Export Cancel	

- **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  $\rightarrow$  Device Administration  $\rightarrow$  Import.
  - 3 The Import Device Settings dialog box opens:

🖆 Import Device Settings 🛛 🔀								
Import Device Settings You have selected to import the settings on the following device:								
0000000-0000000-00409DFF-FF28E7B1 Digi Connect VPN S1X								
Select the file and settings to import to the selected devices.								
Import from file: 🔄 Browse								
Import all settings								
$\bigcirc$ Import all settings except unique network and device identity settings								
Import customized selection of settings								
Customize								
S import Cancel								

- 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  $\rightarrow$  Device Administration  $\rightarrow$  Redirect.

The Redirect Devices dialog box opens:

👙 Redirect Devices	X						
Redirect Devices You have selected to redirect the following device to another server:							
0000000-0000000-00409DFF-FF28E7B1 Digi Connect VPN S1X							
Select the server that the devices should be redirected to. Note that to permanently redirect a device to another server, the device settings for Remote Management must be updated as well.							
Redirect To:							
Redirect Cancel							

- 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  $\rightarrow$  Device Administration  $\rightarrow$  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.

100

. . . . . . . . . . . . . . . . .

- 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:

🔹 Reboot Devices	$\mathbf{X}$	
Reboot Devices You have selected to reboot the following 2 devices:		
00000000-0000000-00409DFF-FF2473F4 Digi Connect EM 00000000-00000000-00409DFF-FF2473F6 Digi Connect VPN S1X		
Are you sure you wish to continue? Note that the reboot process will take approximately 1 minute per device.		
<u>Reboot</u> <u>Cancel</u>		

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**  $\rightarrow$  **Update Firmware**.

The **Update Firmware** page opens:

🛓 Update Device Firmware	$\mathbf{X}$	
Update Device Firmware You have selected to update the firmware on the following device:		
0000000-0000000-00409DFF-FF28D6C6 Digi Connect WAN Edge10		
Select the firmware image to upload to these devices. Upon successfully sending the firmware image to the device, the firmware update may take another few minutes before completing. After successfully completing, the device will be automatically rebooted. Note that updating several devices simultaneously may cause the system to become unresponsive. See the User Guide for more information on how to update several devices.		

- **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

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**  $\rightarrow$  **Serial**. The **Serial** page opens:

🗄 Device Information	
<u>File View Go</u>	
Navigation	Serial
Overview	00000000-0000000-00409DFF-FF28E7B1 Digi Connect VPN S1X
Home	Serial Line Signals
System Information	DTR: on RTS: on CTS: off DSR: off
Device Overview	RTS Toggle:
Serial Ports	Serial Statistics
Mobile	Transmitted Bytes: 9 Received Bytes:
Diagnostics	Overrun Errors: 0 Overflow Errors:
Connection Information	Framing Errors: 0 Parity Errors:
Connection Status	
Connection Reports Connection History	Save Cancel & <u>R</u> efresh
Ready	

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**  $\rightarrow$  **Network**.

#### The Network page opens:

👙 Device Information	
<u>File View G</u> o	
<b>A</b>	
Navigation	Network
Overview	00000000-00000000-00409DFF-FF28E7B1 Digi Connect VPN S1X
Home	IP Statistics
System Information	Datagrams Received: 756993 Datagra
Device Overview	Forwarding: 1
Serial Ports	Routing Discards: 0 Defaul
Network	TCP Statistics
Mobile	Segments Received: 447820 S
Diagnostics	Active Opens: 37925 F
Connection Information	Bad Segments Received: 0
	Segments Retransmitted: 2379 Estal
Connection Status	
Connection Reports	
Connection History	<del> </del>
Ready	1

To view a device's mobile state:

- 1 In the **Device List**, select a device.
- 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**  $\rightarrow$  **Connection Status**.

The Connection Status page opens:

Connection Statu	S		
00000000-00000000-00	409DFF-FF295360 Digi Con	nect VPN C1X	
Protocol		Application	
Protocol Name:	CDP	Connected Application:	DeviceManagementServices
Protocol Version:	0x120	Connected Server:	mcl-sms-cnware.digi.com
Network Information		Connection Information	
Device IP Address:	65.38.221.243	Connection Method:	Modem
Network IP Address:	65.38.221.243	Connection Layer:	MT
Network Type:	normal	Connection Layer Version:	2
Connection Details		Connection Settings	
Session ID:	1139456330306	Receive Timeout Interval:	60
Connected Since:	02/08/06 - 09:38:48 PM	Send Timeout Interval:	60
Connection Speed:	0	Receive Interval Wait Times:	3
🏶 <u>R</u> efresh			

#### 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**  $\rightarrow$  **Connection Reports**.

#### The Connection Reports page opens:

🗄 Device Information					X
File View Go					
Navigation	Connect	ion Reports			
Overview	00000000-0	0000000-00409DF	F-FF28E7B1 C	igi Connect VPN	IS1X
Home	Connection	Methods	Usage Sum	imary	A
System Information	Mobile:	851 connections	Upload:	0.19 MB	000000
Device Overview	Ethernet:	0 connections	Download:	0.46 MB	10000
Serial Ports	Wireless:	0 connections	First Used:	08/24/05	
Network	Other:	0 connections	Last Used:	11/15/05	
Mobile Diagnostics	Total:	851 connections	Total Time:	262:55:47	
Connection Information	Connection	Speed	Transfer Su	ımmary	
Connection Status	Method	Min Max	Method	Min Max	_
Connection Reports					
Connection History	🏾 🏶 <u>R</u> efre	sh			
Ready	,				

- ► 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**  $\rightarrow$  **Connection History**.

The **Connection History** page opens:

👙 Device Information	
<u>File View G</u> o	
1	
Navigation	Connection History
Overview	00000000-0000000-00409DFF-FF28E7B1 Digi Connect VPN S1X
Home	Session Connection Disconnection Dur MethSou
System Information	11320 11/15/05 - 05:46 11/15/05 - 05:46 0:00 Mod 70.2 11320 11/15/05 - 04:19 11/15/05 - 05:45 1:26 Mod 70.2
Device Overview	11320 11/15/05 - 04:18 11/15/05 - 04:19 0:00 Mod 70.2
Serial Ports	11320 11/15/05 - 03:00 11/15/05 - 03:00 0:00 Mod 70.2
Network	11320 11/15/05 - 02:53 11/15/05 - 02:59 0:06 Mod 70.2
Mobile	11320 11/15/05 - 02:53 11/15/05 - 02:53 0:00 Mod 70.2 11320 11/15/05 - 01:29 11/15/05 - 02:51 1:22 Mod. 70.2
Diagnostics	11320 11/15/05 - 01:29 11/15/05 - 01:29 0:00 Mod 70.2
	11320 11/15/05 - 12:38 11/15/05 - 01:28 0:50 Mod 70.2
Connection Information	11320 11/15/05 - 12:38 11/15/05 - 12:38 0:00 Mod 70.2
Connection Status	11320 11/15/05 - 12:32 11/15/05 - 12:37 0:04 Mod 70.2
Connection Reports	
Connection History	🐵 Refresh
Ready	í

## Index

#### A

alarm trigger conditions 26 automatic refreshing 11

#### B

backing up device settings 38

#### С

configuring a device alarm 30 creating a group 16

#### D

default username and password 7 device selecting 16 device alarm, configuring 30 device identity 31 device information, refreshing 11 Device Management Application 26 device settings backing up 38 exporting 40 importing 41 restoring 39 devices adding 14 checking connection status of 51 copying or moving to a group 16 disconnecting 43 rebooting 45 redirecting to a different destination 42 removing 44 removing from a group 18 removing from the Device List 18 restoring factory defaults of 44 restricted and unrestricted 14 selecting 16 updating firmware 45 viewing connection history 52 Digi Connectware Manager, described 2 disconnecting devices 43

#### Ε

Excessive cellular data alarm trigger condition 26 exporting device settings 40

#### F

factory defaults, restoring to a device 44 filtering information in the Device List 8 firmware, updating 45

#### G

group copying or moving devices to 16 removing 17 removing devices from 18 selecting 15

#### 

importing device settings 41

#### J

Java Runtime Environment 6

#### L

logging in to Digi Connectware Manager 6 Low RSSI alarm trigger condition 26

#### Μ

Management link down alarm trigger condition 26 messages selecting severity level of 13 viewing 12 monitoring device connection 51

#### Ρ

password, default 7

#### R

rebooting a device 45 redirecting devices to a different destination 42 refreshing device information 11 removing a group 17 removing devices 43 restoring device settings 38 restoring factory defaults to a device 44 restricted device, defined 14 restriction state, changing 15

#### S

sample trace 35 selecting devices or groups 15 Serial data pattern match alarm trigger condition 26 Server Management application 2, 26 severity level of messages received, selecting 13

### Т

trigger condition configurations 33

#### U

unrestricted device, defined 14 updating firmware 45 username, default 7

#### ۷

viewing device connection history 52 viewing messages 12

