



Intermec



User's Manual



IF61 Fixed Reader

Intermec Technologies Corporation

Worldwide Headquarters
6001 36th Ave.W.
Everett, WA 98203
U.S.A.

www.intermec.com

The information contained herein is provided solely for the purpose of allowing customers to operate and service Intermec-manufactured equipment and is not to be released, reproduced, or used for any other purpose without written permission of Intermec Technologies Corporation.

Information and specifications contained in this document are subject to change without prior noticed and do not represent a commitment on the part of Intermec Technologies Corporation.

© 2007-2008 by Intermec Technologies Corporation. All rights reserved.

The word Intermec, the Intermec logo, Norand, ArciTech, Beverage Routebook, CrossBar, dcBrowser, Duratherm, EasyADC, EasyCoder, EasySet, Fingerprint, i-gistics, INCA (under license), Intellitag, Intellitag Gen2, JANUS, LabelShop, MobileLAN, Picolink, Ready-to-Work, RoutePower, Sabre, ScanPlus, ShopScan, Smart Mobile Computing, SmartSystems, TE 2000, Trakker Antares, and Vista Powered are either trademarks or registered trademarks of Intermec Technologies Corporation.

There are U.S. and foreign patents as well as U.S. and foreign patents pending.

Wi-Fi is a registered certification mark of the Wi-Fi Alliance.

Microsoft, Windows, and the Windows logo are registered trademarks of Microsoft Corporation in the United States and/or other countries.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (www.openssl.org).

This product includes cryptographic software written by Eric Young (EAY@cryptsoft.com).

Part of the software embedded in this product is gSOAP software.

Portions created by gSOAP are Copyright (C) 2001-2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

In no event shall the author be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

ACE(TM), TAO(TM), CIAO(TM), and CoSMIC(TM) (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University, Copyright (c) 1993-2006, all rights reserved.

Document Change Record

This page records changes to this document. The document was originally released as Revision 001.

Revision	Date	Description of Change
003	4/2008	<p>Manual was revised to support IF61 firmware version 2.1x.</p> <p>Moved edgware application information to new documents:</p> <ul style="list-style-type: none">• SAP Device Controller information, previously in Appendix B, is now in the <i>IF61 SAP Device Controller User's Guide</i> (P/N 934-025-xxx).• Application Level Engine (ALE) information, previously in Chapter 3, is now in the <i>IF61 Application Level Engine (ALE) User's Guide</i> (P/N 934-026-xxx). <p>Added new information for RFID services, including BRI and LLRP configuration settings, and the Device Configuration web service.</p>
002	11/2007	<p>Added information and procedures for configuring, using, and troubleshooting the 802.11a/b/g radio.</p> <p>Updated screenshots to match the revised web browser interface.</p> <p>Minor revisions made to RFID application development sections.</p>

Contents

Before You Begin	xi
Safety Information	xi
Global Services and Support	xi
Warranty Information	xi
Web Support	xi
Telephone Support	xii
Service Location Support	xii
Who Should Read This Manual	xiii
Related Documents	xiii
Patent Information	xiv
1 Getting Started	1
Overview of the IF61	2
Understanding the Network and Power Ports	4
Understanding the LEDs	6
About the Intermec Ready-To-Work Indicator	7
Understanding the Top Panel Ports	8
Connecting to the IF61	9
Assigning an Initial IP Address	9
Using the Web Browser Interface	11
Saving Configuration Changes	14
Disabling Help in the Web Browser Interface	14
Installing the IF61	15
Choosing a Mounting Location	15
Connecting the IF61 to Your Network	16
Setting the Date and Time	17
Using the IF61 Securely	18
2 Configuring Network Settings	19
Configuring Settings for Your Network	20
Configuring Ethernet Settings	20
Configuring the 802.11 Radio	23
Setting the 802.11 Network Mode	27
Configuring Common Network Settings	27

Contents

Configuring Security	30
Controlling Access Services	30
Setting Up Logins	33
Configuring the IF61 to Use a Password Server	33
Changing the Default Login	35
Disabling Access Via the Serial Port.	36
Configuring Wireless Security	37
Configuring WEP Security	38
Configuring Dynamic WEP/802.1x Security	39
Configuring WPA Personal (PSK) Security	41
Configuring WPA Enterprise (802.1x) Security.	43
Configuring WPA2 Personal (PSK) Security	45
Configuring WPA2 Enterprise (802.1x) Security.	47
Managing Certificates	49
Viewing Certificates	50
Installing and Uninstalling Certificates	50

3 Developing and Using RFID Applications 53

RFID Applications and the IF61	54
Using the RFID Resource Kit	54
Creating RFID Applications for the IF61	55
Delivering Applications to the IF61.	55
About Configuration Files.	56
Auto-Starting Applications at Boot Time.	57
IF61 .NET Support.	57
IF61 Java Support	57
Executing Java Applications	57
Java Support for Microsoft SQL Server and Sybase.	58
IF61 JavaScript Support	59
Installing RFID Applications on the IF61	59
Managing Applications	60
About the IF61 Edgeware Applications	61
Upgrading or Installing Edgeware Applications	62
About RFID Services.	63
Configuring BRI Settings	63
Changing BRI Attribute Settings.	63
About BRI Attribute Settings	64

Tag Types	64
Read Tries	65
Write Tries.	65
Lock Tries	65
Field Separator.	65
ID Report	65
No Tag Report.	66
Report Timeout.	66
Timeout Configuration Mode	66
Select Tries.	66
Unselect Tries	66
Session	67
Initial Q.	67
Initialization Tries	67
ID Tries.	67
ID Timeout	67
Antenna Tries	67
Antenna Timeout.	68
Dense Reader Mode.	68
LBT Scan Enable	68
LBT Channel.	68
Field Strength 1 to 4	68
Antenna Sequence: First through Eighth	69
Configuring the BRI Server	69
Viewing the BRI Server Log	70
Configuring LLRP Settings.	71
About the Developer Tools	73
Testing the GPIO Interfaces	73
Sending BRI Commands and Running Scripts.	74
Using the Workbench.	76
Configuring a JavaScript File to Auto-Run at Boot Time	77
Editing Remote Startup Files	79

4 Managing, Troubleshooting, and Upgrading the IF61 . . 81

Managing the IF61	82
Using the Device Configuration Web Service	82
Using Simple Network Management Protocol (SNMP)	84
Using SmartSystems Foundation.	87
Configuring the IF61 with Intermec Settings	88

Contents

Using Wavelink Avalanche	89
Importing and Exporting Files	91
Using the IF61 FTP Server	91
Using CIFS File Sharing	92
Accessing the IF61 via the Linux Shell	93
Opening a Secure Shell (SSH) Connection	93
Opening a Telnet Connection	94
Using a Communications Program	95
Opening a Serial Connection to the IF61	96
Maintaining the IF61	97
Viewing the System Log	97
Viewing the About Screen	98
Using the LEDs to Locate the IF61	99
Restoring the IF61 to the Default Configuration	100
Rebooting the IF61	101
Managing USB Devices	101
Troubleshooting the IF61	103
Problems While Working With RFID	103
Connecting Directly to the RFID Module	104
Problems With Connectivity	105
Calling Intermec Product Support	107
Accessing Intermec Web Pages	107
Upgrading Firmware	108
Configuring the Firmware Upgrade	108
Installing the Firmware Upgrade	110
Upgrading from the Web Browser Interface	110
Upgrading with SmartSystems Server	111
Upgrading with a USB Drive	112
Upgrading with an Avalanche Package	112
5 Using the IF61 GPIO Interfaces	113
About the GPIO Interfaces	114
Accessing the Interfaces	114

Contents

Using the Input Interfaces	115
IF61 Powered Input	115
Isolated Input Interface	116
Open Collector Input Interface	116
Using the Output Interfaces	117
Switching the High Side Using IF61 Power	118
Switching the Low Side Using IF61 Power	118
Switching the High Side Using External Power	119
Driving a DC Relay to Control an AC Load	119
Using the Power Interface	120
A Specifications	121
IF61 Specifications	122
RFID Specifications	123
Port Pin Assignments	124
GPIO Port	124
Serial Ports (COM1, COM2)	125
Ethernet Port	125
I Index	127

Contents

Before You Begin

This section provides you with safety information, technical support information, and sources for additional product information.

Safety Information

Your safety is extremely important. Read and follow all cautions in this document before handling and operating Intermec equipment. Your equipment and data can be damaged if you do not follow the safety cautions.

This section explains how to identify and understand cautions and notes that are in this document.



A caution alerts you to an operating procedure, practice, condition, or statement that must be strictly observed to prevent equipment damage or destruction, or corruption or loss of data.



Note: Notes either provide extra information about a topic or contain special instructions for handling a particular condition or set of circumstances.

Global Services and Support

Warranty Information

To understand the warranty for your Intermec product, visit the Intermec web site at www.intermec.com, click **Support > Returns and Repairs**, then click **Warranty**.

Disclaimer of warranties: The sample code included in this document is presented for reference only. The code does not necessarily represent complete, tested programs. The code is provided “as is with all faults.” All warranties are expressly disclaimed, including the implied warranties of merchantability and fitness for a particular purpose.

Web Support

Visit the Intermec technical knowledge base (Knowledge Central) at intermec.custhelp.com to review technical information or to request technical support for your Intermec product.

Before You Begin

Telephone Support

These services are available from Intermec Technologies Corporation.

Services	Description	In the USA and Canada call 1-800-755-5505 and choose this option
Order Intermec products	<ul style="list-style-type: none">Place an order.Ask about an existing order.	1 and then choose 2
Order Intermec media	Order printer labels and ribbons.	1 and then choose 1
Order spare parts	Order spare parts.	1 or 2 and then choose 4
Product Support	Talk to technical support about your Intermec product.	2 and then choose 2.
Service	<ul style="list-style-type: none">Get a return authorization number for authorized service center repair.Request an on-site repair technician.	2 and then choose 1

Outside the U.S.A. and Canada, contact your local Intermec representative. To search for your local representative, visit www.intermec.com and choose **About Us > Contact Us**.

Service Location Support

For the most current listing of service locations, click **Support > Returns and Repairs > Repair Locations**.

For technical support in South Korea, use the after service locations listed below:

AWOO Systems

102-1304 SK Ventium

522 Dangjung-dong

Gunpo-si, Gyeonggi-do Korea, South 435-776

Contact: Mr. Sinbum Kang

Telephone: +82-31-436-1191

E-mail: sbkang@awoo.co.kr

IN Information System PTD LTD

6th Floor
Daegu Venture Center Bldg 95
Shinchun 3 Dong
Donggu, Daegu City, Korea
E-mail: jmyou@idif.co.kr or korlim@gw.idif.co.kr

Who Should Read This Manual

This user's manual is for the person who is responsible for installing, configuring, and maintaining the IF61 Fixed Reader.

This manual provides you with information about the features of the IF61, and how to install, configure, operate, maintain, and troubleshoot it.

Before you work with the IF61, you should be familiar with your network and general networking terms, such as IP address. You should also be familiar with your RFID system.

This revision of the manual supports the IF61 with firmware version 2.1x.

Related Documents

This table contains a list of related Intermec documents and their part numbers.

Document Title	Part Number
<i>IF61 Fixed Reader Quick Reference Guide</i>	930-190-xxx
<i>IF61 Compliance Insert</i>	933-089-xxx
<i>Important BRCM1017 Radio Information</i>	933-125-xxx
<i>Important IM5 Information</i>	075231-xxx
<i>Basic Reader Interface Programmer's Reference Manual</i>	937-000-xxx
<i>IF61 SAP Device Controller User's Guide</i>	934-025-xxx
<i>IF61 Application Level Events (ALE) Engine User's Guide</i>	934-026-xxx
<i>ALE Store and Forward User's Guide</i>	934-034-xxx
<i>Device Configuration Web Services Command Reference Manual</i>	937-012-xxx

The Intermec web site at www.intermec.com contains our documents (as PDF files) that you can download for free.

Before You Begin

To download documents

- 1** Visit the Intermec web site at www.intermec.com.
- 2** Click **Support > Manuals**.
- 3** In the **Select a Product** field, choose the product whose documentation you want to download.

To order printed versions of the Intermec manuals, contact your local Intermec representative or distributor.

Patent Information

Product is covered by one or more of the following patents:

4,739,328; 4,786,907; 4,864,158; 4,888,591; 4,910,794;
4,999,636; 5,030,807; 5,055,659; 5,070,536; 5,280,159;
5,295,154; 5,349,678; 5,394,436; 5,425,051; 5,428,636;
5,483,676; 5,504,485; 5,504,746; 5,521,601; 5,546,397;
5,550,547; 5,574,979; 5,592,512; 5,673,037; 5,680,633;
5,682,299; 5,696,903; 5,740,366; 5,763,867; 5,777,561;
5,790,536; 5,825,045; 5,828,318; 5,828,693; 5,844,893;
5,850,181; 5,850,187; 5,862,171; 5,940,771; 5,942,987;
5,960,344; 5,995,019; 6,078,251; 6,121,878; 6,122,329;
6,172,596; 6,195,053; 6,249,227; 6,280,544; 6,286,762;
6,286,763; 6,288,629; 6,360,208; 6,384,712; 6,404,325;
6,429,775; 6,486,769; 6,501,807; 6,525,648; 6,639,509;
6,645,327; 6,677,852; 6,768,414; 6,784,789; 6,816,063;
6,830,181; 6,838,989; 6,859,190; 6,906,615; 6,919,793;
6,944,424; 7,075,413; 7,103,087; 7,106,196; 7,117,374;
7,121,467; 7,123,129; 7,158,046; 7,158,091.

There may be other U.S. and foreign patents pending.



1 Getting Started

This chapter introduces the IF61 Fixed Reader, explains the ports and LEDs, and explains how the reader fits into your network. It contains these topics:

- Overview of the IF61
- Connecting to the IF61
- Installing the IF61
- Setting the Date and Time
- Using the IF61 Securely

Overview of the IF61

The IF61 Fixed Reader is an RFID reader that provides connectivity between tag data and an enterprise system.



The IF61 Fixed Reader uses an EPCglobal Gen 2-certified IM5 Module (86x MHz RFID frequency band).



The IF61 Fixed Reader uses an EPCglobal Gen 2-certified IM5 Module (915 MHz RFID frequency band).



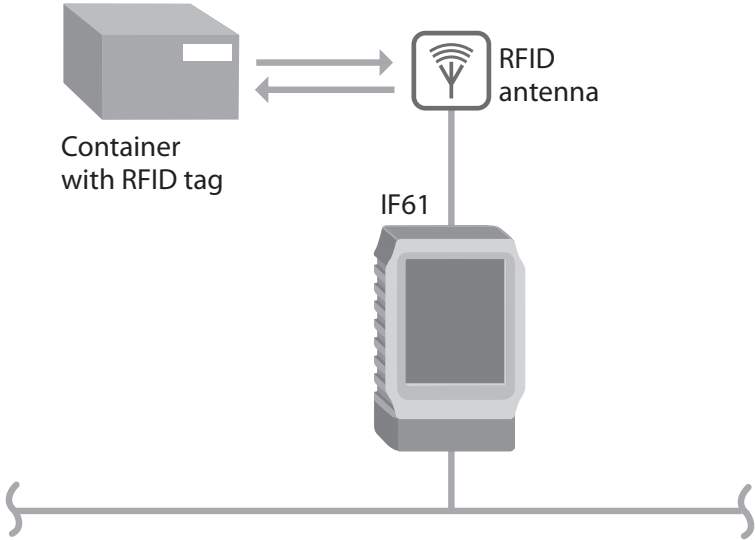
IF61 Fixed Reader



Note: The IF61 does not ship with RFID antennas. For more information on these accessories, contact your Intermec sales representative.

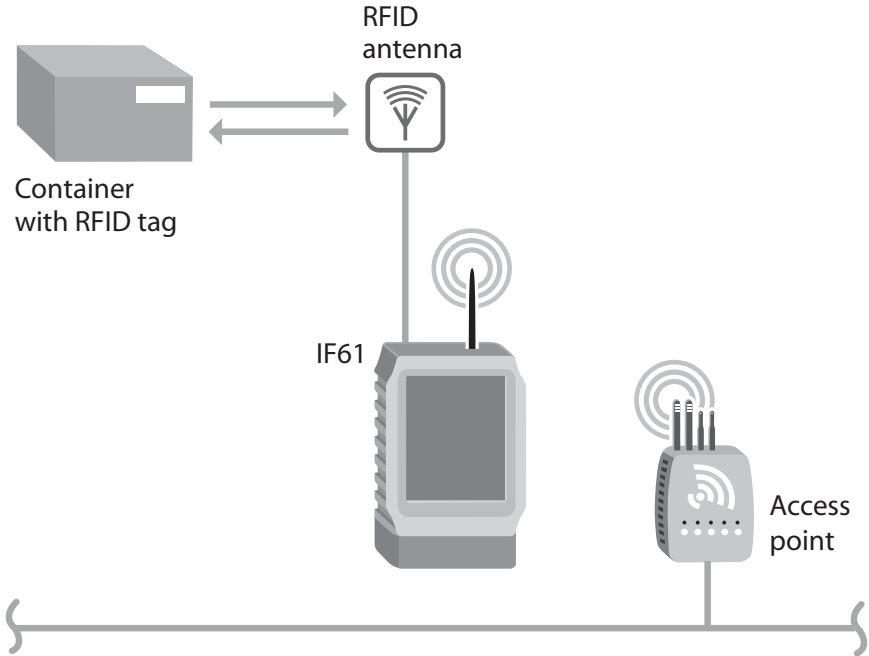
In general, the reader forwards RFID tag data to the Ethernet or wireless network as shown in the next illustrations.

IF61 in a Wired Ethernet Network



This illustration shows the IF61 in a wired Ethernet network. The IF61 sends tag data to the RFID application server through the wired network.

IF61 in a Wireless Network



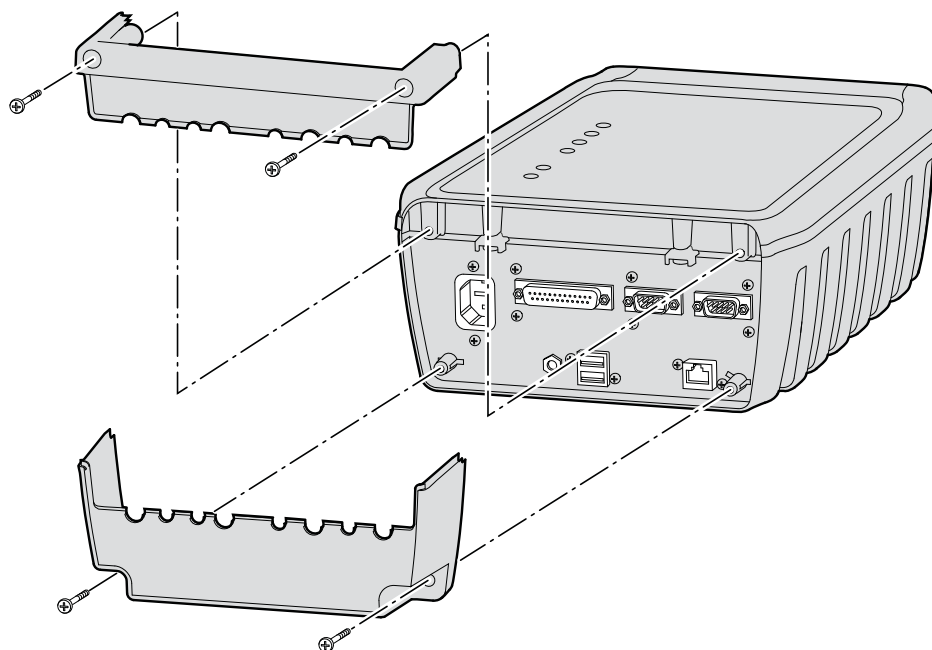
This illustration shows how the IF61 connects to your 802.11a/b/g network. The reader communicates with the access point as it sends tag data to the RFID application server.

Understanding the Network and Power Ports

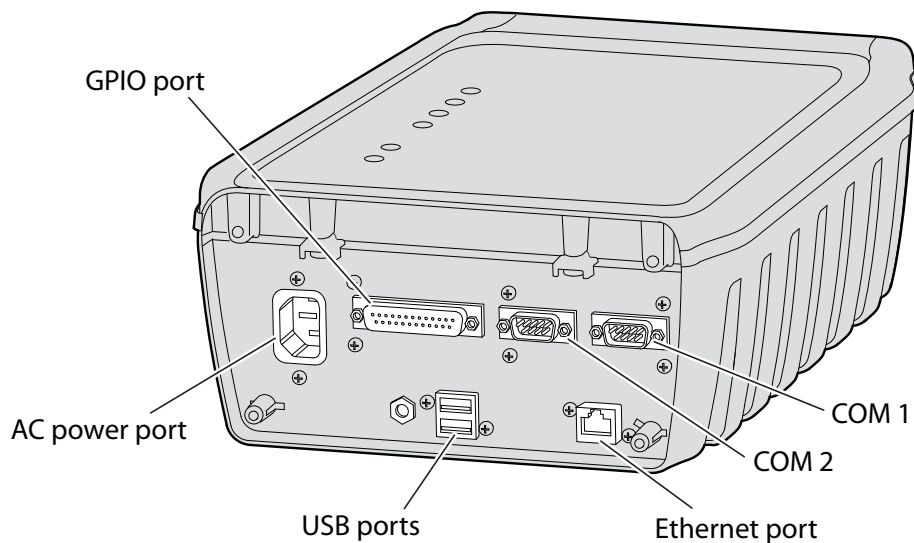
The IF61 network and power ports are located under the removable cable cover.

To remove the cable cover

- Unscrew the four screws on the cable cover to remove it.



Removing the IF61 Cable Cover



IF61 Network and Power Ports

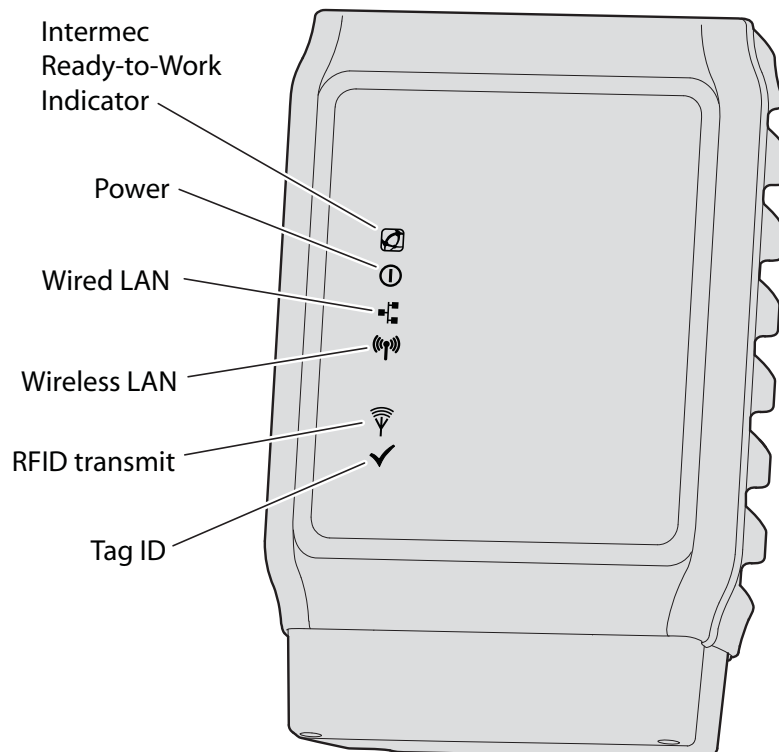
IF61 Port Descriptions

Port	Description
AC power	Connects the reader to an AC power source.
GPIO	General purpose input/output (GPIO) port that connects the IF61 to industrial controls such as relays or indicators. For more information on the IF61 GPIO interfaces, see “About the GPIO Interfaces” on page 114.
COM1	Connects the IF61 to a desktop PC for configuration. Use an RS-232 null modem cable (P/N 059167).
COM2	Pass-through serial port for developer-level access to a serial device.
Ethernet	10BaseT/100BaseTx port that connects the reader to your Ethernet network. The reader auto-negotiates with the server to set the best data rate. This port uses MDI/MDI-X auto-switching so you can connect either a standard Ethernet cable or a crossover cable.
USB	Connect USB devices to the IF61. For more information, see “Managing USB Devices” on page 101.





For more information, see [“Port Pin Assignments” on page 124.](#)

Understanding the LEDs



The IF61 has six LEDs that indicate the status of the reader during operation.



IF61 LED Descriptions

Icon	Name	Description
	Intermec Ready-to-Work™ Indicator	Blue LED remains on when an application is communicating with the IF61 BRI server. Blinks when no application is communicating with the IF61. For more information, see the next section.
	Power	Remains on when the IF61 has power.
	Wired LAN	Flashes when there is activity on the wired Ethernet network.
	Wireless LAN	Flashes when there is activity on the wireless 802.11 network.

IF61 LED Descriptions (continued)

Icon	Name	Description
	RFID Transmit	Flashes when the IF61 RFID reader is transmitting.
	Tag ID	Flashes when an RFID tag ID is successfully read or written to.

About the Intermec Ready-To-Work Indicator

The blue Ready-To-Work Indicator shows when an application is communicating with the Basic Reader Interface (BRI) server on the IF61. The next table explains the different states of the Ready-To-Work indicator.

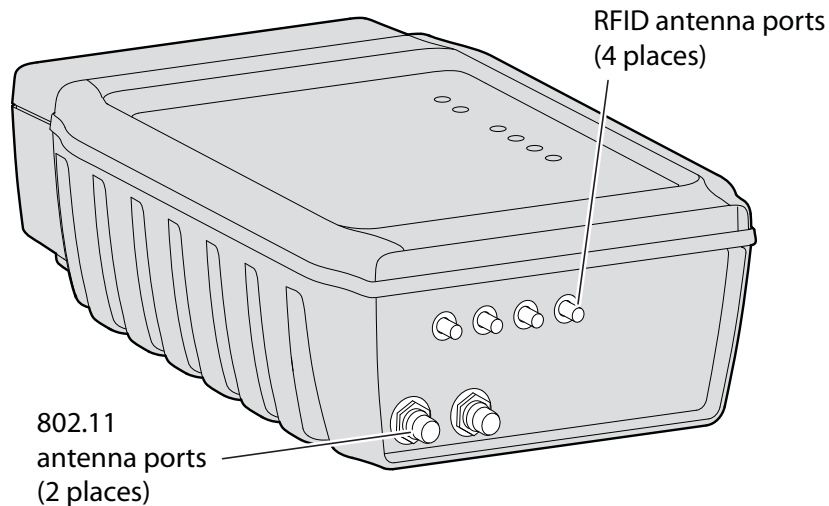
Ready-to-Work Indicator Status Descriptions

Status	Description
Off	IF61 does not have power.
Blinking	IF61 is initializing and not yet ready to use, or no application is currently communicating with the IF61 BRI server.
Steady	An application is communicating with the BRI server. For example, the Ready-to-Work indicator is steady blue when the IF61 developer tools are enabled (default), or when the installed SAP device controller or ALE engine is running. For more information, see “About the IF61 Edgeware Applications” on page 61.

For more information on the BRI server, see [“Configuring the BRI Server” on page 69.](#)

Understanding the Top Panel Ports

Connect RFID and 802.11 radio antennas to the ports on the IF61 top panel.



IF61 Top Panel Ports: This illustration shows the ports on the top panel. The IF61 ships with antenna terminators mounted on RFID antenna ports 2, 3, and 4.

The IF61 RFID antenna ports use these connectors:

- 865-869 MHz: SMA
- 915 MHz: Reverse SMA

Make sure you have appropriate antennas and cables for your IF61. For help, contact your Intermec sales representative.



Caution

Government regulatory agencies require that this RFID reader uses only approved antennas. Therefore, this reader uses a custom antenna connector. Do not use antennas not approved for use with this reader.



Note: The IF61 ships with antenna terminators installed on RFID antenna ports 2, 3, and 4. Do not remove the terminator from any port unless you are installing an antenna or antenna cable on that port.

Connecting to the IF61

By default, the IF61 is configured to be a DHCP client and accepts offers from any DHCP server. Therefore, the IF61 will work out of the box if you connect it to your network and use a DHCP server to assign it an IP address.

In this case, you configure the IF61 using the web browser interface from a desktop PC. For help, see [“Using the Web Browser Interface” on page 11](#).

However, if you are not using a DHCP server to assign an IP address, you use a communications program such as HyperTerminal to assign a static IP address. For help, see the next section, [“Assigning an Initial IP Address.”](#)

After the IF61 has been assigned an IP address, connect it to your network and then complete the configuration by using a web browser interface from a desktop PC. For help, see [“Using the Web Browser Interface” on page 11](#).

Assigning an Initial IP Address

Follow this procedure to assign an initial IP address to the IF61. After you assign the IP address, connect the IF61 to your network and use the web browser interface to complete the configuration.



Note: If configuration via a serial connection has been disabled on the IF61, you need to restore default settings before you use this procedure. For more information, see [“Using a Communications Program” on page 95](#).

To assign an initial IP address

- 1 Open a serial connection to the IF61. For help, see [“Opening a Serial Connection to the IF61” on page 96](#).

```

Loading System...
Intermec: IF61
Login with username/password of "config" to start initial configuration.
IF6101209060110 login:

```

Chapter 1 — Getting Started

- 2 Type `config` and press **Enter**, and then type `config` again in the **Password** field and press **Enter**. The IF61 Initial Configuration screen appears.

```
-----
Intermec IF61 Initial Configuration
-----
Ethernet Configuration Options
-----
D - Enable/Disable DHCP                (Currently Enabled)
R - Refresh DHCP Status                (No Address Established)
L - Advanced Ethernet Link Configuration
Q - Finished with Configuration

Selection: _
```

By default, DHCP is enabled. Because the IF61 is not yet connected to your network, it has not been assigned an IP address and “No Address Established” appears in the window.

- 3 Press **D**. DHCP is disabled and the Ethernet Configuration Options screen appears.

```
-----
Intermec IF61 Initial Configuration
-----
Ethernet Configuration Options
-----
D - Enable/Disable DHCP                (Currently Disabled)
1 - Change IP Address                  (Currently 0.0.0.0)
2 - Change Subnet Mask                 (Currently 255.255.255.0)
3 - Change IP Router                   (Currently 0.0.0.0)
L - Advanced Ethernet Link Configuration
Q - Finished with Configuration

Last Command Status: DHCP Status Changed

Selection: _
```

- 4 To set the IP address, press **1** and enter the static IP address in the entry field.
- 5 Press **Enter**. The static IP address is set. If you do not need to set the subnet mask or IP router values, you can now continue to configure the IF61 through the web browser interface. For help, see [“Using the Web Browser Interface” on page 11](#).

If you need to change the values for subnet mask or the IP router, continue with the next step.

- 6 To set the subnet mask, press **2** and enter the subnet mask value in the entry field. Press **Enter** to save the changes.

To set the IP router address, press **3** and enter the IP router address in the entry field. Press **Enter** to save the changes.

- 7 (Optional) To change the Ethernet link speed, press **L** and choose a link speed from the list of options:

Ethernet Link Speed Options

To choose this speed:	Press:
Auto detect (default)	A
100 Mbps - full duplex	1
100 Mbps - half-duplex	2
10 Mbps - full duplex	3
10 Mbps - half duplex	4
Keep the current selection and close this dialog box	Q

- 8 Press **Q** to close the Initial Configuration screen.
- 9 Disconnect the null-modem cable from the IF61.

The IF61 is now ready to be connected to your network. See [“Connecting the IF61 to Your Network” on page 16.](#)

Using the Web Browser Interface

After the IF61 is assigned an IP address, configure the IF61 using the web browser interface.

To use the web browser interface, the IF61 must be connected to your wired network. For help, see [“Connecting the IF61 to Your Network” on page 16.](#)

When using the web browser interface, remember that your session terminates if you do not use it for 15 minutes.

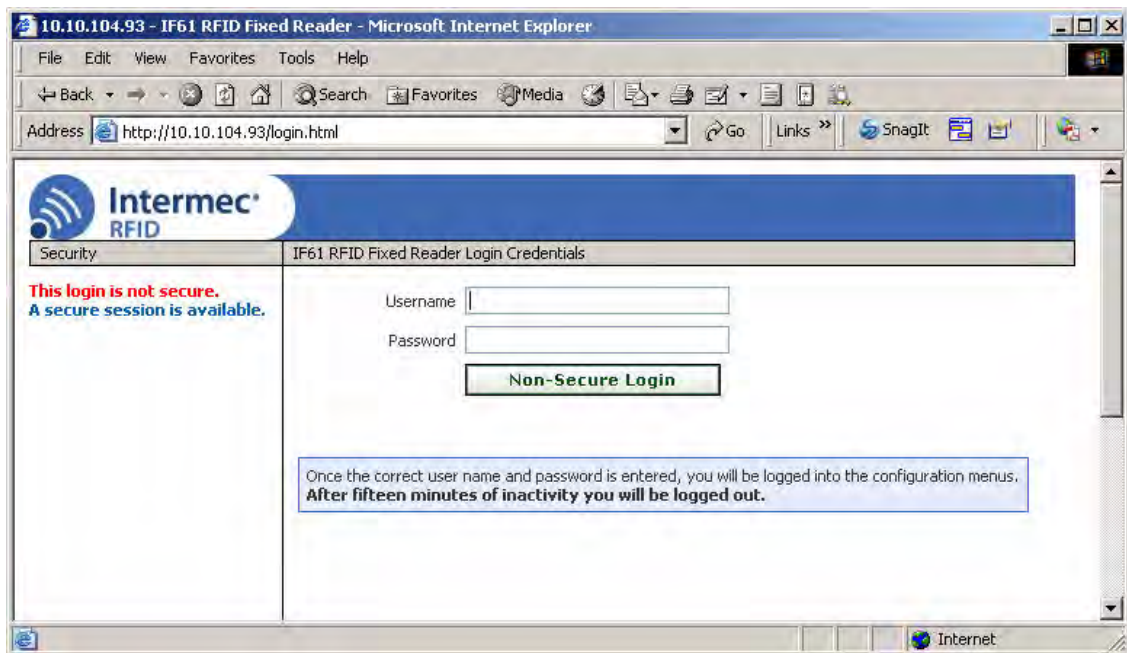


Note: If you access the Internet using a proxy server, add the IF61 IP address to your Exceptions list. The Exceptions list contains the addresses that you do not want to use with a proxy server.

Chapter 1 — Getting Started

To use the IF61 web browser interface

- 1 Determine the IP address of the IF61. If a DHCP server assigned the IP address, you need to get the IP address from that server.
- 2 Start the web browser.
- 3 In the browser address field, enter the IP address, and press **Enter**. The IF61 login screen appears.

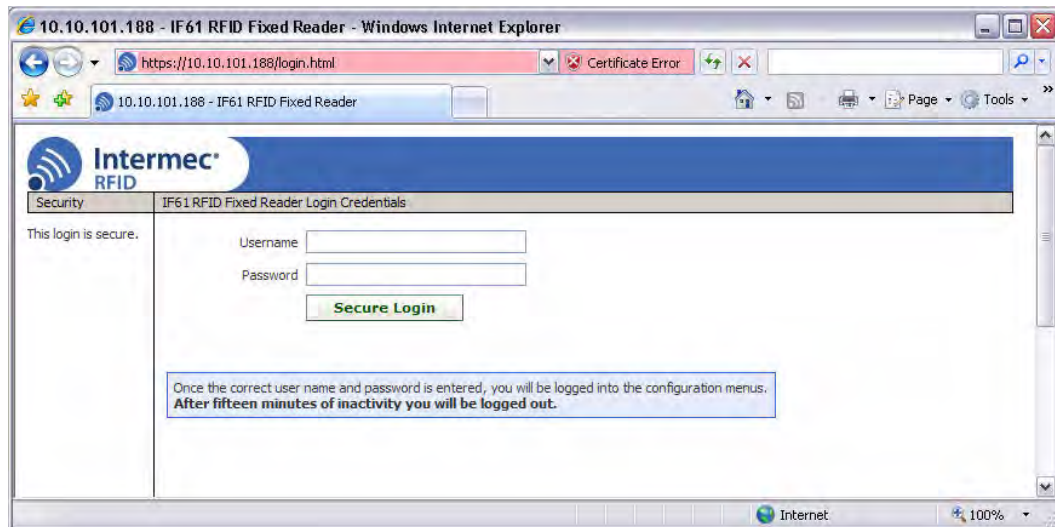


Or, for a secure session, click **A secure session is available**. The secure login screen appears.



Note: If a security alert message appears:

- Click **Yes** to continue to the secure login screen.
- Click **No** to cancel.
- Click **View certificate** to see the security certificate before continuing.



IF61 Secure Login Screen

- 4 If necessary, enter a user name and password. The default user name is `intermec` and the default password is `intermec`. You can define the user name and password. For help, see [“Setting Up Logins”](#) on page 33.
- 5 Click **Login** (or **Secure Login** in the secure login screen). The Ethernet screen appears and your web browser session is established.



Ethernet Screen: These settings appear when the IF61 is configured to use a DHCP server.

For help with configuring network settings, see [“Configuring Settings for Your Network”](#) on page 20.

Chapter 1 — Getting Started

For help with configuring RFID reader settings, see [“Configuring BRI Settings” on page 63.](#)

For more information on other methods for managing the IF61, see Chapter 4, [“Managing, Troubleshooting, and Upgrading the IF61.”](#)

Saving Configuration Changes

After you make configuration changes, click **Activate Changes** in the browser window to save your changes and immediately make the changes active.

Changes are discarded if you click another link in the browser window without clicking **Activate Changes** first.

Disabling Help in the Web Browser Interface

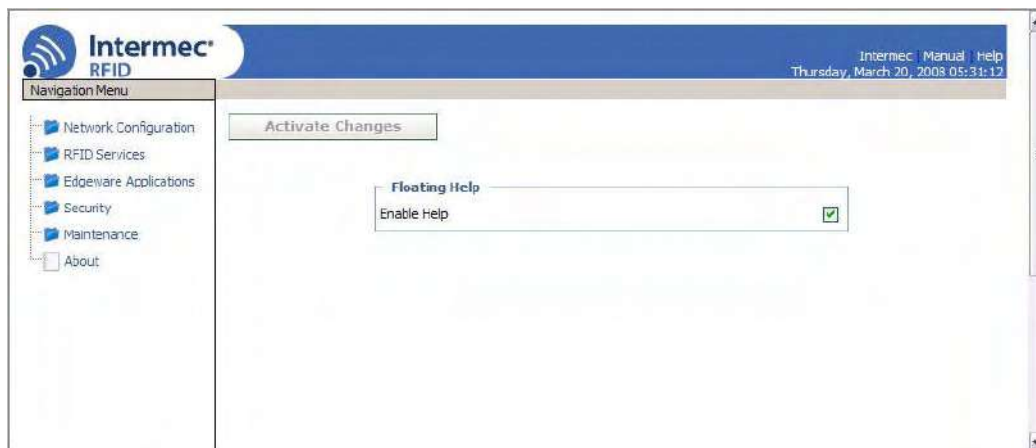
By default, the web browser interface shows help text as you move the cursor over items in each screen. Follow the next procedure to disable the help text feature.

To disable help text

- 1 In the web browser interface, click **Help** in the upper right-hand corner of the screen.



The Help screen appears.



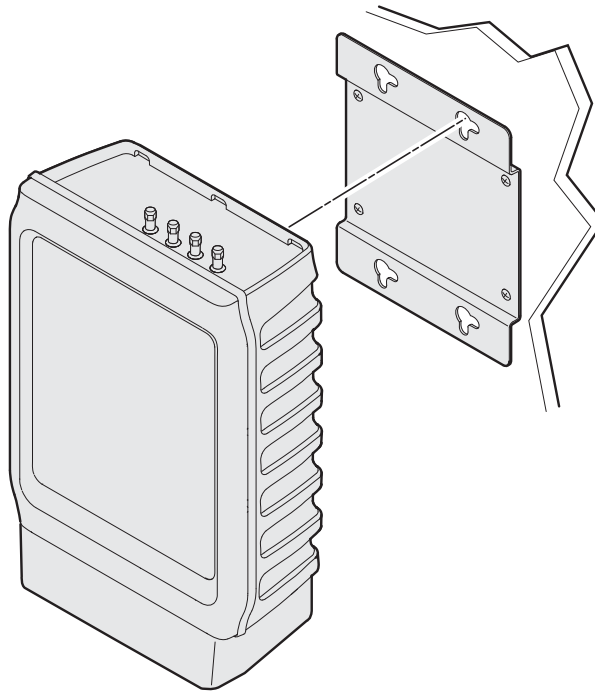
- 2 Uncheck the **Enable Help** check box.
- 3 Click **Activate Changes** to save your changes and immediately make them active. The Help text is disabled.

Installing the IF61

This section explains how to choose a mounting location for the IF61 and connect the IF61 to your network.

Choosing a Mounting Location

You can mount the IF61 to a wall or a beam using the mounting bracket kit (P/N 203-827-xxx). For more information, contact your local Intermec representative.



Mounting the IF61: This illustration shows the correct orientation for mounting the IF61 with the mounting bracket.



Note: The IF61 is certified to an IP54 environmental rating only when mounted as shown.

The next table includes environmental requirements for the IF61. Choose a location that meets these requirements.

IF61 Environmental Requirements

Type	Minimum	Maximum
Operating temperature	-20°C (-4°F)	55°C (131°F)
Storage temperature	-30°C (-22°F)	70°C (158°F)
Humidity (non-condensing)	10%	90%

Connecting the IF61 to Your Network

After you place the IF61 in its mounting location, you can connect it to your network.

To connect the IF61 to your network

- 1 Install the IF61 in its mounting location. For help, see [“Choosing a Mounting Location” on page 15.](#)
- 2 Remove the cable cover. For help, see [“Understanding the Network and Power Ports” on page 4.](#)
- 3 Attach one to four RFID antennas to the RFID antenna ports, starting with port 1. Do not remove the terminators from unused antenna ports. For help, see [“Understanding the Top Panel Ports” on page 8.](#)



Caution

Each port must have either an antenna or a terminator connected. Do not apply power to the reader unless an antenna or terminator is installed on each antenna port.

- 4 Connect an Ethernet cable to the IF61 Ethernet port.
- 5 (Optional) For a wireless network, connect the 802.11 antenna cable to port 1.
- 6 Connect the AC power cord to the power port on the IF61.



Note: The IF61 does not support power over Ethernet (POE).

- 7 Install the bottom half of the cable cover and route the cables through the openings.

- 8 Install the top half of the cable cover. Make sure the cables are not caught in the seam.
- 9 Place the IF61 in its mounting location. For help, see [“Choosing a Mounting Location” on page 15.](#)
- 10 Connect the Ethernet cable to your network.
- 11 Connect the AC power cord to an AC outlet. When you apply power, the IF61 boots and the green Power LED turns on.



Note: If you are using a DHCP server, make sure the server is running before you connect power to the IF61.

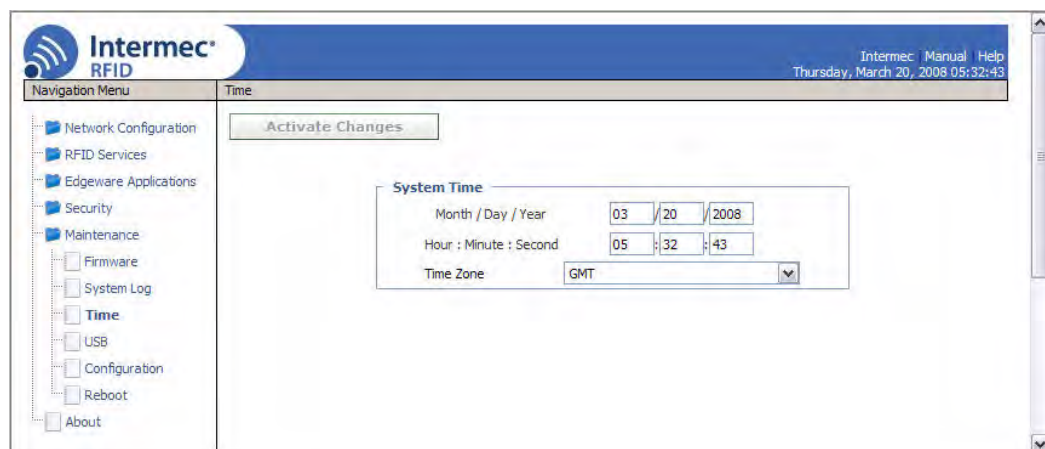
The IF61 is now ready to communicate with your network. Once the IF61 has been assigned an IP address (either manually or from your DHCP server), you can use the web browser interface to complete configuration. For help, see [“Using the Web Browser Interface” on page 11.](#)

Setting the Date and Time

After you have installed the IF61, you can set the date and time via the web browser interface.

To set the date and time

- 1 Connect to the IF61 via the web browser interface. For help, see [“Using the Web Browser Interface” on page 11.](#)
- 2 In the web browser screen, click the date and time in the upper right-hand corner. The Time screen appears.



- 3 Choose your time zone from the drop-down list and then click **Activate Changes**.
- 4 Enter the current month, day, and year in the entry fields.
- 5 Enter the current hour, minute, and second in the entry fields.
- 6 Click **Activate Changes**. The new time and date are set.



Note: If you have applications running on the IF61 when you change the date or time, stop and restart the applications (or reboot the IF61) for the date and time changes to take effect. For help, see “[Managing Applications](#)” on page 60.

Using the IF61 Securely

To help protect the integrity and security of your data, the IF61 supports a variety of secure access methods:

- You can use a secure web browser session (HTTPS) to access the IF61. For help, see “[Using the Web Browser Interface](#)” on page 11.
- To limit developer access to the IF61, you can enable or disable access services such as FTP, Telnet, or Common Internet File System (CIFS) shares. For help, see “[Controlling Access Services](#)” on page 30.
- You can configure and use network security methods, or disable basic configuration through the serial port. For help, see “[Configuring Security](#)” on page 30.



2 Configuring Network Settings

This chapter describes how to configure network settings for the IF61 and includes these topics:

- Configuring Settings For Your Network
- Configuring Security
- Configuring Wireless Security
- Managing Certificates

This chapter assumes that you are familiar with your network, networking terms, and the type of security implemented by your network.

Configuring Settings for Your Network

You use the web browser interface to configure network settings. For more information on using the web browser, see [“Using the Web Browser Interface” on page 11.](#)

This chapter explains how to use the web browser interface to configure settings for:

- wired Ethernet connections. For help, see the next section, “Configuring Ethernet Settings.”
- wireless 802.11 connections. For help, see [“Configuring the 802.11 Radio” on page 23.](#)
- parameters common to both the wired and wireless connections, such as DNS addresses and time servers. For help, see [“Configuring Common Network Settings” on page 27.](#)
- network security, such as passwords and access methods. For help, see [“Configuring Security” on page 30.](#)
- wireless security. For help, see [“Configuring Wireless Security” on page 37.](#)
- certificates. For help, see [“Managing Certificates” on page 49.](#)

From a device management standpoint, there are several other methods you can use to configure network settings, including Intermec SmartSystems, the Wavelink Avalanche client management system, and the Device Configuration web service. For more information on using these methods to configure the IF61, see Chapter 4, [“Managing, Troubleshooting, and Upgrading the IF61.”](#)

Configuring Ethernet Settings

This section explains how to configure wired Ethernet settings using the web browser interface.

If you are using a DHCP server, you may not need to configure Ethernet settings. For more information, contact your network administrator.



Note: The IF61 Ethernet connection must not be on the same subnet as the 802.11 wireless connection or errors may result.

To configure Ethernet settings

- 1 From the menu, click **Network Configuration** or **Ethernet** in the left-hand pane. The Ethernet screen appears.

If DHCP is enabled, you see this screen:

The screenshot shows the Intermecc RFID Ethernet configuration interface. The left navigation pane has 'Ethernet' selected. The main area contains an 'Activate Changes' button and two sections: 'IPv4' and 'IPv6'. In the 'IPv4' section, 'Enable DHCP' is checked, and the IP Address is 10.10.101.188, Subnet Mask is 255.255.0.0, Router (Default) is 10.10.0.1, and Link Local IP Address is 169.254.55.134. In the 'IPv6' section, 'IPv6 Autoconfigure' is checked and the IPv6 Address is fe80::2d0:c9ff:fea1:60df/64.

If DHCP is disabled, the current values for IP address, subnet mask, and router appear in entry fields:

The screenshot shows the Intermecc RFID Ethernet configuration interface with DHCP disabled. The left navigation pane has 'Ethernet' selected. The main area contains an 'Activate Changes' button and two sections: 'IPv4' and 'IPv6'. In the 'IPv4' section, 'Enable DHCP' is unchecked. The IP Address field contains 0.0.0.0, the IP Subnet field contains 255.255.255.0, and the IP Router (Gateway) field contains 0.0.0.0. The Link Local IP Address is 169.254.55.134. In the 'IPv6' section, 'IPv6 Autoconfigure' is checked and the IPv6 Address is fe80::2d0:c9ff:fea1:60df/64.

- 2 Configure the Ethernet settings. For help, see the next table.



Note: Different settings appear in this screen depending on the current DHCP mode for the IF61.

Chapter 2 — Configuring Network Settings

If you need to configure other network settings such as DNS addresses and suffixes or a SYSLOG destination, see “[Configuring Common Network Settings](#)” on page 27.

- 3 Click **Activate Changes** to save your changes and immediately make them active.

Ethernet Settings Descriptions

Parameter	Description
Enable DHCP	Check this check box if you want the IF61 to get its IP address from a DHCP server. If this check box is not checked, you need to specify the IP address, subnet mask, and IP router for your network.
IP Address	IP address of the IF61. The IP address has the form $x.x.x.x$, where x is a number from 0 to 255. If DHCP is enabled, the currently assigned IP address appears in this field. If DHCP is disabled, specify the IP address in the entry field.
Subnet Mask	Subnet mask for this network. The subnet mask has the form $x.x.x.x$, where x is a number from 0 to 255. If DHCP is enabled, the currently assigned subnet mask appears in this field. If DHCP is disabled, you may need to specify the subnet mask for the network.
Router	IP address of the router. The IP address has the form $x.x.x.x$, where x is a number from 0 to 255. If DHCP is enabled, the currently assigned router address appears in this field. If DHCP is disabled, you may need to specify the router address for the network.

Ethernet Settings Descriptions (continued)

Parameter	Description
Link Local IP Address	IP address of the IF61 if an address is not assigned (either manually or by a DHCP server). The IF61 auto-negotiates with other devices on its Ethernet segment to obtain a unique address.
IPv6 Autoconfigure	Enables IPv6 automatic configuration. Uncheck this check box to disable IPv6 auto-configuration on the IF61. Auto-configuration is enabled by default. If you disable auto-configuration, you need to specify an IPv6 address, subnet mask, and router.
IPv6 Address	128-bit IPv6 address for the IF61.
IPv6 Subnet Mask	1 to 128-bit IPv6 subnet mask.
IPv6 Router	128-bit address for the IPv6 router.

Configuring the 802.11 Radio

This section explains how to enable the 802.11 a/b/g radio and configure these settings:

- SSID (Network name)
- Advanced parameters, including network mode and fragmentation threshold
- IPv4 settings, including IP address, subnet mask, router, and DHCP status
- IPv6 autoconfiguration



Note: The IF61 802.11 wireless connection must not be on the same subnet as the Ethernet connection or errors may result.

To configure the radio

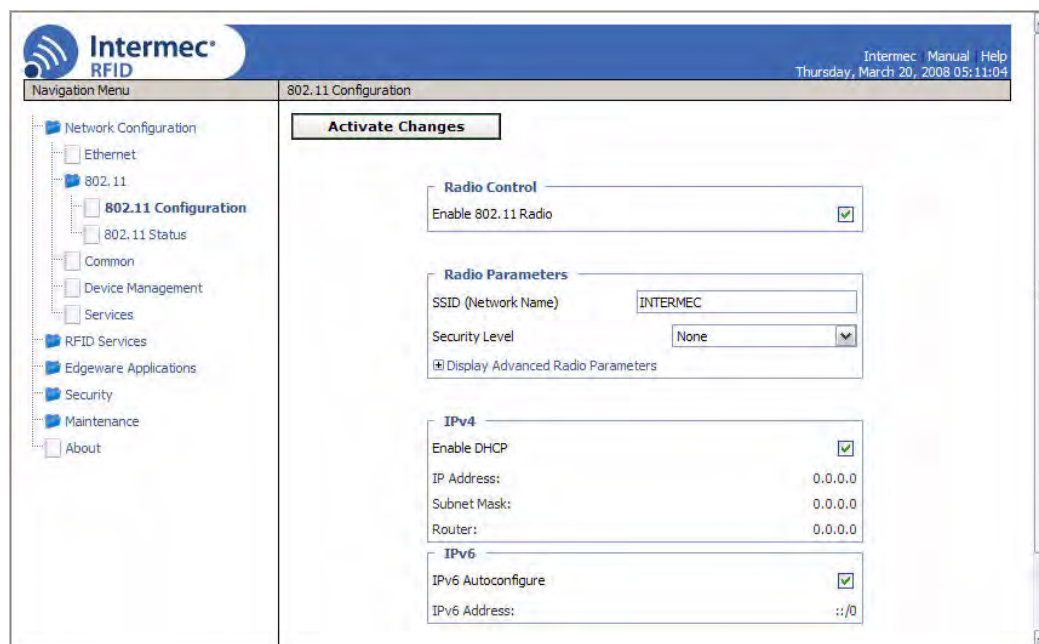
- 1 From the menu, click **802.11** or **802.11 Configuration** in the left-hand pane. The 802.11 Configuration screen appears.

Chapter 2 — Configuring Network Settings

If the radio is disabled, you see this screen:



If the radio is enabled, the Radio Parameters, IPv4, and IPv6 lists include the current settings:



2 Configure the radio settings. For help, see the next table.

- Click **Display Advanced Radio Parameters** to see the current settings for network mode and fragmentation threshold, or to enable medium reservation.

If you need to configure wireless security settings, see [“Configuring Wireless Security” on page 37](#).

- 3 Click **Activate Changes** to save your settings and immediately make them active.

802.11 Radio Settings Descriptions

Setting	Description
Enable 802.11 Radio	Check this check box to enable the 802.11 radio.
SSID (Network Name)	Name of the network. The IF61 will only connect to the specified network.
Security Level	Type of wireless security to enable on the IF61. For more information, see “Configuring Wireless Security” on page 37.
Network Mode	<p>Current 802.11 network type:</p> <ul style="list-style-type: none"> • Auto (default) - IF61 connects to 802.11a, 802.11 b/g, or 802.11g networks automatically. • 802.11b/802.11g - IF61 connects only to 802.11b or 802.11g networks. • 802.11g - IF61 connects only to 802.11g networks. • 802.11a - IF61 connects only to 802.11a networks. <p>Some restrictions may apply depending on your location. For more information, see “Setting the 802.11 Network Mode” on page 27.</p>
Fragmentation Threshold	Size of the largest data packet that can be transmitted without fragmentation. Default is 2346 bytes.
Enable Medium Reservation	Determines if you want to specify a reservation threshold. Check this check box to set a threshold value.

802.11 Radio Settings Descriptions (continued)

Setting	Description
Enable DHCP	<p>Check this check box if you want the IF61 to get its wireless IP address from a DHCP server. DHCP is enabled by default.</p> <p>If this check box is not checked, DHCP is disabled and you need to specify the IP address, subnet mask, and IP router for your network.</p>
IP Address	<p>IP address for the 802.11 radio. The IP address has the form <i>x.x.x.x</i>, where <i>x</i> is a number from 0 to 255.</p> <p>If DHCP is enabled, the currently assigned IP address appears in this field.</p> <p>If DHCP is disabled, set this value to a static IP address for the 802.11g radio.</p>
Subnet Mask	<p>Subnet mask that matches the other devices in your network. The subnet mask has the form <i>x.x.x.x</i>, where <i>x</i> is a number from 0 to 255.</p>
Router (Gateway)	<p>IP address of the router that will forward frames if the IF61 will communicate with devices on another subnet. The IP address has the form <i>x.x.x.x</i>, where <i>x</i> is a number from 0 to 255.</p>
IPv6 Autoconfigure	<p>Enables IPv6 automatic configuration for the radio. Uncheck this check box to disable IPv6 auto-configuration on the IF61.</p> <p>Auto-configuration is enabled by default. If you disable auto-configuration, you need to specify an IPv6 address, subnet mask, and router.</p>
IPv6 Address	<p>128-bit IPv6 address for the IF61.</p>
IPv6 Subnet Mask	<p>1 to 128-bit IPv6 subnet mask.</p>
IPv6 Router (Gateway)	<p>128-bit address for the IPv6 router.</p>

Setting the 802.11 Network Mode

When you set the Network Mode parameter, you should be aware of any restrictions on the use of specific frequency bands in your area.

To eliminate interference to Mobile Satellite Systems (MMS) communications, regulations in the United States, Canada, Australia, and New Zealand require only indoor use if you are operating the IF61 in the 5150-5250 MHz range.

Australia and New Zealand also require only indoor use if you are operating the IF61 in the 5250-5350 MHz range.

All European countries require only indoor use if you are operating the IF61 in the 5150-5350 MHz range.

To comply with regulations in these locations, set Network Mode to **Auto** or **802.11a** only if the IF61 is being used indoors.

Configuring Common Network Settings

Common network settings are configuration items that apply to all network connections.

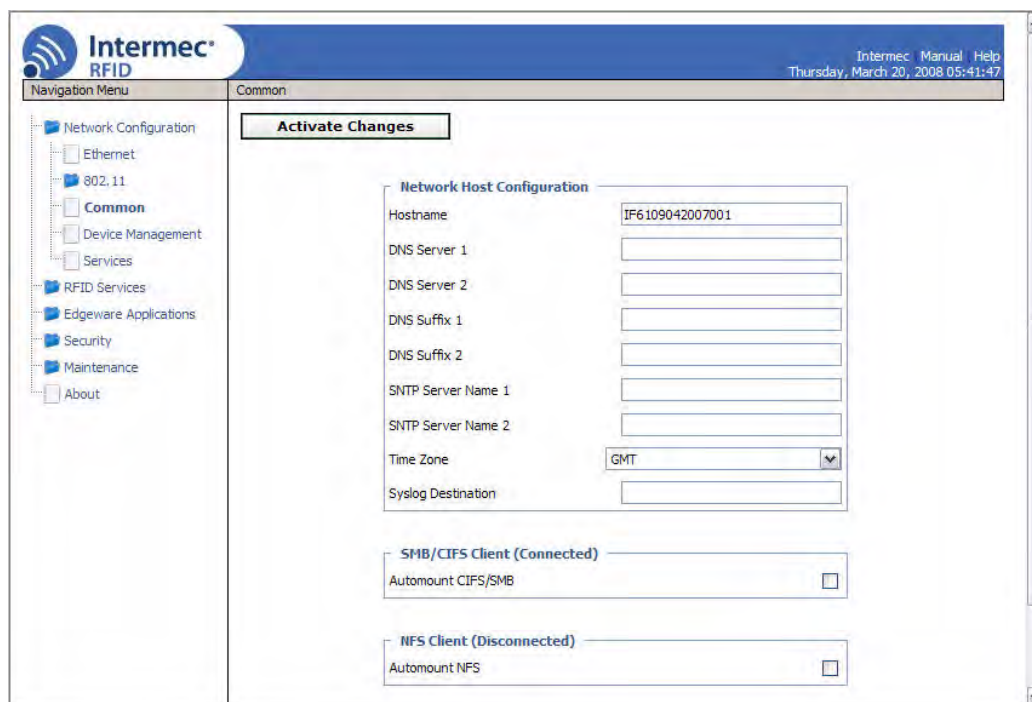
This section explains how to use the web browser interface to configure these common network settings:

- Hostname
- Domain Name Server (DNS) addresses and suffixes
- Simple Network Time Protocol (SNTP) server addresses 1 and 2. For information on public NTP servers, see <http://ntp.isc.org>.
- Local time zone
- SYSLOG destination
- Mounting Common Internet File System (CIFS) and NFS shares on the IF61

To configure common network settings

- 1 In the menu, click **Network Configuration > Common**. The Common screen appears.

Chapter 2 — Configuring Network Settings



- 2 Configure settings. For help, see the next table.
- 3 Click **Activate Changes** to save your changes and immediately make them active.

Common Network Settings Descriptions

Parameter	Description
Hostname	Name for this IF61. The default is “IF61<serial number of the IF61>”. The hostname can be either a simple hostname, or a qualified domain name (FQDN). If this IF61 obtains its IP address via DHCP, this parameter is sent to the DHCP server. If the server supports it, this field is used for dynamic DNS updates.
DNS Server 1	IP address of a domain name server that the IF61 uses to resolve DNS names.
DNS Server 2	IP address of a second domain name server that the IF61 uses to resolve DNS names.
DNS Suffix 1	Primary DNS suffix to be appended to unqualified names.

Common Network Settings Descriptions (continued)

Parameter	Description
DNS Suffix 2	Secondary DNS suffix to be appended to unqualified names.
SNTP Server Name 1	DNS name or IP address of an SNTP or NTP server.
SNTP Server Name 2	DNS name or IP address of a second SNTP or NTP server.
Time Zone	Time zone for this IF61. Choose the time zone from the drop-down list. Default is GMT. For more information, see “Setting the Date and Time” on page 17.
SYSLOG Destination	Domain name or IP address of the SYSLOG server. In Unix networks, system messages are logged to this server.
Automount CIFS/SMB	Check this check box to enable mounting a Common Internet File System/Server Message Block share on the IF61. If you enable automounting a CIFS share, you need to specify: <ul style="list-style-type: none"> • the remote host IP address or name. • the remote share name. • the username, password, and domain of the remote share.
Automount NFS	Check this check box to enable mounting a Network File System volume on the IF61. If you enable mounting an NFS volume on the IF61, you need to specify: <ul style="list-style-type: none"> • the remote host IP address or name. • the remote path to the exported volume.

Configuring Security



Note: Before you configure security settings for this IF61, you should be familiar with the type of security implemented for your network.

The IF61 supports a variety of security features to help maintain the integrity of your secure network. You can:

- change default network parameters. For help, see [“Configuring the 802.11 Radio” on page 23.](#)
- enable/disable access services. For example, if you are not using Telnet sessions to configure or manage the IF61, you can disable Telnet access. For help, see the next section, “Controlling Access Services.”
- change the default user name and password. For help, see [“Setting Up Logins” on page 33.](#)
- use a password server to maintain a list of authorized users who can configure and manage the IF61. For help, see [“Setting Up Logins” on page 33.](#)
- disable serial port access to the IF61. For help, see [“Disabling Access Via the Serial Port” on page 36.](#)
- configure a variety of wireless security protocols. For help, see [“Configuring Wireless Security” on page 37.](#)

For general information on securely using the IF61, see [“Using the IF61 Securely” on page 18.](#)

Controlling Access Services

Access services are the different ways that users (such as developers) can access and configure the IF61.

You can control how developers access the IF61 by enabling or disabling these services:

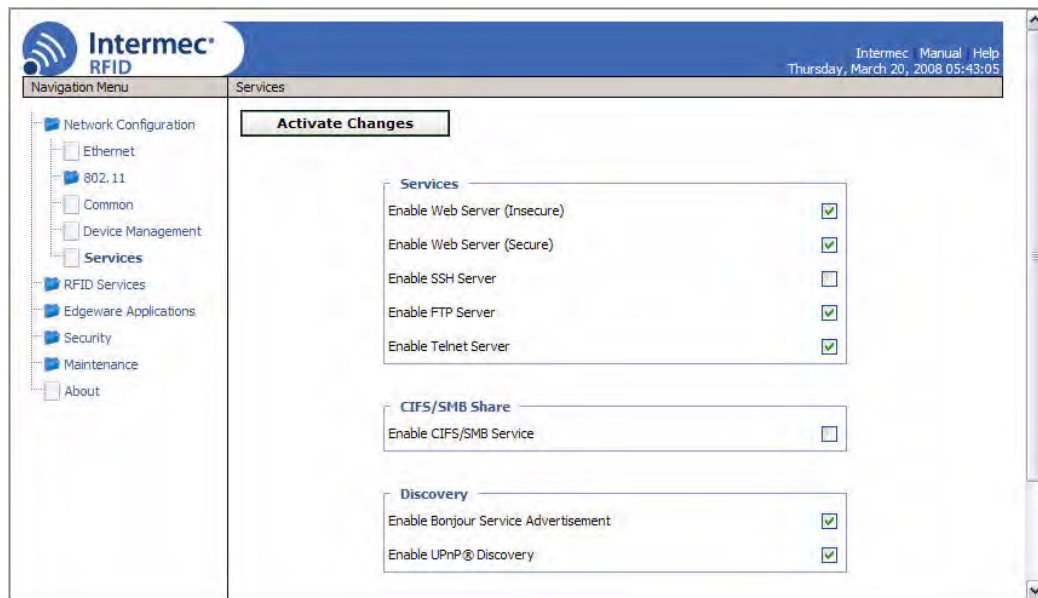
- Web browser interface (secure and non-secure)
- Secure shell access to the Linux console
- FTP access to the IF61 FTP directory
- Telnet access to the Linux console

- Mounting an IF61 Common Internet File System (CIFS) directory
- Discovering the IF61 via Bonjour or Universal Plug and Play™ (UPnP) service advertisement (enabled by default)

To enable or disable these methods, see the next procedure.

To enable developer access methods

- 1 From the menu, click **Network Configuration > Services**. The Services screen appears.



- 2 Enable or disable developer access methods by checking or unchecking the check boxes, or by choosing options from the drop-down list. For help, see the next table.
- 3 Click **Activate Changes** to save your changes and immediately make them active.

Developer Access Method Descriptions

Method	Description
Enable Web Server	<p>Enables access to the IF61 via the web browser interface.</p> <p>Choose Secure Only to allow only the secure web interface through port 443.</p> <p>Choose Secure/Insecure to allow users to log in using either a nonsecure (HTTP via port 80) or secure (HTTPS via port 443) web interface.</p> <p>Choose Disabled to disable web browser access. If you disable browser access to the IF61, you may need to access the IF61 via a communications program.</p>
Enable SSH Server	<p>Enables Secure Shell (SSH) access to the Linux system console using the same login and password as the web browser interface (default is <code>intermec</code>). SSH access is disabled by default.</p>
Enable FTP Server	<p>Enables access to the IF61 via its FTP server. For more information, see “Using the IF61 FTP Server” on page 91. FTP is disabled by default.</p>
Enable Telnet Server	<p>Enables access to the Linux system console via standard Telnet, using the same login and password as the web browser interface. The default login and password is <code>intermec</code>. The Telnet server is disabled by default.</p>
Enable CIFS/SMB Service	<p>Enables the Common Internet File System service, which creates a file sharing connection from a Windows PC to the <code>/home/developer</code> directory on the IF61. CIFS/SMB is disabled by default.</p> <p>When you enable the CIFS/SMB service, entry fields for a username and password appear. Enter these settings and then click Activate Changes.</p>
Enable Bonjour Service Advertisement	<p>Enables the IF61 to advertise services and be discovered by Bonjour zero-configuration networking. Bonjour is enabled by default.</p> <p>To prevent errors when using Bonjour, make sure the IF61 hostname does not include spaces. To set the hostname, see “Configuring Common Network Settings” on page 27.</p>
Enable UPnP Discovery	<p>Enables the IF61 to be discovered by Universal Plug and Play protocols. UPnP is enabled by default.</p>

Setting Up Logins

To ensure login security for configuring or maintaining the IF61, you should use a password server or at least change the default user name and password.

- A password server is typically an embedded authentication server (EAS) or other RADIUS server. To use a password server, you must have a password server on the network that contains the user name/password database. On the IF61, you need to enable RADIUS for login authorization.

When you attempt to log in to the IF61, you must enter a user name and password. This login is sent to the RADIUS server, which compares the login to its list of authorized logins. If a match is found, you can log in to the IF61 with read/write privileges.

For help, see the next section, “Configuring the IF61 to Use a Password Server.”

- If you do not want to use a password server, you should change the default login user name and password, and create a read-only password. For help, see [“Changing the Default Login” on page 35](#).

Configuring the IF61 to Use a Password Server

If you use a password server to manage users who log in to this IF61, you need to tell the IF61 how to communicate with the password server and then you need to configure the password server.



Note: If errors occur and you cannot log in to the IF61, restore defaults via a serial connection to reset all passwords to default values. For help, see [“Restoring the IF61 to the Default Configuration” on page 100](#).

To configure the IF61 to use a password server

- 1 From the menu, click **Security** > **Passwords**. The Passwords screen appears.

Chapter 2 — Configuring Network Settings

The screenshot shows the Intermec RFID configuration interface. The top navigation bar includes the Intermec RFID logo, the text 'Intermec Manual Help', and the date 'Thursday, March 20, 2008 05:47:17'. The left sidebar contains a 'Navigation Menu' with the following items: Network Configuration, RFID Services, Edgware Applications, Security (expanded), Passwords (selected), Import Certificate, Certificate Details, Maintenance, and About. The main content area is titled 'Passwords' and features an 'Activate Changes' button at the top. Below this, there are three sections: 'User Credentials' with fields for Username (intermec), Password (masked with dots), and Read-only Password (masked with dots); 'RADIUS' with an unchecked 'Enable RADIUS' checkbox; and 'Serial Configuration' with a checked 'Enable Serial Configuration' checkbox.

- 2 Check the **Enable RADIUS** check box. A list of RADIUS configuration items appears.

The screenshot shows the Intermec RFID configuration interface after the 'Enable RADIUS' checkbox has been checked. The 'Activate Changes' button remains at the top. The 'RADIUS' section now displays configuration fields for two servers. The first server has 'Enable RADIUS' checked, 'Primary Radius Server' set to '0.0.0.0', 'Secret' masked with dots, and 'Port' set to '1812'. The second server has 'Secondary Radius Server' set to '0.0.0.0', 'Secret' masked with dots, and 'Port' set to '1812'. The 'Serial Configuration' section remains unchanged with 'Enable Serial Configuration' checked.

- 3 Configure the settings. For help, see the next table.
- 4 Click **Activate Changes**.
- 5 Configure the password server database. For help, see the documentation that came with your server.

RADIUS Server Information Descriptions

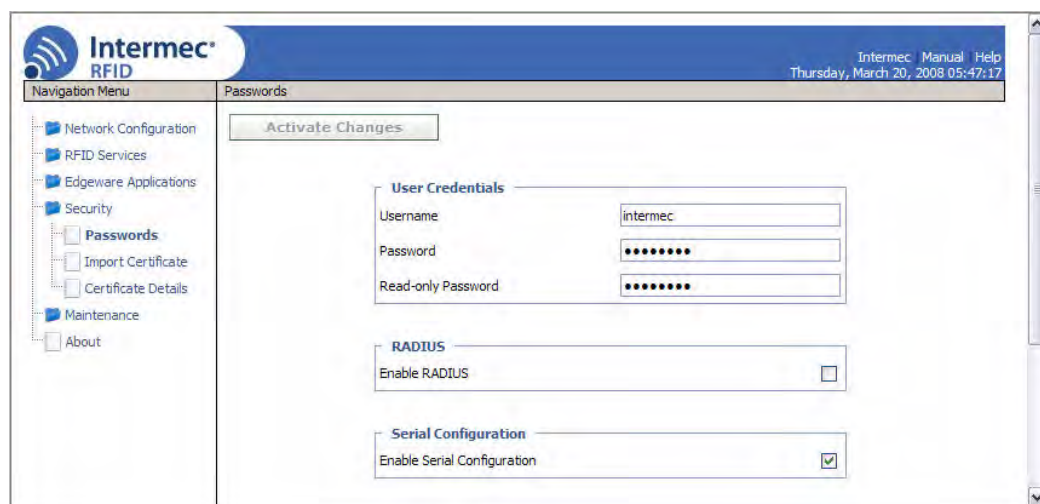
Type	Description
Enable RADIUS	Enables RADIUS authentication for this IF61.
Primary Radius Server	IP address or DNS name of the RADIUS server. If this field is blank, the RADIUS client does not use this entry.
Secret	Secret key for this RADIUS server.
Port	Port number of the primary RADIUS server. Default is 1812.
Secondary Radius Server	IP address or DNS name of the RADIUS server to use if there is no response from the primary RADIUS server.
Secret	Secret key for this RADIUS server.
Port	Port number of the secondary RADIUS server. Default is 1812.

Changing the Default Login

If you are not using a password server to authorize user logins, Intermec recommends that you change the default user name and password and create a read-only password.

To set up logins

- 1 From the main menu, click **Security > Passwords**. The Passwords screen appears.



Chapter 2 — Configuring Network Settings

- 2 Make sure the **Enable RADIUS** check box is not checked. Uncheck this check box if necessary and then click **Activate Changes**.
- 3 Configure the parameters. For help, see the next table.
- 4 Click **Activate Changes** to save your changes and immediately make them active.

Password Parameter Descriptions

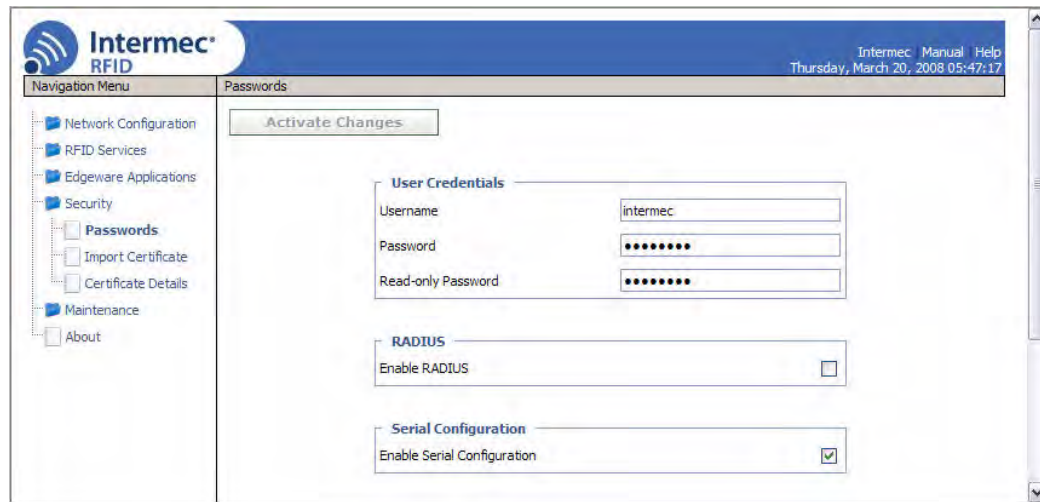
Parameter	Description
Username	Enter the user name you need to use to log in to this IF61. The user name can be from 1 to 32 characters long. You must always specify a user name. Default is <code>intermec</code> .
Password	Enter the password you need to use to log in to this IF61. This password gives you read and write access to the IF61 configuration. The password can be from 8 to 32 characters long. You must always specify a password. Default is <code>intermec</code> .
Read-only Password	Enter the password you need to use to log in to this IF61. This password gives the user read-only access to the IF61. This user can view the configuration and execute diagnostics but cannot perform any tasks that affect IF61 operation, such as changing configuration options or downloading software. Default is <code>readonly</code> . The read-only password cannot be deleted. To disallow read-only access, you need to enable RADIUS authentication. For help, see “Configuring Security” on page 30 .

Disabling Access Via the Serial Port

When serial port access is disabled, you will not be able to configure the IF61 as described in [“Assigning an Initial IP Address” on page 9](#). You must use the web browser interface for all configuration.

To disable serial port access

- 1 From the menu, click **Security > Passwords**. The Passwords screen appears.



- 2 Uncheck the **Enable Serial Configuration** check box.
- 3 Click **Activate Changes** to save your changes and immediately make them active.

Configuring Wireless Security



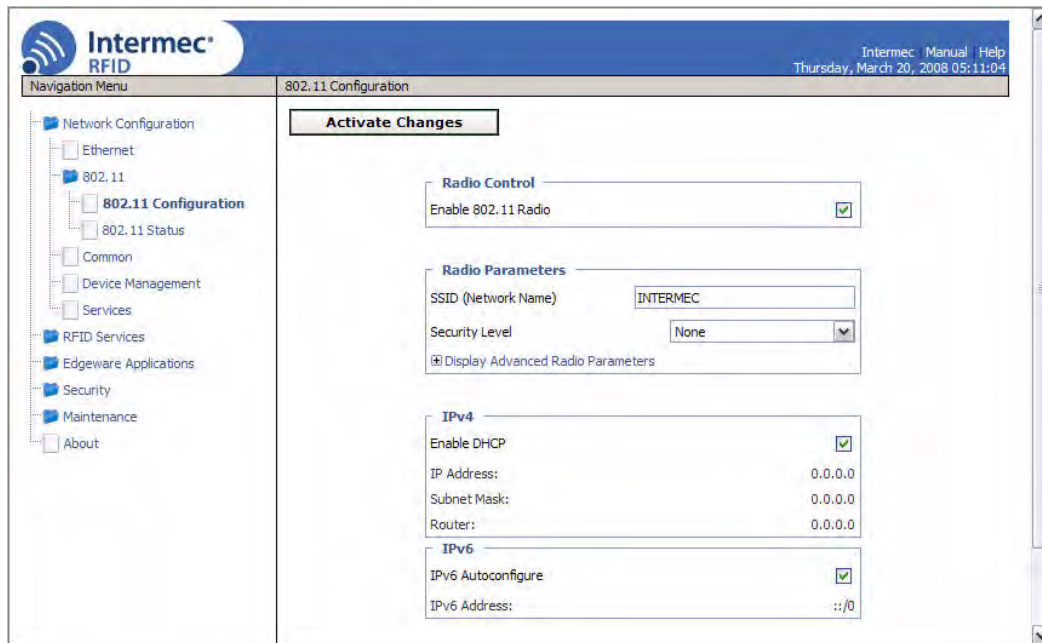
Note: To configure wireless security, the 802.11 radio must be enabled. For help, see [“Configuring the 802.11 Radio” on page 23](#). This section assumes you have already enabled the radio.

The IF61 supports a variety of wireless network security protocols. You can configure:

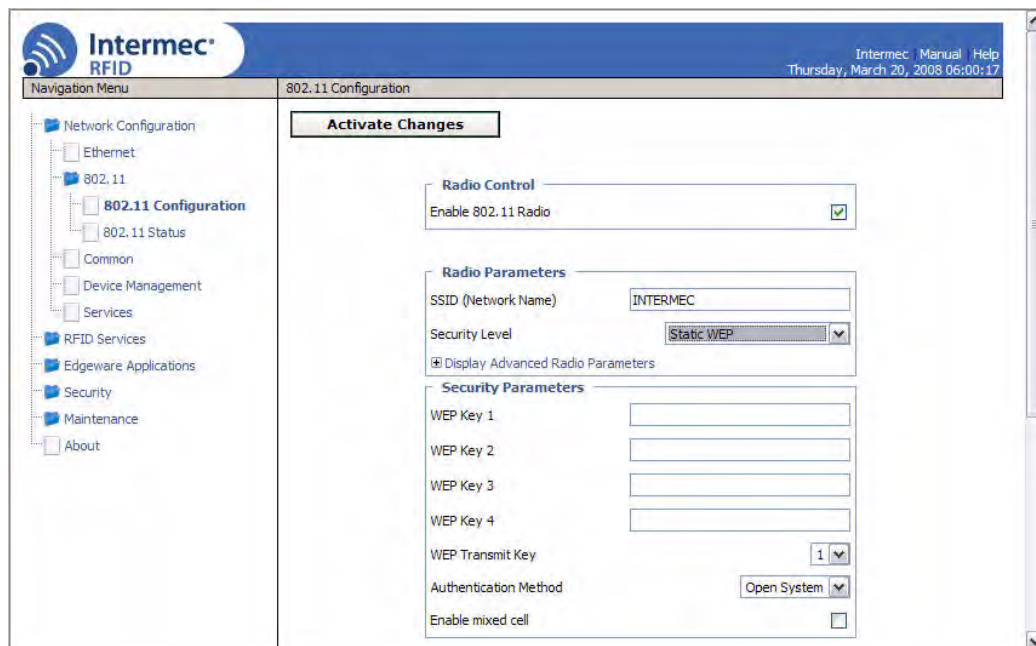
- WPA2 Enterprise (802.1x) security. For help, see [“Configuring WPA2 Enterprise \(802.1x\) Security” on page 47](#).
- WPA2 Personal (PSK) security. For help, see [“Configuring WPA2 Personal \(PSK\) Security” on page 45](#).
- WPA Enterprise (802.1x) security. For help, see [“Configuring WPA Enterprise \(802.1x\) Security” on page 43](#).
- WPA Personal (PSK) security. For help, see [“Configuring WPA Personal \(PSK\) Security” on page 41](#).
- Dynamic WEP/802.1x security. For help, see [“Configuring Dynamic WEP/802.1x Security” on page 39](#).
- basic WEP security. For help, see the next section.

Configuring WEP Security

- 1 From the menu, click **Network Configuration > 802.11** or **802.11 Configuration**. The 802.11 Configuration screen appears.



- 2 Choose **Static WEP** from the **Security Level** drop-down list. The Security Parameters list appears.



Chapter 2 — Configuring Network Settings

- 3 Configure the parameters for WEP security. To ensure maximum security, configure each WEP key with a different WEP code. For help, see the next table.
- 4 Click **Activate Changes** to save your changes and immediately make them active.

Parameters for Static WEP Security

Parameter	Description
WEP Key 1 through WEP Key 4	For WEP 64, enter five ASCII characters or hex pairs. For WEP 128, enter 13 ASCII characters or hex pairs. For example, an ASCII WEP key of ABCDE would be entered in hex format as 4142434445.
WEP Transmit Key	Chooses the WEP key this IF61 uses to encrypt transmitted data. Default is 1.
Authentication Method	Specifies whether encryption will be used as part of the authentication algorithm to authenticate the IF61. Choose Shared Key to require encryption or Open System to require no encryption.
Enable mixed cell	Enable this mode to allow the IF61 to communicate with CCX mixed-cell access points.

Configuring Dynamic WEP/802.1x Security

- 1 From the menu, click **Network Configuration > 802.11** or **802.11 Configuration**. The 802.11 Configuration screen appears.

Chapter 2 — Configuring Network Settings

The screenshot shows the Intermecc RFID web interface. The top navigation bar includes the Intermecc logo and the text 'Intermecc Manual Help Thursday, March 20, 2008 05:11:04'. The left sidebar contains a 'Navigation Menu' with categories like Network Configuration, RFID Services, and Security. The main content area is titled '802.11 Configuration' and features an 'Activate Changes' button. Below this, there are four sections: 'Radio Control' with 'Enable 802.11 Radio' checked; 'Radio Parameters' with 'SSID (Network Name)' set to 'INTERMECC' and 'Security Level' set to 'None'; 'IPv4' with 'Enable DHCP' checked and IP Address, Subnet Mask, and Router all set to '0.0.0.0'; and 'IPv6' with 'IPv6 Autoconfigure' checked and 'IPv6 Address' set to ':::0'.

- 3 Choose **Dynamic WEP/802.1x** from the **Security Level** drop-down list. The Security Parameters list appears.

This screenshot shows the same Intermecc RFID web interface, but with the 'Security Level' dropdown menu set to 'Dynamic WEP/802.1x'. This change has triggered the appearance of a 'Security Parameters' section. The 'Security Level' dropdown is now expanded to show 'Dynamic WEP/802.1x'. The 'Security Parameters' section includes: 'Allowed EAP Authentication Method' set to 'PEAP'; 'Username' and 'Password' input fields; 'Validate CA Certificate' and 'Enable mixed cell' checkboxes, both of which are currently unchecked. The 'Radio Control' and 'IPv4' sections remain visible at the top and bottom of the configuration area.

- 3 Configure the parameters for Dynamic WEP security. For help, see the next table.

- 4 Click **Activate Changes** to save your settings and immediately make them active.

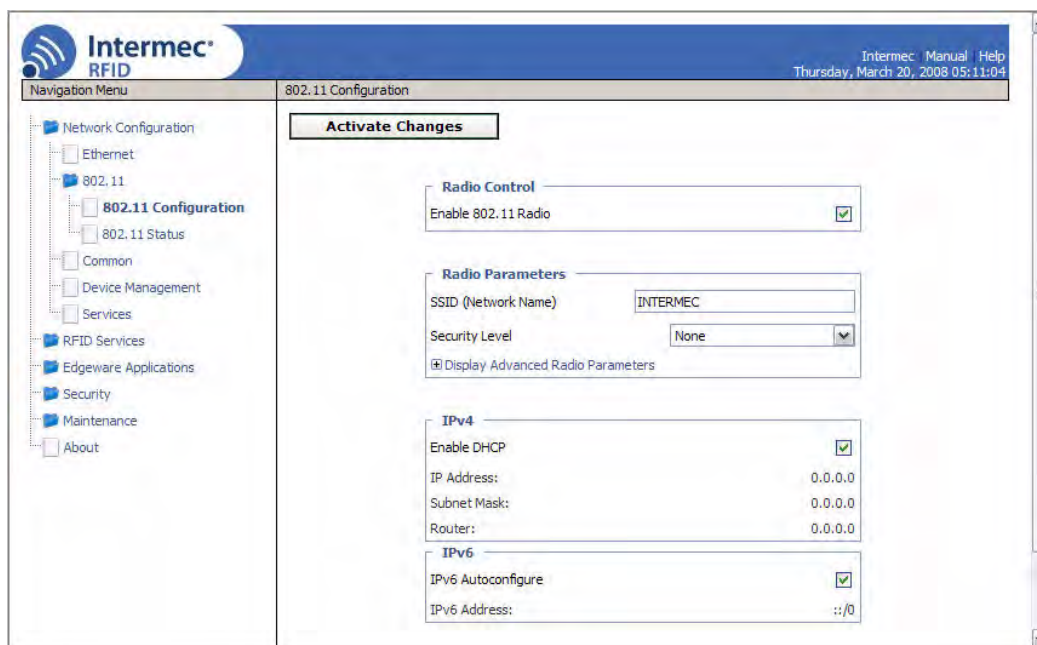
Parameters for Dynamic WEP/802.1x Security

Parameter	Description
Allowed EAP Authentication Method	Specifies which 802.1x authentication protocol (TLS, TTLS, PEAP, or LEAP) the IF61 sends to the authentication server.
Username	User name for the selected protocol.
Password	Password for the selected protocol.
Validate CA Certificate	Enables or disables verification of the server certificate signature against the certificate installed on the IF61. If you enable verification, you need to specify the CA certificate common name.
CA Certificate Common Name	Common name for the server certificate.
Reject Expired Certificates	Check this check box to reject expired certificates.
Enable mixed cell	Enable this mode to allow the IF61 to communicate with CCX mixed-cell access points. Mixed-cell use allows both WEP and non-WEP clients to communicate with the same access point.

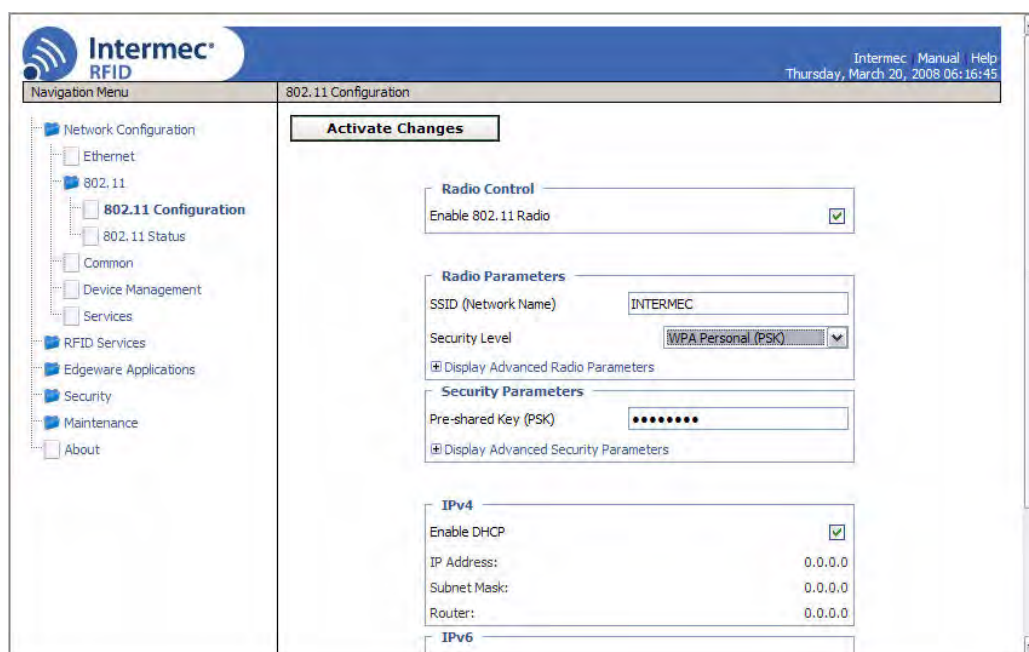
Configuring WPA Personal (PSK) Security

- 1 From the menu, click **Network Configuration > 802.11** or **802.11 Configuration**. The 802.11 Configuration screen appears.

Chapter 2 — Configuring Network Settings



- 2 Choose **WPA Personal (PSK)** from the **Security Level** drop-down list. The Security Parameters list appears.



- 3 Configure the parameters for WPA Personal security. For help, see the next table.
 - Click **Display Advanced Security Parameters** to see the current settings for multicast and pairwise encryption.

- 4 Click **Activate Changes** to save your settings and immediately make them active.

Parameters for WPA Personal Security

Parameter	Description
Pre-Shared Key (PSK)	The pre-shared key for WPA. You can enter an ASCII passphrase (range is 8 to 64 characters), and the key is derived from the passphrase using the PBKDF2 algorithm.
Minimum Multicast Encryption	Choose a data encryption method for non-unicast transmission/reception: CCMP (RSN): Use Counter Mode - CBC MAC Protocol. TKIP (RSN): (Default) Choose Temporal Key Integrity Protocol. WEP (TSN): Choose WEP keying.
Pairwise Encryption (Unicast)	Choose a data encryption method for unicast transmission/reception: TKIP: (Default) Use Temporal Key Integrity Protocol. CCMP: Use Counter Mode - CBC MAC Protocol.

Configuring WPA Enterprise (802.1x) Security

- 1 From the menu, click **Network Configuration > 802.11** or **802.11 Configuration**. The 802.11 Configuration screen appears.

Chapter 2 — Configuring Network Settings

The screenshot shows the Intermecc RFID web interface for 802.11 Configuration. The left navigation menu includes Network Configuration, Ethernet, 802.11, 802.11 Configuration, 802.11 Status, Common, Device Management, Services, RFID Services, Edgware Applications, Security, Maintenance, and About. The main content area is titled '802.11 Configuration' and features an 'Activate Changes' button. Below this, there are three sections: 'Radio Control' with 'Enable 802.11 Radio' checked; 'Radio Parameters' with SSID (Network Name) set to 'INTERMEC', Security Level set to 'None', and 'Display Advanced Radio Parameters' checked; and 'IPv4' with 'Enable DHCP' checked and IP Address, Subnet Mask, and Router all set to '0.0.0.0'. An 'IPv6' section is also visible with 'IPv6 Autoconfigure' checked and 'IPv6 Address' set to ':::0'.

- 3 Choose **WPA Enterprise (802.1x)** from the **Security Level** drop-down list. The Security Parameters list appears:

The screenshot shows the Intermecc RFID web interface for 802.11 Configuration, similar to the previous one but with the Security Level set to 'WPA Enterprise (802.1x)'. The 'Security Parameters' section is now expanded, showing 'Allowed EAP Authentication Method' set to 'PEAP', 'Username' and 'Password' fields, and 'Validate CA Certificate' unchecked. The 'Display Advanced Security Parameters' checkbox is checked. The 'IPv4' section remains visible with 'Enable DHCP' checked.

- 3 Configure WPA Enterprise security settings. For help, see the next table.
 - Click **Display Advanced Security Parameters** to see the current settings for multicast and pairwise encryption.

- 4 Click **Activate Changes** to save your settings and immediately make them active.

Parameters for WPA Enterprise Security

Parameter	Description
Allowed EAP Authentication Method	Specifies which 802.1x authentication protocol (TLS, TTLS, PEAP, or LEAP) the IF61 sends to the authentication server.
Username	User name for selected protocol.
Password	Password for selected protocol.
Validate CA Certificate	Enables or disables verification of the server certificate signature against the certificate installed on the IF61. If you enable verification, you need to specify the CA certificate common name.
CA Certificate Common Name	Common name for the server certificate.
Reject Expired Certificates	Check this check box to reject expired certificates.
Minimum Multicast Encryption	Choose a data encryption method for non-unicast transmission/reception: CCMP (RSN): Use Counter Mode - CBC MAC Protocol. TKIP (RSN): (Default) Choose Temporal Key Integrity Protocol. WEP (TSN): Choose WEP keying.
Pairwise Encryption (Unicast)	Choose a data encryption method for unicast transmission/reception: TKIP: (Default) Use Temporal Key Integrity Protocol. CCMP: Use Counter Mode - CBC MAC Protocol.

Configuring WPA2 Personal (PSK) Security

- 1 From the menu, click **Network Configuration > 802.11** or **802.11 Configuration**. The 802.11 Configuration screen appears.

Chapter 2 — Configuring Network Settings

The screenshot shows the Intermecc RFID web interface for 802.11 Configuration. The left navigation menu includes: Network Configuration, Ethernet, 802.11 (expanded), 802.11 Configuration (selected), 802.11 Status, Common, Device Management, Services, RFID Services, Edgware Applications, Security, Maintenance, and About. The main content area is titled '802.11 Configuration' and features an 'Activate Changes' button at the top. Below this, there are three sections: 'Radio Control' with 'Enable 802.11 Radio' checked; 'Radio Parameters' with 'SSID (Network Name)' set to 'INTERMEC', 'Security Level' set to 'None', and 'Display Advanced Radio Parameters' checked; and 'IPv4' with 'Enable DHCP' checked and IP Address, Subnet Mask, and Router all set to '0.0.0.0'. The 'IPv6' section is partially visible at the bottom.

- 2 Choose **WPA2 Personal (PSK)** from the **Security Level** drop-down list. The Security Parameters list appears:

This screenshot shows the same Intermecc RFID web interface, but with the 'Security Level' dropdown menu set to 'WPA2 Personal (PSK)'. This action has revealed the 'Security Parameters' section, which includes a 'Pre-shared Key (PSK)' field with masked characters (dots). The 'Display Advanced Security Parameters' checkbox is also checked. The other sections, including 'Radio Control', 'Radio Parameters', and 'IPv4', remain the same as in the previous screenshot.

- 3 Configure WPA2 Personal settings. For help, see the next table.
 - Click **Display Advanced Security Parameters** to see the current settings for multicast and pairwise encryption.

- 4 Click **Activate Changes** to save your settings and immediately make them active.

Parameters for WPA2 Personal Security

Parameter	Description
Pre-Shared Key (PSK)	The pre-shared key for WPA. You can enter an ASCII passphrase (range is 8 to 64 characters), and the key is derived from the passphrase using the PBKDF2 algorithm.
Minimum Multicast Encryption	Choose a data encryption method for non-unicast transmission/reception: CCMP (RSN): (Default) Use Counter Mode - CBC MAC Protocol. TKIP (RSN): Choose Temporal Key Integrity Protocol.
Pairwise Encryption (Unicast)	Choose a data encryption method for unicast transmission/reception: CCMP: (Default) Use Counter Mode - CBC MAC Protocol. TKIP: Use Temporal Key Integrity Protocol.

Configuring WPA2 Enterprise (802.1x) Security

- 1 From the menu, click **Network Configuration > 802.11** or **802.11 Configuration**. The 802.11 Configuration screen appears.

Chapter 2 — Configuring Network Settings

Intermec RFID
802.11 Configuration
Thursday, March 20, 2008 05:11:04

Navigation Menu

- Network Configuration
 - Ethernet
 - 802.11
 - 802.11 Configuration**
 - 802.11 Status
 - Common
 - Device Management
 - Services
- RFID Services
- Edgeware Applications
- Security
- Maintenance
- About

Activate Changes

Radio Control

Enable 802.11 Radio

Radio Parameters

SSID (Network Name)

Security Level

Display Advanced Radio Parameters

IPv4

Enable DHCP

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Router: 0.0.0.0

IPv6

IPv6 Autoconfigure

IPv6 Address: ::0

- Choose **WPA2 Enterprise (802.1x)** from the **Security Level** drop-down list. The Security Parameters list appears:

Intermec RFID
802.11 Configuration
Thursday, March 20, 2008 06:37:21

Navigation Menu

- Network Configuration
 - Ethernet
 - 802.11
 - 802.11 Configuration**
 - 802.11 Status
 - Common
 - Device Management
 - Services
- RFID Services
- Edgeware Applications
- Security
- Maintenance
- About

Activate Changes

Radio Control

Enable 802.11 Radio

Radio Parameters

SSID (Network Name)

Security Level

Display Advanced Radio Parameters

Security Parameters

Allowed EAP Authentication Method

Username

Password

Validate CA Certificate

Display Advanced Security Parameters

IPv4

Enable DHCP

- Configure WPA2 Enterprise settings. For help, see the next table.
 - Click **Display Advanced Security Parameters** to see the current settings for multicast and pairwise encryption.

- 4 Click **Activate Changes** to save your settings and immediately make them active.

Parameters for WPA2 Enterprise Security

Parameter	Description
Allowed EAP Authentication Method	Specifies which 802.1x authentication protocol (TLS, TTLS, PEAP, or LEAP) the IF61 sends to the authentication server if the server sends an unauthorized protocol.
Username	User name for TTLS, PEAP, or LEAP authentication.
Password	Password for TTLS, PEAP, or LEAP authentication.
Validate CA Certificate	Enables or disables verification of the server certificate signature against the certificate installed on the IF61.
CA Certificate Common Name	Common name for the server certificate.
Reject Expired Certificates	Check this check box to reject expired certificates.
Minimum WPA2 Multicast Encryption	Choose a data encryption method for non-unicast transmission/reception: CCMP (RSN): (Default) Use Counter Mode - CBC MAC Protocol for multicast/group keying. TKIP (RSN): Choose Temporal Key Integrity Protocol for multicast/group keying.
Pairwise Encryption (Unicast)	Choose a data encryption method for unicast transmission/reception: CCMP: (Default) Use Counter Mode - CBC MAC Protocol for multicast/group keying. TKIP: Use Temporal Key Integrity Protocol for multicast/group keying.

Managing Certificates

The default server certificate on the IF61 (ValidForHTTPSOnly) supports the secure web browser interface. You can use a third-party CA to issue unique client certificates and a root certificate.



Note: To install or uninstall certificates, you need to access the IF61 via a secure web browser. For help, see [“Using the Web Browser Interface” on page 11](#).

Viewing Certificates

You can use the web browser interface to view the certificates loaded on the IF61.

To view certificates

- From the menu, click **Security > Certificate Details**. The Certificate Details screen appears.



The Server Certificate table lists the server certificate that is installed, and the CA Certificate table lists the trusted CA certificate that is installed.

Installing and Uninstalling Certificates

Once you have determined that you need to install or uninstall a certificate, use this procedure.



Note: To install or uninstall certificates, you need to access the IF61 via a secure web browser. For help, see [“Using the Web Browser Interface” on page 11](#).

To install or uninstall certificates

- 1 From the main menu, click **Security > Import Certificate**. The Import Certificate screen appears.

Intermecc RFID

Intermecc Manual Help
Thursday, March 20, 2008 06:39:05

Navigation Menu

- Network Configuration
- RFID Services
- Edgeware Applications
- Security
 - Passwords
 - Import Certificate**
 - Certificate Details
- Maintenance
- About

Import Certificate

Warning: Do not close or navigate away from this page during import.

Server Certificate Trusted CA Certificate

Enter or select the name of the certificate file to import:

Enter the associated passphrase for this certificate:

This page allows server and trusted certificate authority (CA) certificates to be uploaded to this device.

Server certificates may be uploaded in either PKCS12 (.p12 or .pfx) or PEM (.pem) format. The server certificate file should contain the entire certificate chain with the server certificate and private key being first, followed by CA certificates in increasing order. If a server certificate is being imported, the passphrase used to encrypt the private key needs to be entered as well.

Trusted CA certificates may be uploaded in either PEM (.pem or .cer) or DER (.cer) format. The trusted CA certificate file should only contain the public certificate issued by the trusted CA.

The new certificate will be activated immediately upon successful import. If the import fails, a page will display the status and reason for failure.

- 2 Click **Browse** and follow the prompts to browse to the location of the certificate you want to install. Or, enter the path to the certificate in the **Enter or select the name of the certificate file to import** entry field.



Note: If you are not using a secure web browser, you will be prompted to log in again. Click **A secure session is available** and log in to the IF61. If a Security Alert dialog box appears, click **Yes** to proceed. Repeat Steps 1 and 2.

- 3 Click **Server Certificate** or **Trusted CA Certificate**.
- 4 (Server Certificate only) In the **Enter the associated passphrase for this certificate** field, carefully enter the passphrase for the certificate.
- 5 Click **Import Certificate**. If a Security Alert dialog box appears, click **Yes** to proceed.

Chapter 2 — Configuring Network Settings



3 Developing and Using RFID Applications

This chapter explains how you can develop and test RFID applications for the IF61 and includes these topics:

- RFID Applications and the IF61
- Creating RFID Applications for the IF61
- Installing RFID Applications on the IF61
- About the IF61 Edgeware Applications
- About RFID Services
- Configuring BRI Settings
- Configuring LLRP Settings
- About the Developer Tools

This chapter assumes you are familiar with developing applications and with your RFID system.

RFID Applications and the IF61

The IF61 supports Java and C# applications. Your application communicates with the IF61 through one of two RFID services:

- the Basic Reader Interface (BRI) server, which controls the reader by issuing BRI commands. For more information on the BRI server, see “[Configuring the BRI Server](#)” on page 69.

For more information on using BRI, see the *Basic Reader Interface Programmer’s Reference Manual* (P/N 937-000-xxx).

- the Low-Level Reader Protocol (LLRP), based on the EPCglobal standard. For more information on LLRP settings, see “[Configuring LLRP Settings](#)” on page 71.

There are two ways to use the IF61 with your RFID application:

- You can run the application on a remote server. In this case, all processing is performed by the server.
- You can run the application locally on the IF61. In this case, the application resides on the IF61, and much of the processing occurs on the IF61 and not remotely on the server.

Running your application on the IF61 improves system scalability by minimizing network traffic, since the IF61 can handle many processing tasks such as data filtering.

You can set up your application to auto-start when the IF61 boots. For more information, see “[Auto-Starting Applications at Boot Time](#)” on page 57.

If your application uses the IF61 GPIO interfaces to control external devices such as indicator lamps, running the application on the IF61 decreases response time for those devices. For more information, see Chapter 5, “[Using the IF61 GPIO Interfaces.](#)”

Using the RFID Resource Kit

The Intermec Developer Library RFID Resource Kit includes Java and C# tools you can use to develop applications that enable control of the reader and data management.

The resource kit is available as part of the Intermec Developer Library (IDL). To learn more about the RFID Resource Kit, go to www.intermec.com and choose **Products > Applications and Software > Development Tools > Developer Resource Kits**.

Creating RFID Applications for the IF61

Intermec recommends this general outline for developing your RFID application:

- 1 Write and test your application on a development workstation (your desktop PC). The application can access the IF61 via TCP on port 2189.
- 2 After testing is complete, install the application on the IF61. For help with installing applications on the IF61, see [“Installing RFID Applications on the IF61” on page 59](#).



Note: If you plan to auto-start your application when the IF61 boots, Intermec recommends that you install your software on the IF61 and start it manually to verify that the executable or script runs properly. Then you can use the web browser interface to configure the application to auto-start at boot time. For information about starting an application manually, see [“Managing Applications” on page 60](#).

Delivering Applications to the IF61

For Java applications:

- Create a .zip file that includes your Java application (.tar, .gz, .bz2, or .zip format only), RFID Java libraries, and a configuration file. Install the .zip file on the IF61 as described in [“Installing RFID Applications on the IF61” on page 59](#). Be sure to specify the class path to the libraries.

For more information on configuration files, see the next section.

For help with executing Java applications, see [“Executing Java Applications” on page 57](#).

For C# applications:

- Create a .zip file that includes your application (.exe), all required DLLs, and a configuration file. Install the .zip file on the IF61 as described in [“Installing RFID Applications on the IF61” on page 59](#).

For more information on configuration files, see the next section.

About Configuration Files

When you package your application for installation on the IF61, you need to include a configuration file in the root directory of the archive. The file must be named “userapp.conf” and must include this syntax:

```
AUTOSTART=true|false  
RUNAFTERINSTALL=true|false  
CMDLINE=<command line to start the application>
```

where:

`AUTOSTART` specifies whether or not the application should automatically be executed when the IF61 boots. When `AUTOSTART=true`, the Auto-Start check box for this application on the Application Control screen will be checked.



Note: After you install the application on the IF61, you can enable or disable the auto-start feature from the web browser interface. For help, see [“Managing Applications” on page 60](#).

`RUNAFTERINSTALL` specifies whether or not the application should be started immediately after installation.

`CMDLINE` specifies the application name and optional parameters it accepts. Specify command line parameters as if the application is being executed from inside the directory containing the application.



Note: Do not use the `$JAVA_HOME` environment variable in the command line.

This example runs a C# application named “testapp.exe” using the Mono runtime:

```
CMDLINE=./testapp.exe
```

For Java applications, `CMDLINE` should specify the Java interpreter location, the classpath, and the class containing the application’s entry point. This example runs the class “HelloWorld”:

```
CMDLINE=/usr/java/bin/java -cp . HelloWorld
```



Note: The IF61 executes applications from their installation directories, so the userapp.conf file does not need to include path information.

Auto-Starting Applications at Boot Time

There are two ways to configure your application to auto-start when the IF61 boots:

- Specify `AUTOSTART=true` in the configuration file that you deliver with the application. For more information, see the previous section, “About Configuration Files.”
- After you install the application on the IF61, you can use the web browser interface to configure the application to auto-start at boot time. For help, see “[Managing Applications](#)” on [page 60](#).

IF61 .NET Support

The IF61 supports applications based on .NET Framework 1.0, 1.1, and 2.0. The IF61 uses Mono open source software to provide support for .NET applications deployed on the IF61 Linux operating system.



Note: The IF61 does not support ASP.NET.

IF61 Java Support

The IF61 comes with a JDBC driver you can use to create applications that write data directly from the IF61 to a remote database. For more information, see “[Java Support for Microsoft SQL Server and Sybase](#)” on [page 58](#).

For more sophisticated Java development, the IF61 supports the open standard OSGi service-oriented architecture. This allows system administrators to install, uninstall, enable, and disable system services (also known as bundles) without having to reboot the IF61 each time. To use OSGi effectively, you need an OSGi server. For more information, see www.osgi.org.

Executing Java Applications

To execute a Java application on the IF61, use this command:

```
$JAVA_HOME/bin/java myJavaClass
```

To execute .jar files, use this command:

```
$JAVA_HOME/bin/java -jar myApplication.jar
```



Note: Your .jar files must have manifest files included within them or the command will not work.

- The manifest needs to include an attribute called “Main-Class” to specify the application’s entry point (for example, Main-Class: MyJavaClass).
- If the executable .jar needs to reference other .jar files, specify the files in the manifest file using the “Class-Path” attribute.

To enable the Java just-in-time (JIT) compiler for maximum performance, use this command:

```
$JAVA_HOME/bin/java -jit java -jar MyJar.jar
```

where:

`$JAVA_HOME` is an environment variable that indicates the Java runtime installation path (`/usr/java`). Always use this variable for simplicity and to insure that the correct runtime files are used.

`java` is the name of the Java runtime executable installed in the IF61.

If your application references third party Java libraries (such as components from the Intermec RFID Resource Kit), you must use the “-cp” option to specify the class path for the JVM to find the Java classes. Be sure to include the current path so classes in the current directory can be found, as shown in this example:

```
$JAVA_HOME/bin/java -cp ../BasicRFID.jar MyClass
```

Java Support for Microsoft SQL Server and Sybase

The IF61 jTDS driver (version 1.2) provides JDBC capabilities to Java applications running on the IF61. You need to include the location of the JDBC drivers in the class path. Use the environment variable `$JDBC_HOME` as shown in this example:

```
$JAVA_HOME/bin/java -cp $JDBC_HOME/jtds-j2me-1.0.2.jar:. MyClass
```

The IF61 JDBC driver supports JDBC 1.0 and:

- Microsoft SQL Server versions 6.5, 7, 2000, and 2005.
- Sybase versions 10, 11,12, and 15.

For more information on the jTDS driver, see <http://jtds.sourceforge.net>.

IF61 JavaScript Support

The IF61 supports applications developed with JavaScript. Because JavaScript RFID applications can generally be written quickly, JavaScript is an ideal tool for creating demonstration or proof-of-concept applications as well as production RFID software.

You can configure the IF61 to auto-start a JavaScript application residing on the IF61 or on a remote server. The IF61 JavaScript implementation includes built-in objects that provide access to the BRI and the TCP, HTTP, SQL, and XML interfaces.

For help with running a JavaScript file at boot time, see [“Configuring a JavaScript File to Auto-Run at Boot Time” on page 77.](#)

Installing RFID Applications on the IF61

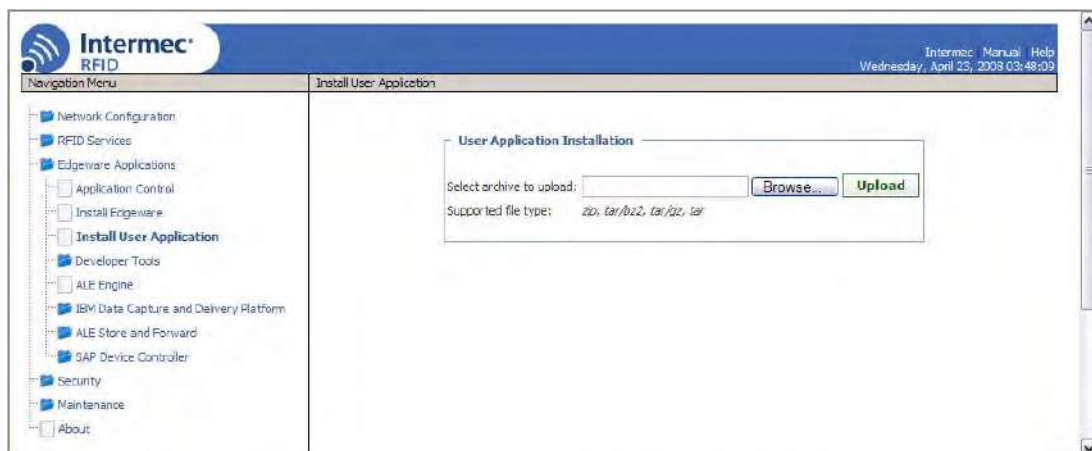
The IF61 provides up to 1 GB of memory for your applications. You use the web browser interface to install applications on the IF61. For help, see the next procedure.



Note: The IF61 only supports these formats: .zip, .tar, .tar/bz2, and .tar/gz. To install Intermec edgeware applications in .bin format, see [“Upgrading or Installing Edgeware Applications” on page 62.](#)

To install applications on the IF61

- 1 From the menu, click **Edgeware Applications > Install User Application**. The Install User Application screen appears.



Chapter 3 — Developing and Using RFID Applications

- 2 Click **Browse** and follow the prompts to navigate to the location of the application file.
- 3 Click **Upload**. The application is uploaded to the IF61.

Managing Applications

To maximize IF61 resources, you can start, stop, or uninstall IF61 edgware applications or your installed applications from the web browser interface. You can also configure applications to auto-start at boot time. For more information, see the next section.

To manage applications

- 1 From the menu, click **Edgware Applications > Application Control**. The Application Control screen appears.






The Edgware Applications section lists all installed edgware. The User Applications section lists all applications you have installed through the web browser interface.

In this screen, you can:

- specify which applications automatically start when the IF61 boots.
- turn applications on and off in real time.
- uninstall applications (except for Developer Tools).

- 2 Choose an option:

- Check the Auto-Start check box if you want an application to automatically launch when the IF61 boots.

- Click  to stop a running application.
- Click  to start an application.
- Click  to uninstall an application.
- Click **Activate Changes** to save your changes and immediately make them active.



Note: If you change the date or time on the IF61, stop and restart any running applications (or reboot the IF61) for the date and time changes to be made effective.

About the IF61 Edgeware Applications

Edgeware applications are supplied by Intermec and its partner developers, and provide immediate functionality for your RFID system. The IF61 includes these edgeware applications:

- The Developer Tools. Use the Developer Tools to test your RFID systems and settings. For more information, see [“About the Developer Tools” on page 73](#).
- The SAP device controller. Enable this edgeware so the controller communicates with the SAP backend module on your server. For more information on SAP implementation on the IF61, see the *IF61 SAP Device Controller User’s Guide* (P/N 934-025-xxx).
- The Application Level Events (ALE) Engine. Enable this edgeware so the IF61 ALE engine communicates with your ALE application. For more information on ALE implementation on the IF61, see the *IF61 Application Level Engine (ALE) User’s Guide* (P/N 934-026-xxx).
- ALE Store and Forward. This application reads tags, saves tag data, and forwards the data to a shared folder on a host PC or to a TCP/IP socket. Store and Forward works as an ALE client using the IF61 ALE engine. For more information, see the *ALE Store and Forward User’s Guide* (P/N 934-034-xxx).

You can uninstall any edgeware application other than the Developer Tools. For help, see the previous section, “Managing Applications.”

Chapter 3 — Developing and Using RFID Applications

Intermec may provide upgrades for existing edgeware applications, as well as additional edgeware applications you can install. For help with locating IF61 upgrades at www.intermec.com, see “[Accessing Intermec Web Pages](#)” on [page 107](#). To install or upgrade edgeware applications, see the next section.

Upgrading or Installing Edgeware Applications

You use the web browser interface to install or upgrade IF61 edgeware applications, such as the SAP device controller or ALE engine. For help, see the next procedure.



Note: Use only .bin files provided by Intermec. To install your own applications in .zip, .tar, .tar/bz2, or .tar/gz formats, see “[Installing RFID Applications on the IF61](#)” on [page 59](#).

To install or upgrade edgeware

- 1 From the menu, click **Edgeware Applications > Install Edgeware**. The Install Edgeware screen appears.



- 2 Click **Browse** and follow the prompts to navigate to the location of the .bin file.
- 3 Click **Upload**. The application file is installed on the IF61. When the installation is complete, the IF61 reboots.



Note: For information on uninstalling edgeware applications, see “[Managing Applications](#)” on [page 60](#).

About RFID Services

The RFID service sets the protocol your application uses to communicate with the RFID module. The available services are:

- BRI (Basic Reader Interface) - Intermec proprietary protocol for controlling the reader. To configure BRI settings, see the next section.
- LLRP (Low-Level Reader Protocol) - EPCglobal standard for network interfaces between the RFID reader and its controlling software. To configure LLRP settings, see [“Configuring LLRP Settings” on page 71](#).

Configuring BRI Settings

By default, the IF61 reader module uses BRI as its main protocol. This section explains how to configure BRI settings that control reader operation and communication with your application:

- To configure BRI attribute settings that control reader operation, such as read and write tries, tag types, or antenna settings, see the next section, “Changing BRI Attribute Settings.”
- To configure BRI server settings, which manage how your application communicates with the reader, see [“Configuring the BRI Server” on page 69](#).

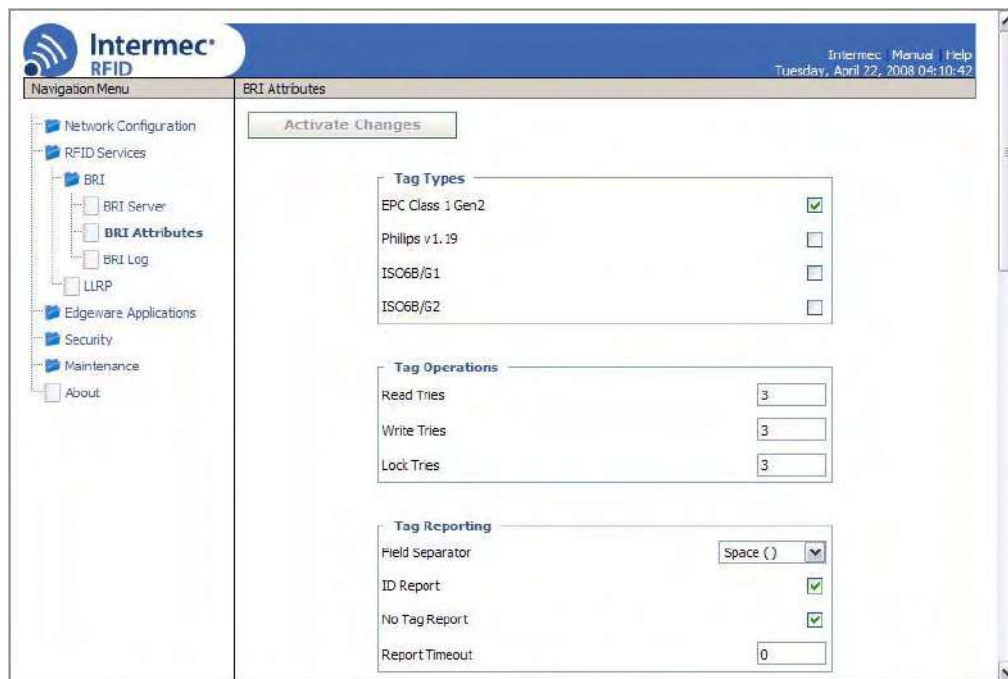
Changing BRI Attribute Settings

BRI attribute settings control how the IF61 reader module reads tags. Follow the next procedure to change attribute settings.

When you use the Diagnostics tool to display tags, the IF61 RFID module uses settings from the BRI Attributes screen. For help, see [“Testing the GPIO Interfaces” on page 73](#).

To change BRI attribute settings

- 1 From the menu, click **RFID Services > BRI > BRI Attributes**. The BRI Attributes screen appears.



- 2 Change RFID settings as needed. For help, see the next section.
- 3 Click **Activate Changes** to save your changes and immediately make them active.

About BRI Attribute Settings

This section explains the BRI attribute settings that control how the reader operates. For more information, see the *Basic Reader Interface Programmer's Reference Manual* (P/N 937-000-xxx).

Tag Types

Check the appropriate check boxes to enable RFID operations for these kinds of tags:

- EPC Class 1 Gen 2 (default)
- Phillips v1.19
- ISO6B/G1
- ISO6B/G2

This setting is equivalent to the TAGTYPE BRI attribute.

Read Tries

Sets the maximum number of times the read algorithm is executed before a response is returned to a Read command.

In practice, this is the number of times an identified tag is read until the Read is successful. Valid range is 1 to 254 (default is 3).

This setting is equivalent to the RDTRIES BRI attribute.

Write Tries

Sets the maximum number of times the write algorithm is executed before a response is returned to a Write command.

In practice, this is the number of times an identified tag is written to until the Write is successful. Valid range is 1 to 254 (default is 3).

This setting is equivalent to the WRTRIES BRI attribute.

Lock Tries

Sets the maximum number of times the lock algorithm is executed before a response is returned to a Lock command. Valid range is 1 to 254 (default is 3).

This setting is equivalent to the LOCKTRIES BRI attribute.

Field Separator

Sets the space character to be used for separating fields in tag data. Choose from space (), comma (,), colon (:), semicolon (;), tab, caret (^), or tilde (-). Default is space.

This setting is equivalent to the FIELDSEP BRI attribute.

ID Report

Enables or disables tag ID reporting after a Read, Write, or Lock command is executed:

- For ISO tags, the tag identifier corresponds to TAGID.
- For EPC tags, the identifier corresponds to EPCID.

Check the check box to enable tag ID reporting. This setting is equivalent to the IDREPORT BRI attribute, and is enabled by default.

No Tag Report

Enables or disables a NOTAG message, which is sent when no tags are found during execution of a Read, Write, or Lock command. Check the check box to enable the message. This setting is equivalent to the NOTAGRPT BRI attribute, and is enabled by default.

Report Timeout

Sets the timeout (in ms) for delays in tag reporting when the IF61 is in continuous read mode. Range is 0 (default) to 65534.

Timeout Configuration Mode

Enables a timeout mode. Instead of specifying the number of antenna or ID tries, you specify an antenna or ID timeout value. If the IF61 does not find any tags after an antenna or ID try, the reader waits this long before starting the next antenna or ID try. If you enable timeout mode, you need to set the ID Timeout and Antenna Timeout values.

This setting is equivalent to the TIMEOUTMODE BRI attribute, and is disabled by default.

To enable Timeout Configuration mode

- 1 Check the check box and then click **Activate Changes**. The screen refreshes. The Antenna Tries setting is replaced by Antenna Timeout, and the ID Tries setting is replaced by ID Timeout.
- 2 Specify the value (in ms) for the antenna or ID timeout in the entry fields and then click **Activate Changes**.

For more information on ID Timeout and Antenna Timeout, see those topics later in this section.

Select Tries

(Not supported by EPCglobal Class 1 Gen 2 tags) Sets the number of times a group select is attempted. A group select is the command that starts the identity process. Valid range is 1 (default) to 254.

This setting is equivalent to the SELTRIES BRI attribute.

Unselect Tries

(Not supported by EPCglobal Class 1 Gen 2 tags) Sets the number of times a group unselect is attempted. Valid range is 1 (default) to 254.

Session

(EPCglobal Class 1 Gen 2 tags only) Sets the command session parameter to the corresponding EPCglobal Class 1 Gen 2 air protocol command (default is QueryAdjust).

This setting is equivalent to the SESSION BRI attribute. For more information on this setting, see the EPCglobal Class 1 Gen 2 documentation.

Initial Q

(EPCglobal Class 1 Gen 2 tags only) Sets the initial Q parameter value used by the Query command. Valid range is 0 to 15 (default is 4). If you know there is only one tag in the field, set this attribute to 0 for best performance.

This setting is equivalent to the INITIALQ BRI attribute.

Initialization Tries

Sets the maximum number of times the reader attempts to initialize a tag. Valid range is 1 (default) to 254.

This setting is equivalent to the INITTRIES BRI attribute.

ID Tries

Sets the maximum number of times the reader executes the identify algorithm before a response is returned to a Read or Write command.

In practice, this is the number of times a tag ID attempt is made for each antenna being used. Valid range is 1 to 254 (default is 3).

This setting is equivalent to the IDTRIES BRI attribute.

ID Timeout

Sets the ID timeout value (in ms) when Timeout Configuration mode is enabled. Range is 0 to 65534 (default is 100). This setting is visible only if Timeout Configuration mode has been enabled. For help, see “Timeout Configuration Mode” in this section.

This setting is equivalent to the IDTIMEOUT BRI attribute.

Antenna Tries

Sets the maximum number of ID Tries that the reader executes per antenna. Valid range is 1 to 254 (default is 3).

This setting is equivalent to the ANTTRIES BRI attribute.

Antenna Timeout

Sets the antenna timeout value (in ms) when Timeout Configuration mode is enabled. Range is 0 to 65534 (default is 50). This setting is visible only if Timeout Configuration mode has been enabled. For help, see “Timeout Configuration Mode” in this section.

This setting is equivalent to the ANTTIMEOUT BRI attribute.

Dense Reader Mode

Check this check box to enable dense reader mode, which is only supported by EPC Class 1 Gen 2 tags. When dense reader mode is enabled, these tags respond with Miller Sub carrier encoded data instead of FM0 encoded data.

LBT Scan Enable

(Supported only by 865 MHz readers) Enables Listen Before Talk (LBT) scanning. LBT scanning is enabled by default (disabled by default on IF61 models with 4 channels).

When LBT scanning is enabled, the algorithm scans the available ETSI 302-208 channels for a free transmit channel. The scan sequence begins with the channel specified by LBT Channel (default is 8), and every third channel is checked (for example, 8, 11, 4, 7, 10, 13, 6, 9, 12, 5) until a free channel is found. If a free channel is not found, LBT repeats the scan sequence.

When LBT scanning is not enabled, the IF61 does not scan for a free transmit channel, and the transmit channel is set by LBT Channel.

LBT Channel

(Supported only by 865 MHz readers) Sets the default transmit channel (of the available ETSI 302-208 channels). When LBT scanning is enabled, the channel scan sequence starts with this channel. When LBT scanning is not enabled, this is the only transmit channel used. Range is 4 to 13 and default channel is 8.

For IF61 models with 4 channels, choose from channels 4, 7 (default), 10, or 13.

Field Strength 1 to 4

Sets the RF power level (in dBm) for each of the 4 antenna ports. Valid range is 15 to 30 (maximum power). Default is 30.

Use this setting to attenuate the antenna field strength. In some situations, full output power can cause unnecessary interference. For example, if the tag is close to the antenna, full output power might overload the tag and cause unreliable behavior.

This setting is equivalent to the FIELDSTRENGTH BRI attribute.

Antenna Sequence: First through Eighth

Sets the RFID antenna to be used for each of up to eight tag inventory operations. Choose any one of the four available antennas from the drop-down list. If more than one antenna is enabled, the antennas fire in this sequence.

This setting is equivalent to the ANTS BRI attribute.

Configuring the BRI Server

The IF61 BRI server handles communication between your application and the RFID module. When your application is communicating with the BRI server, the blue Intermec Ready-To-Work Indicator on the IF61 front panel turns on and stays on. For more information, see [“About the Intermec Ready-To-Work Indicator” on page 7](#).

To configure BRI server settings

- 1 From the menu, click **RFID Services > BRI > BRI Server**. The BRI Server screen appears.



- 2 Change BRI server settings as needed. For help, see the next table.

- 3 Click **Activate Changes** to save your changes and immediately make them active.

BRI Server Parameter Descriptions

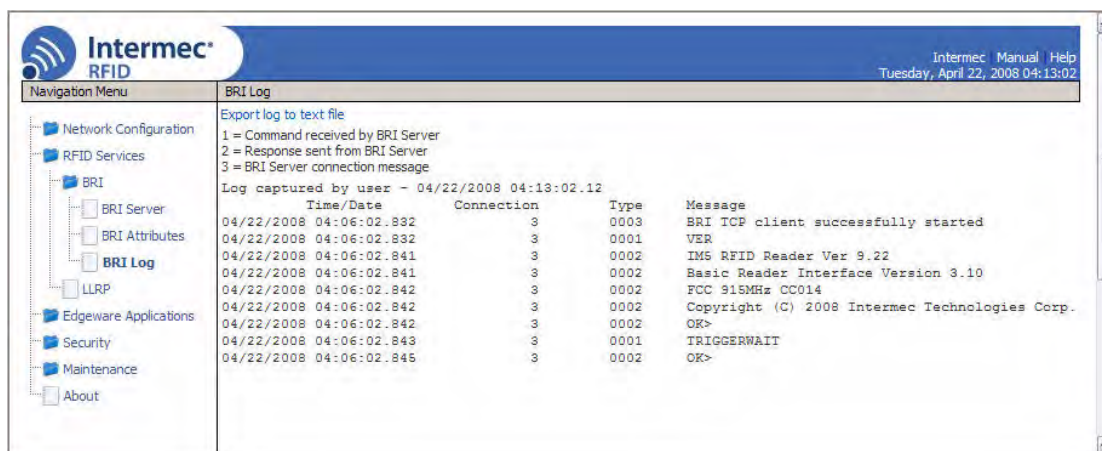
Parameter	Description
Enable External BRI Connections	Enables/disables external TCP connections to the BRI server. If this check box is not checked, the BRI server only accepts connections from applications installed on the IF61.
BRI TCP Port	Specifies the TCP port used for incoming connections to the BRI server. This port must be unique for all TCP services running on the IF61. Valid range is 2189 to 65535. Default is 2189.
Enable Logging	Enables/disables logging of BRI server events. For more information on logging, see the next section.

Viewing the BRI Server Log

If you enable logging, you can see a list of BRI server events. You can save the logfile as a .txt file.

To enable BRI server logging and view the logfile

- 1 Enable BRI logging as described in the previous section, “Configuring the BRI Server.”
- 2 In the left-hand navigation list, click **RFID Services > BRI > BRI Log**. The BRI Log screen appears with a list of BRI events. For more information on server events, see the next table, “BRI Event Descriptions.”



- 3 To save the log file, click **Export log to text file** and then choose **File > Save As**. Follow the prompts to save the log file to your desktop PC.

BRI Event Descriptions

Event Name	Description
Time/Date	Time and date of the event.
Connection	TCP port of the event. 0 indicates a serial connection.
Type	Message type of the event, generally indicating which system sent the message: 1 = Command received by BRI server 2 = Response sent by BRI server 3 = BRI server connection message
Message	Text of the message, including responses.

Configuring LLRP Settings

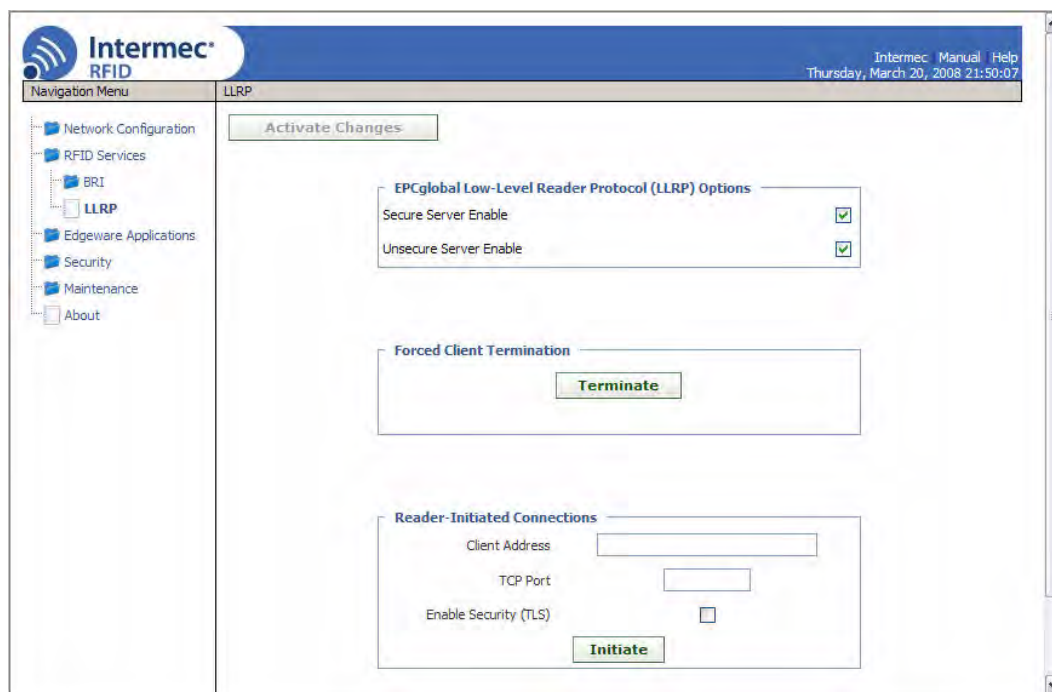
The IF61 supports version 1.0.1 of the EPCglobal Low-Level Reader Protocol (LLRP), which establishes a specific interface method between a reader and its corresponding client. Follow the next procedure to configure LLRP settings.



Note: For information on LLRP, including standards, see <http://www.epcglobalinc.org/standards/llrp>.

To configure LLRP settings

- 1 From the menu, click **RFID Services > LLRP**. The LLRP screen appears.



2 Configure LLRP settings as needed. For help, see the next table.

- To disconnect an existing LLRP connection, click **Terminate**.
- To connect to a remote LLRP client, enter information in the Reader-Initiated Connections section, and then click **Initiate**.

3 Click **Activate Changes** to save your changes and immediately make them active.

LLRP Settings Descriptions

Setting	Description
Secure Server Enable	Check this check box to allow connections to the secure LLRP server on port 5085.
Unsecure Server Enable	Check this check box to allow connections to the unsecure LLRP server on port 5084.

LLRP Settings Descriptions (continued)

Setting	Description
Reader-Initiated Connections	<p>For reader-initiated TCP/IP connections to a remote LLRP client, enter this information:</p> <ul style="list-style-type: none"> • Client Address - IP address of the remote LLRP client. • TCP Port - Port number for the TCP/IP socket connection. • Enable Security (TLS) - Check this check box to enable Transport Layer Security for this TCP/IP connection.

About the Developer Tools

Use the Developer Tools for basic testing of your RFID system. The Developer Tools support these features:

- General purpose input/output (GPIO) testing. For help, see the next section.
- Sending BRI commands or BRI script files to the IF61 from an interactive browser interface. For help, see [“Sending BRI Commands and Running Scripts” on page 74.](#)
- Editing and testing JavaScript files. For help, see [“Using the Workbench” on page 76.](#)



Note: To use the Developer Tools, you need to enable them. For help, see [“About the IF61 Edgware Applications” on page 61.](#)

Testing the GPIO Interfaces

If you have external GPIO controls such as motion sensors or indicator lamps connected to the IF61, you can use the Diagnostics tool to test the interfaces and verify that the controls behave as expected. Leave the controls connected to the IF61 GPIO port when using the Diagnostics tool.

To test the GPIO interfaces

- 1 From the menu, click **Edgware Applications > Developer Tools > GPIO**. The GPIO screen appears.



When this screen appears, the four IF61 GPIO interfaces are turned off.

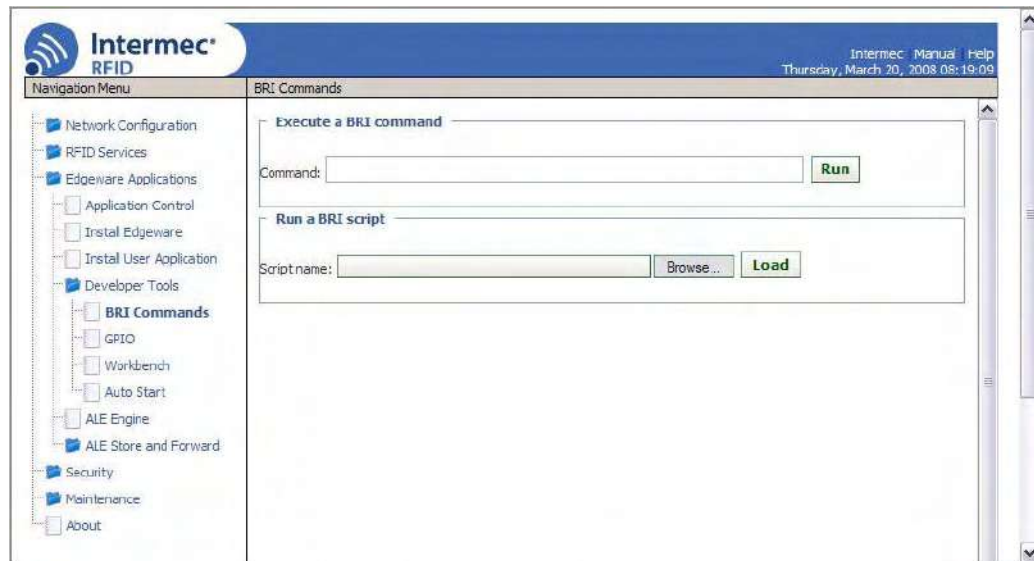
- 2 Check the check box for each of the GPIO interfaces you want to test. When you check the check box, that GPIO output will be turned on, and its associated GPIO input is turned on.
- 3 Click **Read and Write GPIO**. The GPIO interface state is changed.

Sending BRI Commands and Running Scripts

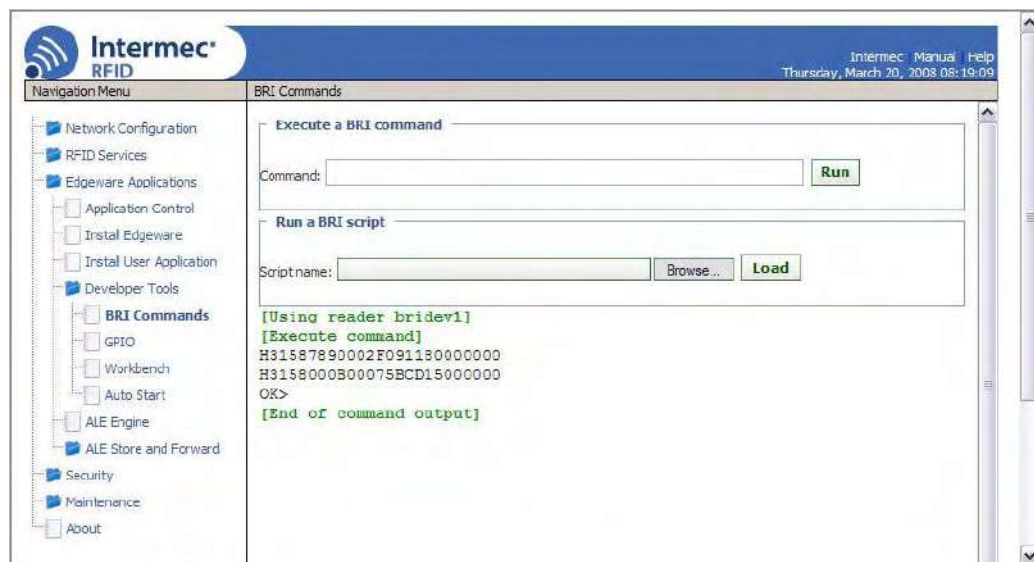
You can send BRI commands to the IF61 or load and run a BRI script through the web browser interface. For more information on BRI commands and syntax, see the BRI programmer's reference manual.

To send BRI commands

- 1 From the menu, click **Edgeware Applications > Developer Tools > BRI Commands**. The BRI Commands screen appears.



- 2 Enter the BRI command in the **Command** entry field.
- 3 Click **Run**. The command is executed and return values appear onscreen. For example, if you sent the ATTRIB command, the reader attributes appear in the list.



To load and run a BRI script

- 1 From the menu, click **Edgeware Applications > Developer Tools > BRI Commands**. The BRI Commands screen appears.
- 2 Click **Browse** and browse to the location of the BRI script.

Chapter 3 — Developing and Using RFID Applications

- 3 Double-click the name of the file. The script filename appears in the **Script name** field.
- 4 Click **Load**. The script is loaded and run, and return values appear onscreen.

Using the Workbench

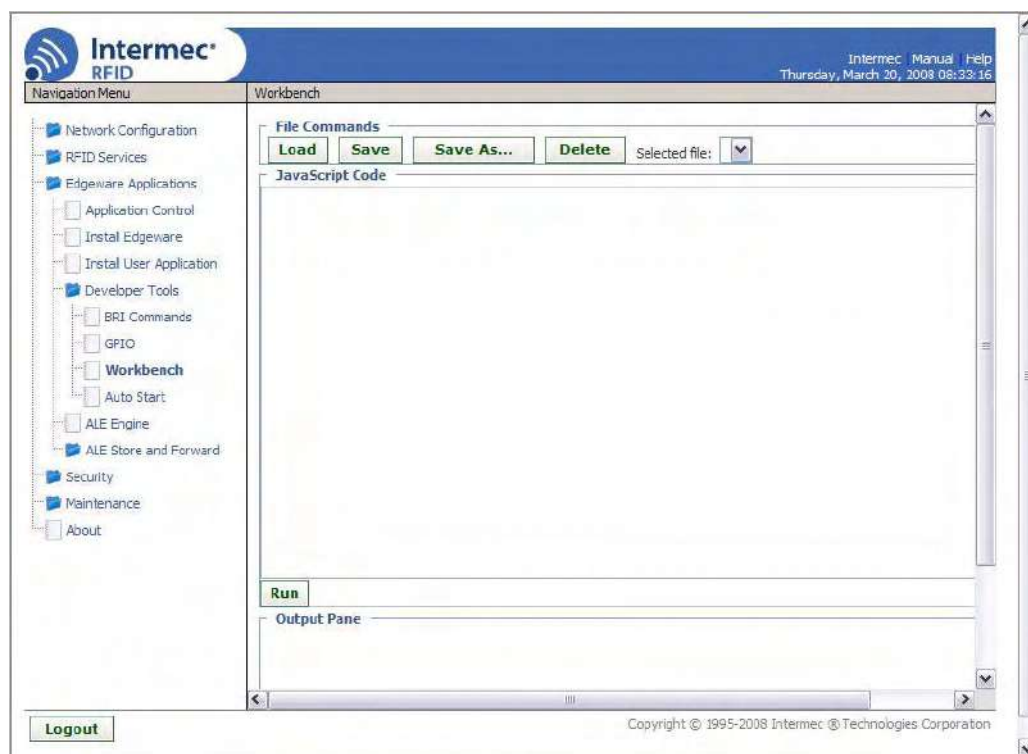
You can create and edit a JavaScript file, load the file on the IF61, and run the file from the Workbench.



Note: These instructions assume you understand how to create and edit JavaScript files.

To create and run a JavaScript file

- 1 From the menu, click **Edgware Applications > Developer Tools > Workbench**. The Workbench screen appears.



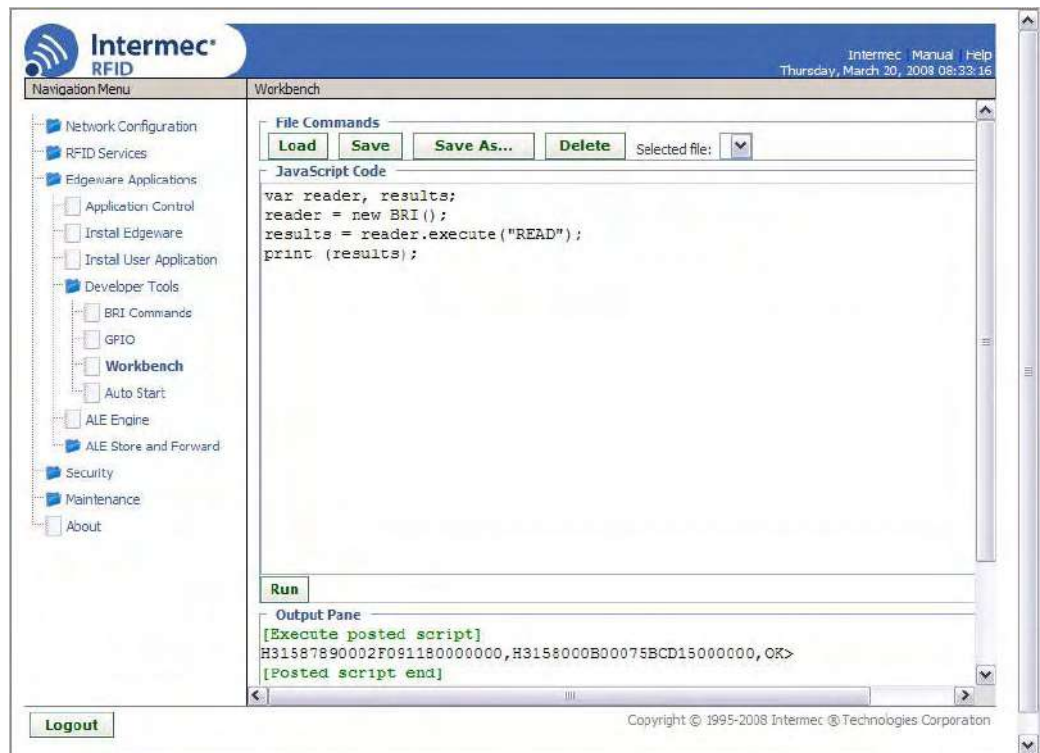
- 2 Click in the JavaScript Code box to enter code. You can also paste text copied from Notepad or another application. Copy the text from the other application and choose **Edit > Paste** in the browser menu.

- 3 To save your JavaScript code to the IF61 work buffer, click **Save**. The script is saved with the path and filename `/conf/js/work.js`.

To save your JavaScript to a different directory or with a different file name, click **Save As** and enter the new path and file name in the entry field. Click **OK**.

If you previously saved your JavaScript, click **Load** to reload it in the JavaScript Code box.

- 4 Click **Run**. The IF61 runs the JavaScript. Responses from the reader appear in the output pane. For example, if your script instructed the reader to read tags, the tag IDs appear in the Output Pane.



Configuring a JavaScript File to Auto-Run at Boot Time



Note: For help with configuring the IF61 to run other executables or scripts when the IF61 boots, see [“Auto-Starting Applications at Boot Time”](#) on page 57.

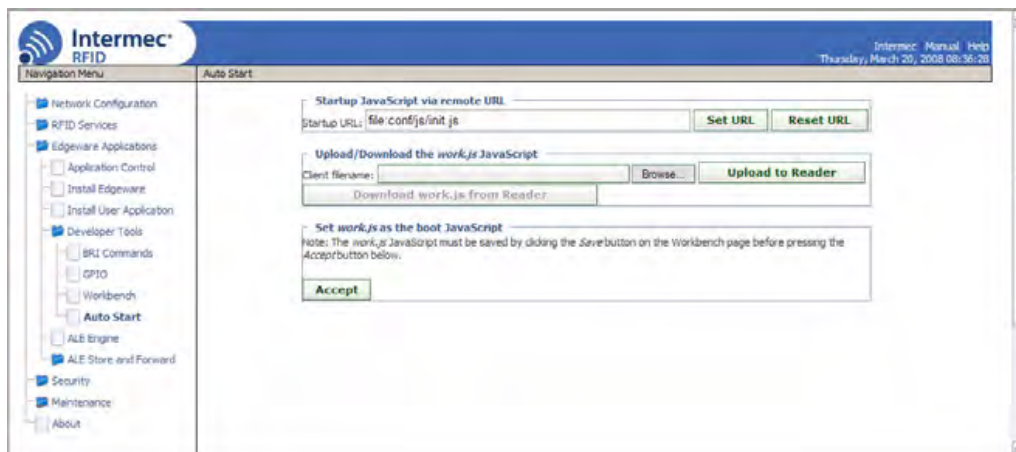
This section explains how to configure a JavaScript file to run automatically when the IF61 is rebooted.

Chapter 3 — Developing and Using RFID Applications

The startup file can be located on the IF61 or hosted on a remote server. When you set the file URL, a copy of the file is cached on the IF61 and executed if the server is unavailable at boot time.

To configure a JavaScript file to auto-run at boot time

- 1 From the menu, click **Edgeware Applications > Developer Tools > Auto Start**. The Auto Start screen appears with the default startup path (`file:conf/js/init.js`) in the **Startup URL** field.



- 2 To specify a different startup file, enter the path to and name of the file in the **Startup URL** field.

- For a startup file that will reside on the IF61, use this format:

`file:mydirectory/myfilename.js`

where:

mydirectory is the name of the directory on the IF61 where the file will be located.

myfilename.js is the name of the file.

- For a startup file on a remote server, enter the URL as you would in a web browser Address field, as in this example:

`http://www.mycompany.com/IF61startup/myfilename.js`

- 3 Click **Set URL**. The file is configured to be the startup file. If the file is hosted remotely, a copy of the file is cached on the IF61 for use if the remote server is not available at boot time.

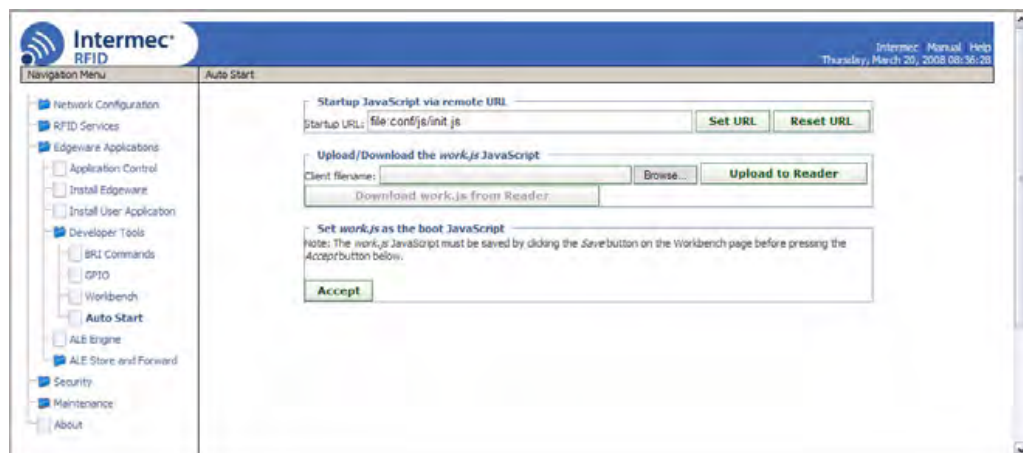
To reset the URL to the default (file:conf/js/init.js), click **Reset URL**.

Editing Remote Startup Files

To edit a remote startup file, you can upload the file from a remote server to the Workbench screen, where you can edit, test, and save your changes. You can also download the file from the IF61 to your desktop PC.

To edit a remote startup file

- 1 From the menu, click **Edgeware Applications > Developer Tools > Auto Start**. The Auto Start screen appears.



- 2 Click **Browse** to browse to the startup file location, and double-click the file name. The path to and name of the file appear in the **Client filename** field.
- 3 Click **Upload to Reader**. The file is uploaded to the IF61.
- 4 In the left-hand pane, click **Workbench**. The Workbench screen appears.
- 5 Click **Load**. The file contents appear in the JavaScript Code box.
- 6 Edit the file. You can run the file to test it, and save it when you are finished editing. For help, see [“Using the Workbench” on page 76](#).

Chapter 3 — Developing and Using RFID Applications

7 After you save the file, click **Auto Start** in the left-hand pane. The Auto Start screen appears.

8 To set the saved file as the startup file, click **Accept**.

To download the file from the IF61 to another location, click **Download work.js from Reader**. Follow the prompts to save the file.



Note: Before you can set the saved file as the startup file or download it from the reader, you need to save the file as described in Step 6.



4 Managing, Troubleshooting, and Upgrading the IF61

This chapter includes information on managing the IF61 and includes these topics:

- Managing the IF61
- Using the Device Configuration Web Service
- Using Simple Network Management Protocol (SNMP)
- Using SmartSystems Foundation
- Using Wavelink Avalanche
- Importing and Exporting Files
- Accessing the IF61 via the Linux Shell
- Opening a Serial Connection to the IF61
- Maintaining the IF61
- Troubleshooting the IF61
- Calling Intermec Product Support
- Accessing Intermec Web Pages
- Upgrading Firmware

Managing the IF61

There are several methods you can use to manage the IF61. You can use:

- a web browser. For help, see “[Using the Web Browser Interface](#)” on page 11. This manual assumes you are using this method for all procedures.
- the Device Configuration web service. For help, see the next section.
- an SNMP management station. For help, see “[Using Simple Network Management Protocol \(SNMP\)](#)” on page 84.
- the Wavelink Avalanche client management system. For help, see “[Using Wavelink Avalanche](#)” on page 89.
- the Intermec SmartSystems Console. For help, see “[Using SmartSystems Foundation](#)” on page 87.

Using the Device Configuration Web Service

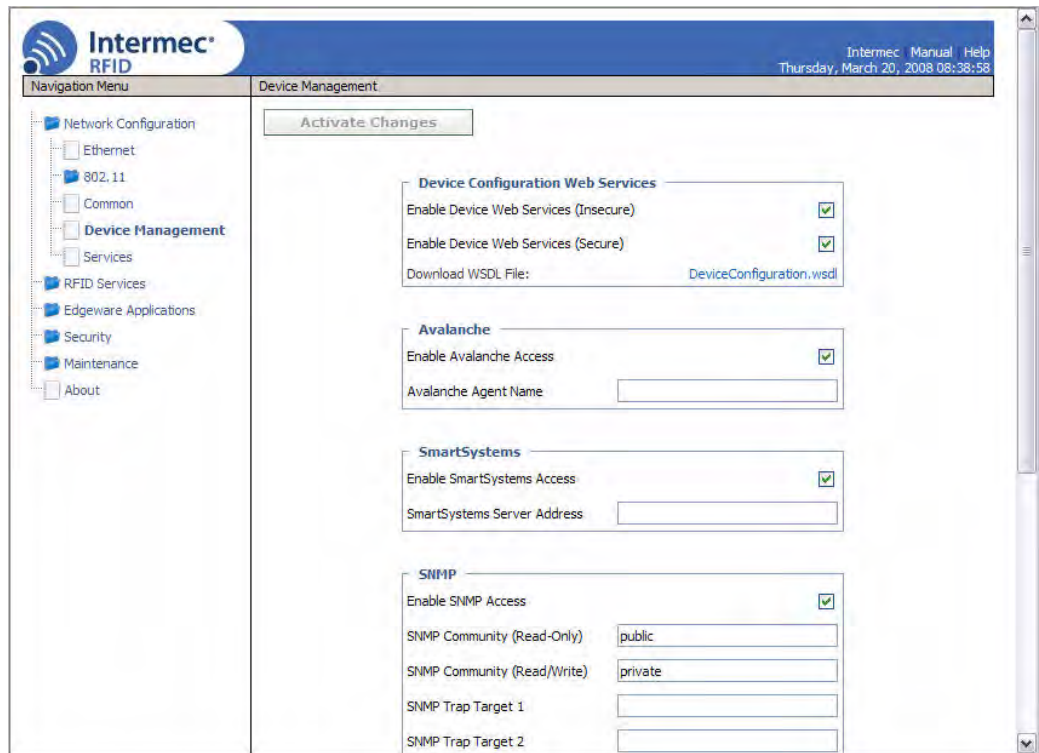
The Device Configuration web service provides a way to programmatically configure the IF61 over your network. This SOAP-based service provides a configuration API that allows you to specify a variety of network, RFID, edgware application, and system settings via XML-encoded messages.

Follow the next procedure to enable the web service or to download the Device Configuration web service description language (WSDL) document.

For more information on the Device Configuration web service, see the *Device Configuration Web Service Command Reference Manual* (P/N 937-012-xxx).

To enable the web service and download the WSDL document

- 1 From the menu, click **Network Configuration > Device Management**. The Device Management screen appears.



By default, Device Configuration web services are enabled for either secure or insecure connections.

- 2 To disable web services over a secure connection, uncheck the **Enable Device Web Services (Secure)** check box, and then click **Activate Changes**.

To disable web services over an insecure connection, uncheck the **Enable Device Web Services (Insecure)** check box, and then click **Activate Changes**.

To download the device configuration WSDL document, click **DeviceConfiguration.wsdl**. The document opens in the browser window.

```
<?xml version="1.0" encoding="UTF-8" ?>
- <definitions name="DeviceConfiguration" targetNamespace="http://10.10.102.9:64907/DeviceConfiguration.wsdl"
  xmlns:tns="http://10.10.102.9:64907/DeviceConfiguration.wsdl" xmlns:SOAP-
  ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-
  ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:idws="
  xmlns:SOAP="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:MIME="http://schemas.xmlsoap.org/wsdl/mime/"
  xmlns:DIME="http://schemas.xmlsoap.org/ws/2002/04/dime/wsdl/"
  xmlns:WSDL="http://schemas.xmlsoap.org/wsdl/" xmlns="http://schemas.xmlsoap.org/wsdl/">
- <types>
- <schema targetNamespace="idws" xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:idws="idws"
  xmlns="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
  attributeFormDefault="unqualified">
  <import namespace="http://schemas.xmlsoap.org/soap/encoding/" />
- <simpleType name="ReadyToWorkState">
- <restriction base="xsd:string">
  <enumeration value="RTW-Error" />
  <!-- enum const = 0 -->
  <enumeration value="RTW-Warning" />
  <!-- enum const = 1 -->
  <enumeration value="RTW-Ready" />
  <!-- enum const = 2 -->
</restriction>
</simpleType>
- <simpleType name="RadioMode">
- <restriction base="xsd:string">
  <enumeration value="RadioMode-Unknown" />
  <!-- enum const = 0 -->
  <enumeration value="RadioMode-Auto" />
  <!-- enum const = 1 -->
```

You can copy and paste the document into an XML editing tool.

Using Simple Network Management Protocol (SNMP)

You can access and manage the IF61 from a Simple Management Network Protocol (SNMP) station. Contact your Intermec representative for a copy of the management information base (MIB).

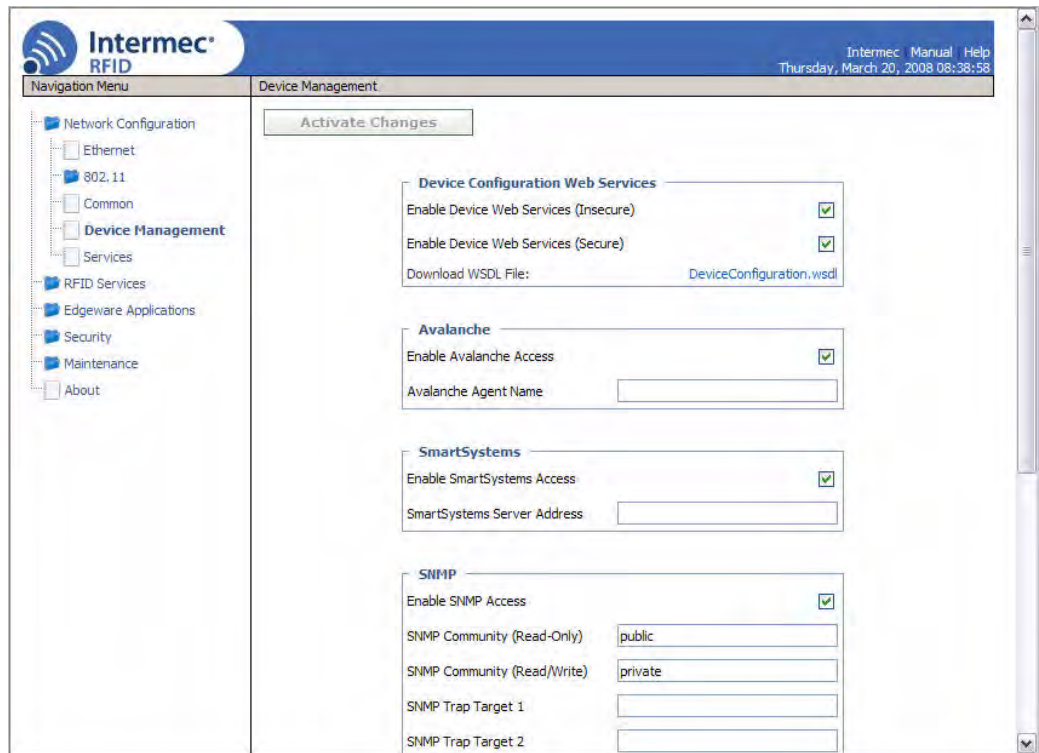
Before you can use an SNMP management station, you need to:

- enable SNMP access to the IF61. By default, SNMP access is enabled.
- define the IF61 SNMP community strings.

To enable SNMP access and define SNMP community strings

- 1 From the menu, click **Network Configuration > Device Management**. The Device Management screen appears.

Because SNMP access is enabled by default, the **Enable SNMP Access** check box is checked, and a list of configurable settings appears in the SNMP list.



- 2 Configure SNMP settings for your network. For help, see the next table.
- 3 Click **Activate Changes** to save your changes and immediately make the changes active.

SNMP Community Parameter Descriptions

Parameter	Description
Enable SNMP Access	Uncheck this check box to disable SNMP access to the IF61. SNMP access is enabled by default.
SNMP Community (Read-Only)	Password for read-only access. Range is 1 to 15 characters, case-sensitive. Default is <code>public</code> .
SNMP Community (Read/Write)	Password for read/write access. Range is 1 to 15 characters, case-sensitive. Default is <code>private</code> .
SNMP Trap Target 1	Authoritative name for trap target 1.

SNMP Community Parameter Descriptions (continued)

Parameter	Description
SNMP Trap Target 2	Authoritative name for trap target 2.
SNMPv3 Username (Read-Only)	User name for SNMPv3 read-only access. Default is <code>readonly</code> .
SNMPv3 Password (Read-Only)	Password for SNMPv3 read-only access. Default is <code>intermec</code> .
SNMPv3 Authentication Type (Read-Only)	Specifies the protocol for encrypted SNMPv3 messages. This must match a supported encryption protocol on the SNMP management station. Choose MD5 , SHA1 (default), or None .
SNMPv3 Privacy Type (Read-Only)	Specifies the protocol for read-only access to encrypted SNMPv3 messages. Must match a supported protocol on the SNMP management station. Choose DES , AES (128 bit) , or None . Default is AES (128 bit).
SNMPv3 Username (Read/Write)	User name for SNMPv3 read/write access. Default is <code>intermec</code> .
SNMPv3 Password (Read/Write)	Password for SNMPv3 read/write access. Default is <code>intermec</code> .
SNMPv3 Authentication Type (Read/Write)	Specifies the protocol for encrypted SNMPv3 messages. This must match a supported encryption protocol on the SNMP management station. Choose MD5 , SHA1 (default), or None .
SNMPv3 Privacy Type (Read/Write)	Specifies the protocol for read/write access to encrypted SNMPv3 messages. Must match a supported protocol on the SNMP management station. Choose DES , AES (128 bit) , or None . Default is AES (128 bit).

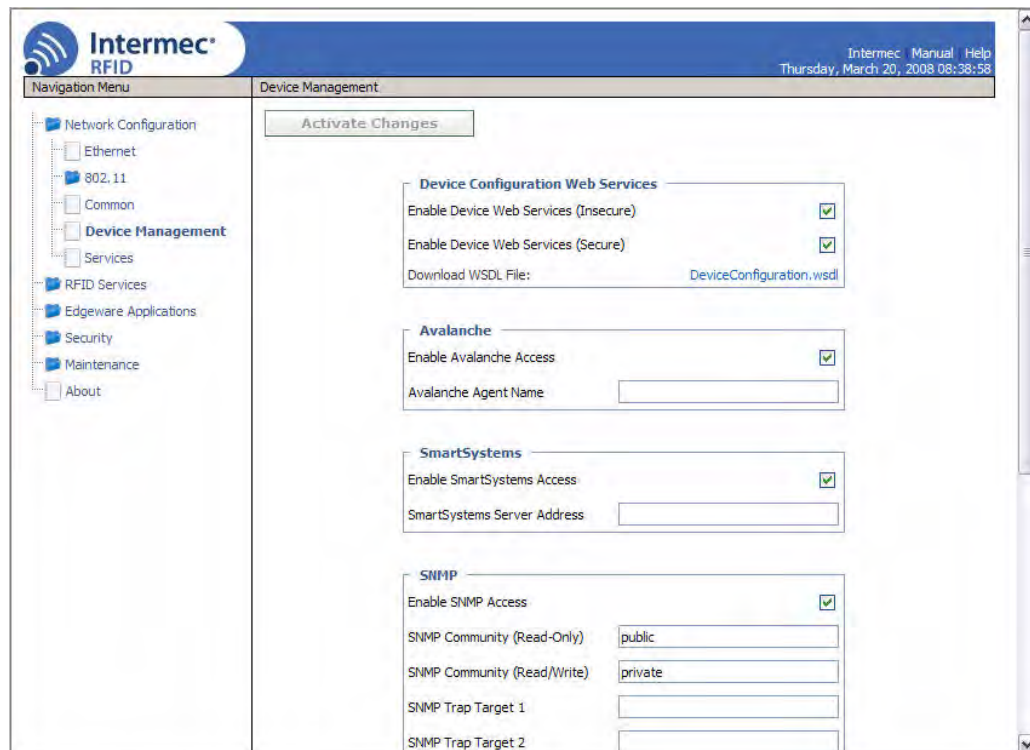
Using SmartSystems Foundation

The IF61 ships with a SmartSystems™ Client, which means you can manage it from a central host PC using Intermecc's SmartSystems Foundation. The SmartSystems Console displays all discovered SmartSystems devices in your network.

For more information on SmartSystems Foundation, go to www.intermec.com/SmartSystems. For information on using the SmartSystems Console, in the Console choose **SmartSystems > Help**.

To configure SmartSystems

- 1 From the menu, click **Network Configuration > Device Management**. The Device Management screen appears.



On the IF61, SmartSystems is enabled by default.

- 2 To automatically connect to the SmartSystems server at boot time, enter the server address in the **SmartSystems Server Address** entry field. After you specify the server address, SmartSystems will discover the IF61 during the next broadcast interval.

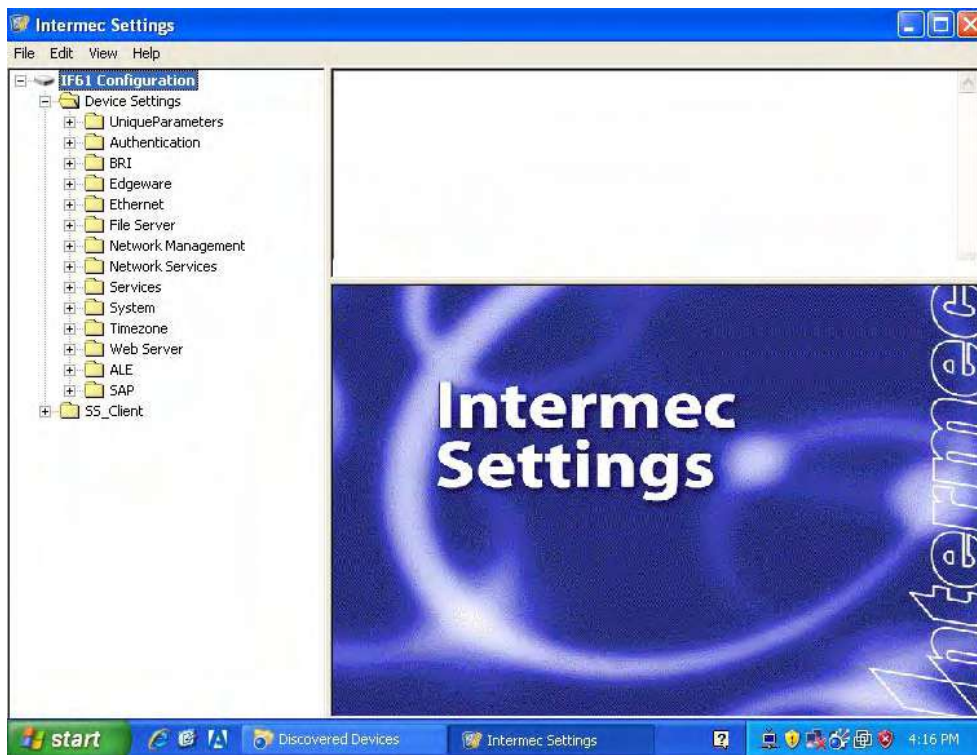
Chapter 4 — Managing, Troubleshooting, and Upgrading the IF61

To disable SmartSystems access to the IF61, uncheck the **Enable SmartSystems Access** check box.

- 3 Click **Activate Changes** to save your settings and immediately make them active.

Configuring the IF61 with Intermec Settings

In the Console, right-click an IF61 and choose **Intermec Settings** from the menu. The Intermec Settings window appears.



Intermec Settings: If you use the SmartSystems Console to manage the IF61, you can use Intermec Settings to configure the IF61.

For help with using Intermec Settings, in the Intermec Settings browser choose **Help > Online Manual**.

Using Wavelink Avalanche

The Wavelink Avalanche client management system uses three main components to help you easily manage your network.

Avalanche Component Descriptions

Component	Description
Enabler	Resides on all devices that can be managed by the Avalanche system. It communicates information about the device to the Avalanche Agent and manages software applications on the device.
Agent	Automatically detects and upgrades all devices in the Avalanche system and manages the daily processing functions.
Console	The administrative user interface that lets you configure and communicate with the Avalanche Agent. From the console, you can configure and monitor devices and build and install software packages and software collections.

The enabler is already installed on your IF61. Avalanche uses a hierarchical file system organized into software packages and software collections:

- Software packages are groups of files for an application that resides on the device.
- Software collections are logical groups of software packages.

For more information, see the Wavelink Avalanche documentation and online help, or visit the Wavelink web site at www.wavelink.com.

To use Avalanche to manage the IF61, you need to enable Avalanche as described in the next procedure.

To enable Avalanche

- 1 From the menu, click **Network Configuration > Device Management**. The Device Management screen appears.

The screenshot shows the Intermec RFID Device Management web interface. The navigation menu on the left includes Network Configuration, Ethernet, 802.11, Common, Device Management (selected), Services, RFID Services, Edgeware Applications, Security, Maintenance, and About. The main content area features an 'Activate Changes' button at the top. Below it are four configuration sections: 'Device Configuration Web Services' with 'Enable Device Web Services (Insecure)' and 'Enable Device Web Services (Secure)' checked, and a 'Download WSDL File' link; 'Avalanche' with 'Enable Avalanche Access' checked and an empty 'Avalanche Agent Name' field; 'SmartSystems' with 'Enable SmartSystems Access' checked and an empty 'SmartSystems Server Address' field; and 'SNMP' with 'Enable SNMP Access' checked, 'SNMP Community (Read-Only)' set to 'public', 'SNMP Community (Read/Write)' set to 'private', and two empty 'SNMP Trap Target' fields.

- 2 Check the **Enable Avalanche Access** check box to enable Avalanche.
- 3 In the **Avalanche Agent Name** entry field, enter the IP address or DNS name of the Avalanche console. Or, leave this field blank and the IF61 sends a broadcast request looking for any available agent.
- 4 Click **Activate Changes** to save your changes and immediately make the changes active.

Importing and Exporting Files

This section explains how to move files between the IF61 and your desktop PC.



Note: Do not use this procedure to copy RFID applications or firmware upgrades to the IF61.

- For help with upgrades, see [“Upgrading Firmware” on page 108](#).
- For help with installing applications, see [“Installing RFID Applications on the IF61” on page 59](#).

To move files between the IF61 and your desktop PC, you can:

- use the IF61 FTP server. For help, see the next section, “Using the IF61 FTP Server.”
- access the IF61 directories via Common Internet File System (CIFS) file sharing. For help, see [“Using CIFS File Sharing” on page 92](#).

For help with enabling CIFS, see [“Configuring Common Network Settings” on page 27](#).

- auto-mount a Network File System (NFS) share at boot time. For help, see [“Controlling Access Services” on page 30](#).

Using the IF61 FTP Server

You can move files to and from the IF61 by using its resident FTP server. The IF61 FTP server is disabled by default. To enable the FTP server, see [“Controlling Access Services” on page 30](#).

After you enable the IF61 FTP server, you can access the FTP directory directly through Internet Explorer. As with any Windows directory, you can click-and-drag or copy-and-paste to move files.

To access the IF61 via FTP

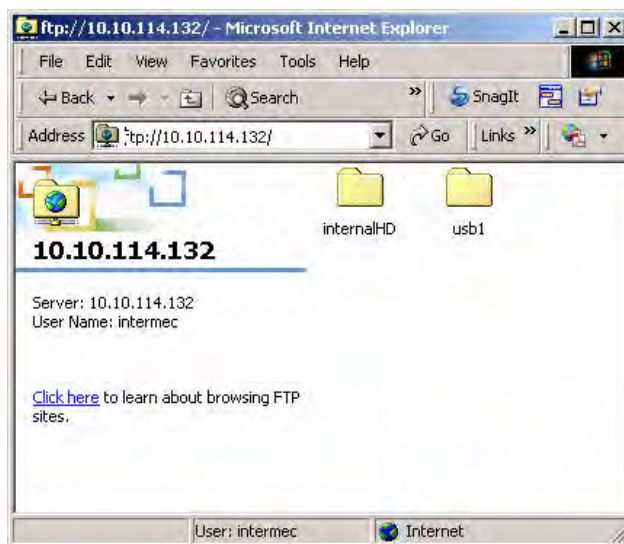
- 1 Open Internet Explorer.
- 2 In the **Address** field, enter this text:

```
ftp://xxx.xxx.xxx.xxx
```

where *xxx.xxx.xxx.xxx* is the IF61 IP address.

Chapter 4 — Managing, Troubleshooting, and Upgrading the IF61

- 3 Press **Enter**. The **Login As** dialog box appears.
- 4 Type your user name and password in the **User Name** and **Password** fields (default for both is `intermec`), and then click **Login**. The IF61 FTP directory appears.



Using CIFS File Sharing

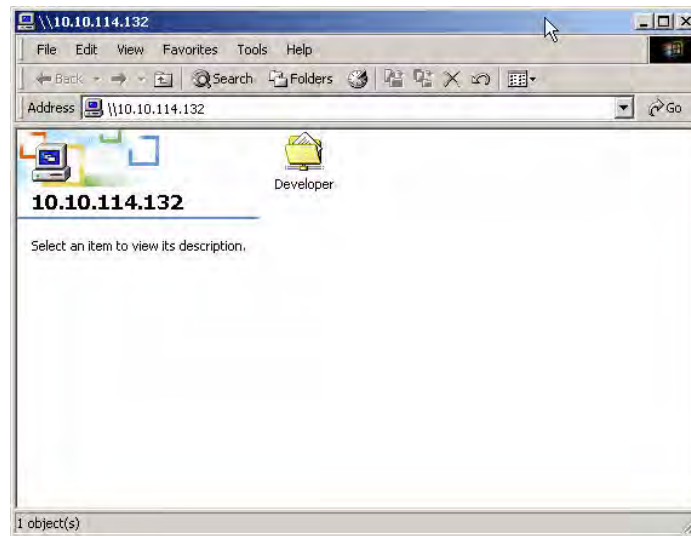
When you enable Common Internet File System (CIFS) file sharing on the IF61, you can use a file browser such as Windows Explorer to access IF61 directories and folders. The next procedure describes one way to use CIFS file sharing in a Windows environment.

To access the IF61 directories via CIFS file sharing

- 1 Enable CIFS file sharing on the IF61. For help, see [“Configuring Common Network Settings” on page 27](#).
- 2 On your desktop PC, choose **Start > Run**. The Run dialog box appears.
- 3 Enter the IP address of the IF61 (in the form `//xxx.xxx.xxx.xxx`) and press **OK**. A Windows Explorer screen appears showing the IF61 root directory.



Note: If a message box appears prompting you for a username and password, enter your user name and password in the entry fields and press **Enter**. The default user name and password is `intermec`.



You can also map a drive on your desktop PC to the IF61 via its IP address or hostname. For help, see the Windows documentation.

Accessing the IF61 via the Linux Shell



Note: This section is for advanced users who understand Linux command syntax.

There are three ways you can access the IF61 Linux shell:

- For the most secure access, you can open a Secure Shell (SSH) connection. For help, see the next section.
- You can open a Telnet session. For help, see [“Opening a Telnet Connection” on page 94](#).
- You can open a connection through a communications program such as HyperTerminal. For help, see [“Using a Communications Program” on page 95](#).

Opening a Secure Shell (SSH) Connection

You can open a Secure Shell (SSH) connection to the IF61 Linux shell. SSH connections require password authentication and offer a secure method for accessing the IF61.

By default, SSH connections to the IF61 are disabled. To enable SSH, see [“Controlling Access Services” on page 30](#).

Chapter 4 — Managing, Troubleshooting, and Upgrading the IF61

When you establish an SSH session with the IF61, you will be prompted to enter a login and password. These are the same as currently enabled for the web browser interface (default for both is `intermec`).

```
login as: intermec
intermec@10.10.111.84's password:
~ $ df
Filesystem          1k-blocks      Used Available Use% Mounted on
/dev/sda3            33024          33024      0 100% /
tmpfs                46640           0    46640   0% /dev
tmpfs                16384          196    16188   1% /tmp
tmpfs                46640           0    46640   0% /var/upgrade
/dev/sda1            7870           3466     4404  44% /mfg
/dev/sda2            7901           1079     6822  14% /nvram
/dev/sda4            30545          2502    28043   8% /home/developer
OSGI-RW              63569          35526    28043  56% /usr/equinox/bundles
~ $
```

SSH Connection Sample Screen: This illustration shows an SSH connection to the IF61 via a connection utility.

Opening a Telnet Connection

Follow the next procedure to open a Telnet connection to the IF61 for access via the Linux shell.

To open a Telnet session, you need to enable Telnet shell access to the IF61. For help, see [“Controlling Access Services” on page 30](#).



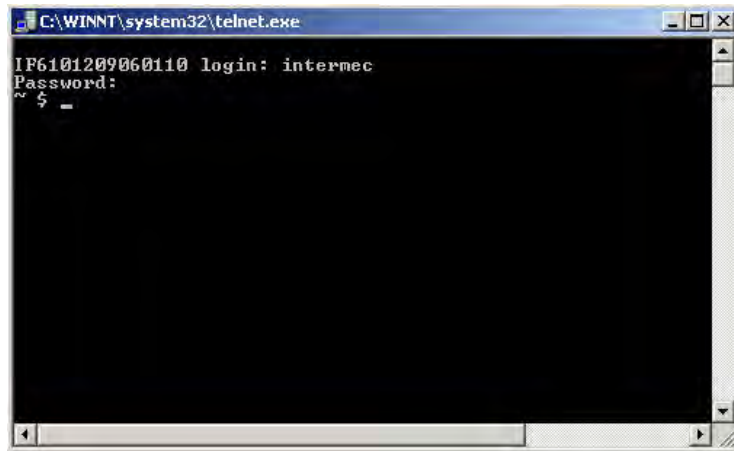
Note: Telnet sessions are unencrypted. Use an SSH session for more secure access to the IF61. For help, see the previous section, “Opening a Secure Shell (SSH) Connection.”

To open a Telnet connection

- 1 On your desktop PC, start Telnet.
- 2 In the Telnet window, type `open xxx.xxx.xxx.xxx`, where `xxx.xxx.xxx.xxx` is the IP address of the IF61.
- 3 Press **Enter**. The login prompt appears. The login and password are the same as currently enabled for the web browser interface (default is `intermec`).
- 4 Enter the login and press **Enter**. The password prompt appears.

Chapter 4 — Managing, Troubleshooting, and Upgrading the IF61

- 5 Enter the password and press **Enter**. The \$-prompt appears. Your Telnet session with the IF61 is established.



Using a Communications Program

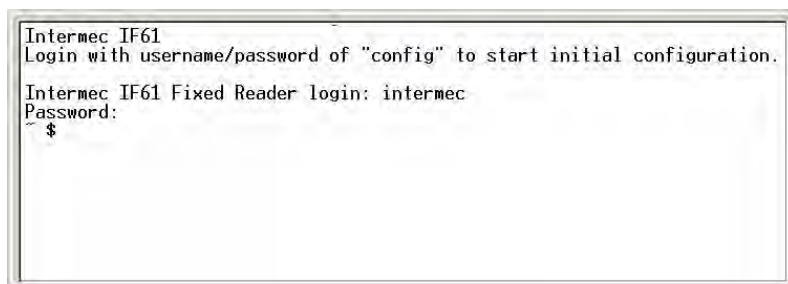


Note: For more secure access to the IF61, use a Secure Shell (SSH) connection. For help, see [“Opening a Secure Shell \(SSH\) Connection” on page 93](#).

To access the Linux shell via a communications program, you need a null-modem cable (P/N 059167).

To access the Linux shell through a communications program

- 1 Open a serial connection to the IF61 as described in the next section, “Opening a Serial Connection to the IF61.”
- 2 Type the login for the IF61 (default is `intermec`) and press **Enter**.
- 3 Type the password for the IF61 (default is `intermec`) and press **Enter**. The Linux \$-prompt appears.



You now have access to the IF61 Linux shell.

Opening a Serial Connection to the IF61

You can connect the IF61 to your desktop PC via the serial port to perform these tasks:

- assigning the IF61 an initial IP address.
- restoring default settings.
- accessing the Linux shell.

You need a null-modem cable (P/N 059167) and a communications program such as HyperTerminal.



Note: If you have Microsoft ActiveSync running on your desktop PC, disable ActiveSync to make the serial port available.

To connect to the IF61 via the serial port

- 1 Connect the null-modem cable from the serial port on the IF61 to a serial port on your PC.
- 2 Start the communications program and configure the serial port communications parameters to:

Bits per second	115200
Data bits	8
Parity	None
Stop bit	1
Flow control	None

- 3 Connect the IF61 to power. The IF61 boots as soon as you apply power. In a minute or two, the message “Loading System” appears as the IF61 initializes, and in another minute or two the login message appears.

```
Loading System...
Intermec IF61
Login with username/password of "config" to start initial configuration.
IF6101209060110 login:
```

Chapter 4 — Managing, Troubleshooting, and Upgrading the IF61

The serial connection is established. From here you can do these tasks:

- You can assign an initial IP address to the IF61 for configuration. For help, see [“Assigning an Initial IP Address” on page 9](#).
- You can restore default settings. This does not remove applications you have installed on the IF61. For help, see [“To restore defaults via a serial connection” on page 101](#).
- You can access the Linux shell. For help, see [“Accessing the IF61 via the Linux Shell” on page 93](#).

Maintaining the IF61

The Maintenance menu lets you view IF61 parameters and statistics, including a list of logged events. You may need this information if you need to call Intermec Product Support.

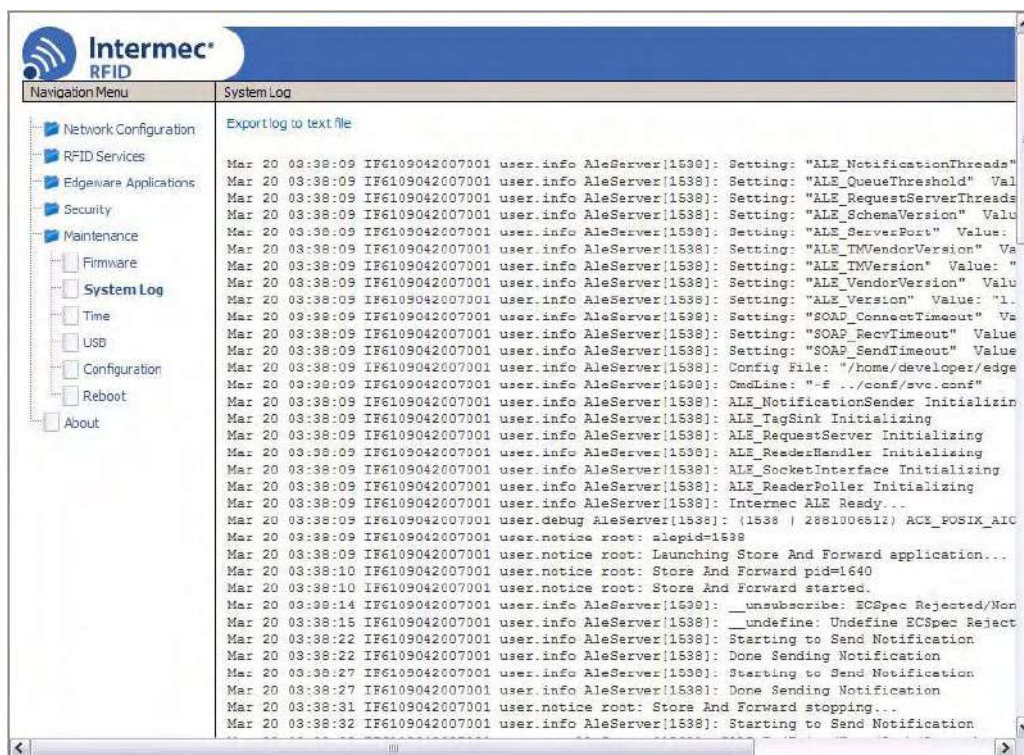
Viewing the System Log

The System Log screen shows events that have been logged by the IF61. These events are cleared when the IF61 loses power or is rebooted.

To view the System Log screen

- 1 From the menu, click **Maintenance > System Log**. The System Log screen appears. This screen is read-only.

Chapter 4 — Managing, Troubleshooting, and Upgrading the IF61



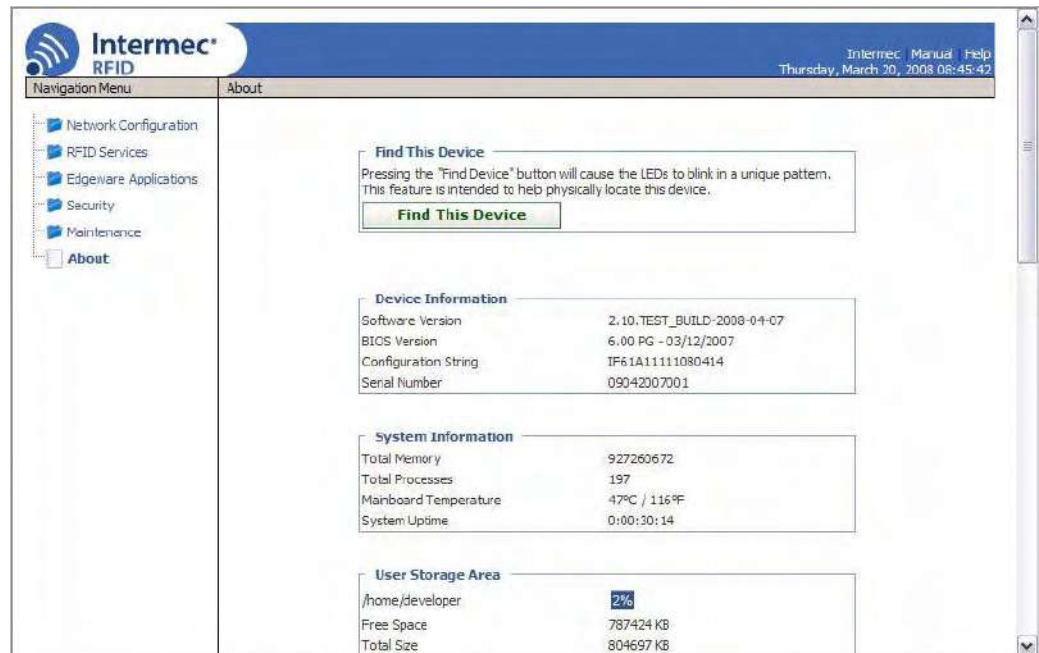
- 2 To save the list, click **Export log to text file**. The log is saved as Syslog.log and appears in the browser window.
- 3 Choose **File > Save As** and follow the prompts to save the log file to your desktop PC.

Viewing the About Screen

The About screen lists installed software versions, serial numbers, and other IF61-specific information.

To view the About screen

- From the menu, click **About**. The About screen appears. This screen is read-only.



The About screen includes:

- Device information: IF61 firmware version, hardware configuration string, and serial number.
- System information: Amount of memory used, available memory, number of running processes, main PC board temperature, and amount of time the IF61 has been running.
- User storage area information: Percentage of available storage space used, available space (in KB), and total storage space (in KB).
- RFID Module firmware: Bootloader and firmware versions.
- Network interface information, including MAC addresses.
- Installed subsystems: versions of all currently loaded IF61 subsystems, including Linux.

Using the LEDs to Locate the IF61

You can use the LEDs to help locate a specific IF61 in your location.

To locate an IF61

- In the About This IF61 RFID Reader screen, click **Find This Device**. The Intermec Ready-to-Work indicator and the Wireless LAN LED start flashing, and other available LEDs

turn on and stay on. Click **Finished Finding This Device** to turn off the LEDs.

Restoring the IF61 to the Default Configuration



Note: Restoring default settings as described in this section does not affect applications or security certificates you have installed.

There are two ways to restore the default configuration on the IF61:

- You can restore default settings from the web browser interface. For help, see the next section.
- You can restore default settings via a serial connection. For help, see [“To restore defaults via a serial connection” on page 101.](#)



Note: If you are communicating with the IF61 through your wireless network, do not attempt to restore defaults from the web browser interface or you will lose your wireless connectivity. The IF61 802.11 radio is disabled by default.

To restore defaults using the web browser

- 1 From the menu, click **Maintenance > Configuration**. The Configuration screen appears.



- 2 Click **Restore Defaults**. A confirming message appears.
- 3 Click **OK**. The IF61 reboots and the default configuration is restored.

Chapter 4 — Managing, Troubleshooting, and Upgrading the IF61

Or, click **Cancel** to close the confirming message without restoring defaults.

To restore defaults via a serial connection

- 1 Open a serial connection to the IF61. For help, see “[Opening a Serial Connection to the IF61](#)” on page 96.
- 2 In the login field, type `restore_defaults` and then press **Enter**.
- 3 In the Password field, type `restore_defaults` and then press **Enter**. The IF61 reboots and the default settings are restored.

Rebooting the IF61

You can reboot the IF61 from the web browser interface as described in the next procedure. For example, you may need to reboot the IF61 to enable changes in an application.

To reboot the IF61

- 1 From the menu, click **Maintenance > Reboot**. The Reboot screen appears.



- 2 Click **Reboot** to reboot the IF61. You need to log in again after the IF61 reboots.

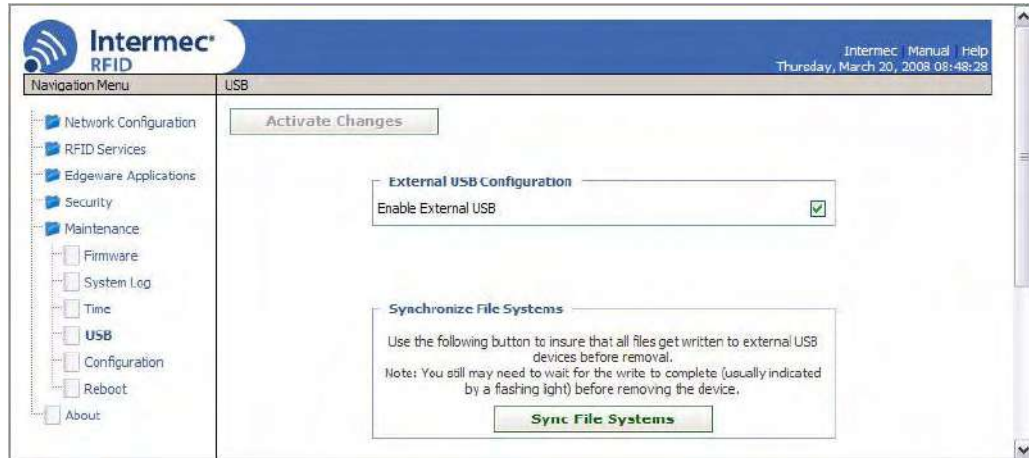
Managing USB Devices

You can connect USB devices such as flash drives or memory sticks to the IF61 USB ports. By default, the IF61 looks for USB devices installed in its USB ports and shows the devices in the local file system.

Chapter 4 — Managing, Troubleshooting, and Upgrading the IF61

To manage USB devices

- 1 From the menu, click **Maintenance > USB**. The USB screen appears.



The **Enable External USB** check box is checked by default. When external USB is enabled, the IF61 looks for upgrade files on USB devices and automatically loads the upgrade files if found. For more information, see [“Upgrading with a USB Drive” on page 112](#).

- 2 To disable automatic upgrades, uncheck the **Enable External USB** check box.

If you made changes to files in the `/home/developer/usb1` directory on the IF61, click **Sync File Systems** to copy the files to the USB device.

Troubleshooting the IF61

This section includes lists of problems and possible solutions.

Problems While Working With RFID

Many problems you may encounter when working with your RFID system can be solved by carefully checking the RFID settings and changing them accordingly. For help, see [“About RFID Services” on page 63](#).

RFID Problems and Solutions

Problem	Solution
The IF61 is unable to read RFID tags, or seems to read tags slowly or inconsistently.	<p>Check these conditions:</p> <ul style="list-style-type: none">• Your RFID antennas must be connected correctly to the IF61 and mounted in optimum locations. Make sure all antenna connections are tight and that the cables are in good condition. For help, contact your Intermec RFID system consultant.• For best performance, terminators should be installed on all unused RFID antenna ports. If you have operated the IF61 without terminators on all unused antenna ports, the RFID module may be damaged. For help, contact Intermec Product Support.• To maximize IF61 performance, make sure you have chosen the correct tag types for your application. For help, see “Configuring BRI Settings” on page 63.
The IF61 does not respond to your RFID application.	<p>Your application may not be communicating with the IF61 BRI server.</p> <p>You may need to change BRI server settings to communicate with your application. For example, if your application is running on a desktop PC, you need to enable external BRI connections to the IF61. For help, see “Configuring the BRI Server” on page 69.</p>

RFID Problems and Solutions (continued)

Problem	Solution
Your applications do not automatically start at boot time.	<p>Make sure your installation includes a configuration file with the command <code>AUTOSTART=true</code>. Or, use the web browser interface to configure the application to start at boot time.</p> <p>For help with configuration files, see “About Configuration Files” on page 56.</p> <p>For help with configuring applications to start at boot time, see “Auto-Starting Applications at Boot Time” on page 57.</p>

Connecting Directly to the RFID Module

If your application does not appear to be communicating with the IF61 RFID module, you can use a communications program to verify that the RFID module is working properly.

You need to know the IF61 IP address to connect directly to the RFID module. To verify that the RFID reader is reading tags, you need a known good RFID antenna and at least one good RFID tag.

To connect directly to the IF61 RFID module and verify operation

- 1 Make sure the RFID antenna is connected properly to the IF61.
- 2 Apply power to the IF61.
- 3 Use a communications program (such as HyperTerminal) to open a TCP/IP connection to the IF61 with these parameters:

IP Address IP address of the IF61

Port 2189

Configure the communications program to echo typed characters locally and to send line feeds with line ends.

- 4 Press **Enter**. The BRI prompt (OK>) appears.

If the prompt does not appear, there may be a problem with the RFID module or your connection to the module.

Chapter 4 — Managing, Troubleshooting, and Upgrading the IF61

- 5 Type `ATTRIB` and press **Enter**. A list of the current settings for the RFID module appears, indicating that the module is receiving commands.

```
OK>
FIELDSEP=" "
ANTS=1
FIELDSTRENGTH=30DB,30DB,30DB,30DB
TAGTYPE=EPCC1G2
TIMEOUTMODE=OFF
CHKSUM=OFF
NOTAGRPT=ON
IDREPORT=ON
SESSION=2
INITIALQ=4
INITTRIES=1
IDTRIES=1
ANTRIES=3
IDTIMEOUT=100
ANTTIMEOUT=50
RDTRIES=3
WRTRIES=3
LOCKTRIES=3
SELTRIES=1
UNSELTRIES=1
RPTTIMEOUT=0
OK>
```

If the list does not appear, there may be a problem with the RFID module.

- 6 (Optional) To verify that the RFID module is reading tags:
 - a Place a known good RFID tag within range of the antenna.
 - b Type `READ` and press **Enter**. The tag ID appears, indicating that the module is reading tags.

If the tag ID does not appear, there may be a problem with the RFID module or antenna system.

Problems With Connectivity

When troubleshooting problems with connectivity, make sure you know and understand these network-specific items:

- TCP/IP settings
- COM port settings for serial connections
- Wireless network settings, including the SSID, 802.1x security, user names, and passwords

You should also make sure all physical network connectors and cables are in good working order.

Connectivity Problems and Solutions

Problem	Solution
You cannot connect to the IF61 using the serial port.	<ol style="list-style-type: none">1 Verify that you are using a null-modem cable to connect to the desktop PC.2 Verify that you are communicating through the correct serial port (COM1).3 Verify that your PC is set to 115200, N, 8, 1, no flow control.
You cannot connect to the IF61 using a web browser.	<ol style="list-style-type: none">1 Verify that you have the correct IP address for the IF61.2 If you access the Internet through a proxy server, be sure you have added the IP address of the IF61 to the Exceptions list.
You cannot connect to the IF61 via Telnet.	Make sure that Telnet access is enabled on the IF61. For help, see “Controlling Access Services” on page 30 .
You cannot access the IF61 FTP directory.	Make sure that the IF61 FTP server is enabled. For help, see “Controlling Access Services” on page 30 .
You cannot load a security certificate.	You must use a secure web browser connection to load certificates. For help, see “Using the Web Browser Interface” on page 11 .
You cannot mount an NFS drive or a CIFS share.	Make sure that NFS mounting or CIFS/SMB shares are enabled on the IF61. For help, see “Controlling Access Services” on page 30 .
You have assigned a static IP address to the IF61 but cannot connect to the IF61 over your network.	Make sure that DHCP is disabled and that your TCP/IP parameters are set correctly. For help, see “Connecting to the IF61” on page 9 .
You cannot consistently maintain the 802.11 radio connection.	Make sure the 802.11 radio antennas are positioned for best performance with your wireless network.
You cannot connect to the IF61 through the 802.11 radio.	<ol style="list-style-type: none">1 Make sure the radio is enabled and that all 802.11 radio parameters are set correctly, including all necessary security parameters. For help, see “Configuring the 802.11 Radio” on page 23.2 Verify that the wired Ethernet and wireless 802.11 connections are on different subnets. Otherwise, errors may result.3 If you used the web browser interface to restore defaults, the 802.11 radio was disabled. You need to connect to the IF61 via a wired Ethernet connection to enable and configure the radio. For help, see “Configuring the 802.11 Radio” on page 23.

Calling Intermec Product Support

You may need to call Intermec Product Support if you have problems operating the IF61. Before calling, be sure you can answer the following questions:

- What kind of network are you using?
- What were you doing when the error occurred?
- What error message did you see?
- Can you reproduce the problem?
- What versions of IF61 and RFID software are you using? For help, see “[Viewing the About Screen](#)” on page 98.

When you have gathered this information, call Intermec Product Support at 1-800-755-5505.

Accessing Intermec Web Pages

Periodically, IF61 firmware and edgeware application updates can be downloaded from www.intermec.com.

You can use the IF61 web browser interface to visit www.intermec.com or to download manuals from Intermec as described next.

To access Intermec web pages

- 1 Open a web browser interface to the IF61. For help, see “[Using the Web Browser Interface](#)” on page 11.
- 2 To go to www.intermec.com, click **Intermec** in the upper right-hand corner.



- To locate IF61 firmware or edgeware updates, from the main Intermec web page choose **Support > Downloads** and search for IF61.

Or, to download an Intermec product manual, click **Manual** in the upper right-hand corner.



Follow the prompts to search for and download manuals or other documentation.

Upgrading Firmware



Make sure the IF61 is connected to a reliable AC power source before you upgrade the firmware. Do not cycle power to the IF61 during the upgrade. If AC power is lost during the upgrade, the IF61 may require factory repair.

This section explains how to configure and install firmware upgrades on the IF61.



Note: To upgrade the firmware, use only .bin files provided by Intermec. Be sure to contact your Intermec RFID system consultant before upgrading. To locate IF61 upgrades at www.intermec.com, see the previous section, “Accessing Intermec Web Pages.”

To upgrade the firmware

- 1 Download the Intermec IF61 OS Upgrade Package utility from the Intermec web site. For help, see the previous section, “Accessing Intermec Web Pages.”
- 2 Run the Upgrade Package utility to configure the firmware upgrade file. For help, see the next section.
- 3 Install and run the firmware upgrade file on the IF61. For help, see “[Installing the Firmware Upgrade](#)” on page 110.

Configuring the Firmware Upgrade

The Upgrade Package installer configures IF61 firmware upgrades. The configuration you need depends on the method you use to upgrade the IF61:

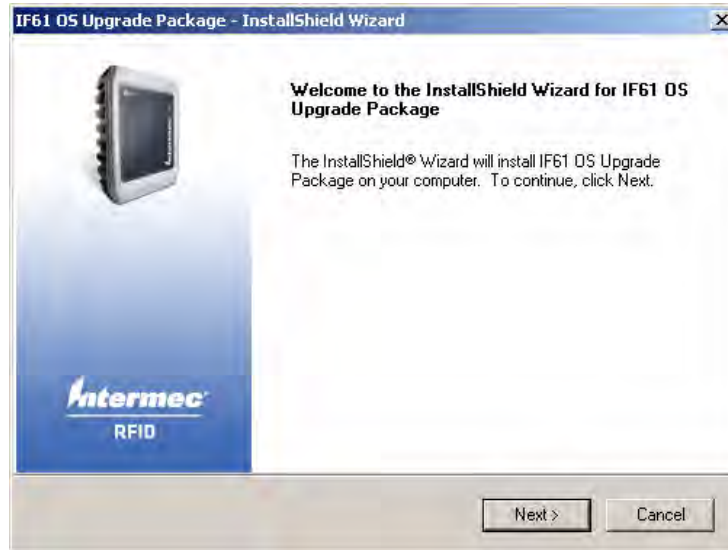
- via the web browser interface.
- by inserting a USB flash drive into one of the IF61 USB ports.
- using Intermec SmartSystems Server.
- using Wavelink Avalanche.

This section explains how to choose the correct configuration.

Chapter 4 — Managing, Troubleshooting, and Upgrading the IF61

To configure the firmware upgrade file

- 1 Double-click the Upgrade Package utility to run it. The opening screen appears.



- 2 Click **Next**. This screen appears:



Web Upgrade Bundle Only is selected by default.

- 3 If you are going to upgrade the IF61 via the web browser interface, by installing a USB drive in the IF61, or by using a Wavelink Avalanche Package, click **Next**. The bundle install location screen appears.

Chapter 4 — Managing, Troubleshooting, and Upgrading the IF61

If you are going to use Intermec SmartSystems Server to upgrade the IF61, click the **SmartSystems Upgrade Bundle** button and then click **Next**. The bundle install location screen appears.

- 4 Click **Next** to install the upgrade file at the default location, and then click **Install**. The upgrade file is installed.

To choose a different location:

- a Click **Browse** to browse to a different location.
 - b Double-click a folder to choose the location.
 - c Click **Next**.
 - d Click **Install**. The file is installed at the new location.
- 5 Click **Finish** to close the utility.

Installing the Firmware Upgrade

This section describes how to install and run the IF61 firmware upgrade.

Upgrading from the Web Browser Interface

- 1 From the menu, click **Maintenance > Firmware**. The Firmware screen appears.



- 2 Click **Browse** to browse to the location of the upgrade file, and then double-click the filename. The name of the file appears in the **Enter or select the name of the firmware upgrade file** entry field.

Chapter 4 — Managing, Troubleshooting, and Upgrading the IF61

- 3 Click **Upgrade IF61 RFID Fixed Reader**. The upgrade process begins and the firmware is transferred to the IF61. You see this screen:



During the upgrade, the web browser interface screen does not auto-refresh. Click **Refresh** in the web browser to check the progress of the upgrade. When the login screen appears, the upgrade is complete and the IF61 has already rebooted.

Upgrading with SmartSystems Server

You can use the SmartSystems Server to upgrade the firmware on the IF61. The server is part of SmartSystems Foundation, which is available from the Intermecc web site.

Before you can upgrade the IF61, you need:

- SmartSystems Foundation. For more information, go to www.intermec.com/SmartSystems.
- the IF61 upgrade file. For help, see “[Configuring the Firmware Upgrade](#)” on page 108.

To upgrade the IF61 using SmartSystems Server

- 1 Install SmartSystems Foundation on your PC and open the server.
- 2 Make sure the server and your IF61 are on the same subnet.
- 3 In the software vault, locate the IF61 upgrade to install.

- 4 Drag-and-drop the upgrade file onto the IF61 you want to upgrade. SmartSystems server tells you that it is installing the upgrade on the IF61.

The SmartSystems server shows the IF61 as being offline until the reader reboots and reconnects to the system.

Upgrading with a USB Drive



Note: To use this method, make sure the **Enable External USB** check box in the IF61 web browser interface is checked. For help, see [“Managing USB Devices” on page 101](#).

- 1 Follow the procedure for configuring the upgrade file. For help, see [“Configuring the Firmware Upgrade” on page 108](#).
- 2 Copy the upgrade file to a USB flash drive.
- 3 Insert the USB drive into one of the IF61 USB ports. If the IF61 is on, it automatically loads the upgrade file and begins the upgrade process. Otherwise the IF61 runs the upgrade the next time it boots.



Caution

Do not cycle power to the IF61 during the upgrade. If AC power is lost during the upgrade, the IF61 may require factory repair.

Upgrading with an Avalanche Package

After you configure the upgrade file, create an Avalanche software package using SmartSystems Software Bundles. For more information, see the Avalanche and SmartSystems documentation.



5 Using the IF61 GPIO Interfaces

This chapter explains how to access the IF61 general purpose input/output (GPIO) interfaces and how to connect industrial controls such as motion sensors or indicator lamps to the IF61.

About the GPIO Interfaces

The IF61 has four general purpose input and output (GPIO) interfaces. You connect external controls such as motion sensors or indicator lamps to the GPIO interfaces, which can then trigger IF61 operations.

Each interface is electrically isolated from the IF61 and designed for low voltage DC loads. The IF61 can also supply 12VDC at 0.5A to external devices.

How the inputs and outputs are used depends on the RFID application software being used in the system. You need to coordinate input and output control wiring with the software developer.

Accessing the Interfaces

You can access the GPIO interfaces through the IF61 GPIO port. The port uses a standard 25-pin serial cable. For port pin assignments, see [“Port Pin Assignments” on page 124](#).

Intermec offers these GPIO accessories:

- The GPIO Terminal Block (P/N 203-726-xxx). Use this accessory to connect devices to the IF61 GPIO interfaces. The block provides access to the IF61 GPIO interfaces via standard screw terminals.
- The Light Stack Kit (P/N 203-858-xxx). This 3-color indicator light and beeper connects directly to the IF61 GPIO port and is triggered by the output interfaces. The kit includes a connecting cable.
- The Sensor Kit (P/N 203-859-xxx). This motion sensor connects directly to the IF61 GPIO port and triggers the input interfaces. The kit includes a mounting bracket and connecting cable.
- The Light Stack and Sensor Kit (P/N 203-860-xxx). This kit includes the light stack, a sensor with mounting bracket, and connecting cable.

For more information on these GPIO accessories, contact your local Intermec distributor.

Using the Input Interfaces

Each of the four inputs is compatible with input signals of 10 to 36 VDC. Both the high and low signal contacts are exposed and isolated to 1500V. Input impedance is 1.8K minimum.

GPIO Input Signal Descriptions

Signal	Description	Min.	Typical	Max.
V_{in} (High)	High input voltage	10V	24V	36V
V_{in} (Low)	Low input voltage	-1V	0V	1V

In a typical application, the IF61 senses input from an external control like a switch and then starts a tag read operation.

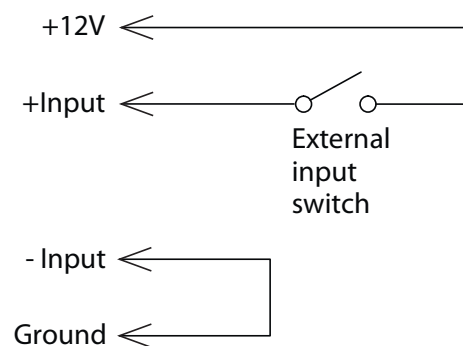
There are three basic ways to connect input controls to the IF61 input interfaces:

- Supply the input interface with power from the IF61.
- Isolate the IF61 from the input power source.
- Use an open collector solid state drive from a remote device to control the inputs.

For more information, see the next examples.

IF61 Powered Input

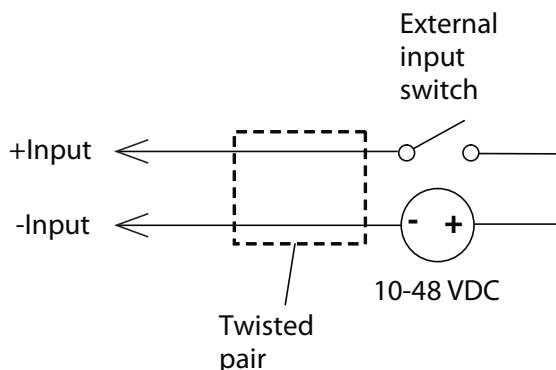
This is the simplest way to connect a control to an IF61 input interface. If the external control device is a switch, you can connect one side of the switch to an IF61 +Input pin, and the other side of the switch to one of the +12 VDC sources. Ground the corresponding -Input pin as shown in the next illustration.



IF61 Powered Input

Isolated Input Interface

Use this method to minimize noise induced by distance or grounding characteristics. The isolated input avoids induced noise by referencing a remote input to chassis return of the IF61. The next illustration shows how this method is wired.

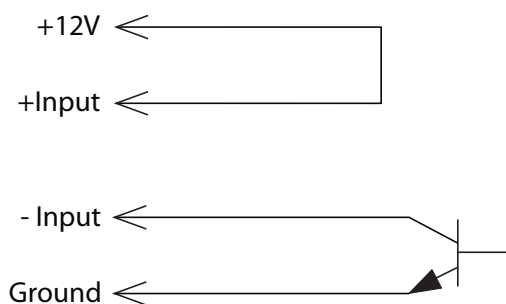


Isolated Input Interface

Open Collector Input Interface

The input can be connected to an open collector interface of an external device. This typically implies that the grounds are tied together for the two systems. The common ground can be a source of input noise, so you should follow good grounding practices for both the IF61 and the input device.

In this situation, the IF61 provides power to the pull-up resistor for the open collector. Connect the +Input pin to the +12 VDC source as shown in the next illustration.



Open Collector Input Interface

Using the Output Interfaces

Each IF61 output interface is optically isolated from the IF61, polarized, and rated for 5 to 48 VDC at 0.25A. All IF61 outputs include internal thermal fuses that trip if the load exceeds 0.25A, and the fuses are self-recovering once the excessive load is removed. The high and low contacts are exposed and isolated from ground. Transient suppression limits output voltage spikes to 65 VDC.

GPIO Output Specifications

Signal	Description	Min.	Typical	Max.
Leakage current (High)	Switch output, high leakage current	0 mA	1 mA	10 mA
V_{sat} (Low)	Switch output on, saturation voltage with 0.25A load	0V	1V	1.5V

Because the outputs are optically isolated, each one can be configured to switch the high side or the low side of the load. You can power the load directly from the IF61 or from an external power supply.

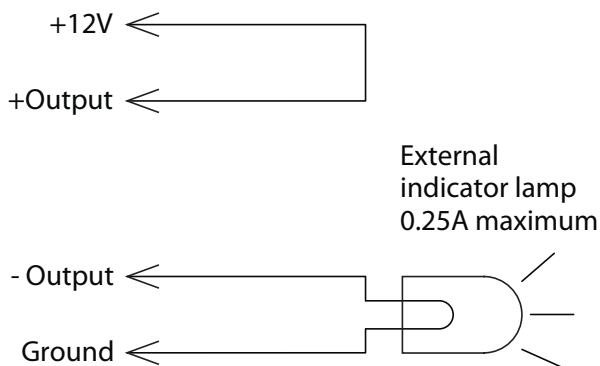
In a typical application, the outputs control indicator lamps that signal good reads or errors. The basic methods for connecting external devices to the GPIO outputs include:

- Switching the high side, with the load powered by the IF61
- Switching the low side, with the load powered by the IF61
- Switching the high side, with the load powered externally
- Driving a DC relay that controls an AC load

These methods are shown in the next examples.

Switching the High Side Using IF61 Power

In this example, an external indicator lamp (0.25A maximum current) is connected to the -Output and Ground pins, and the corresponding +Output pin is connected to the +12 VDC source.

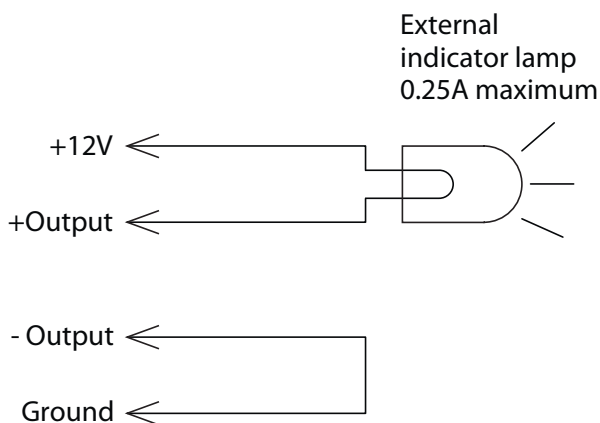


Switching the High Side

Switching the Low Side Using IF61 Power

For low side switching applications, the lamp power is routed to all the lamps in common and the low side of the load is routed to the switch.

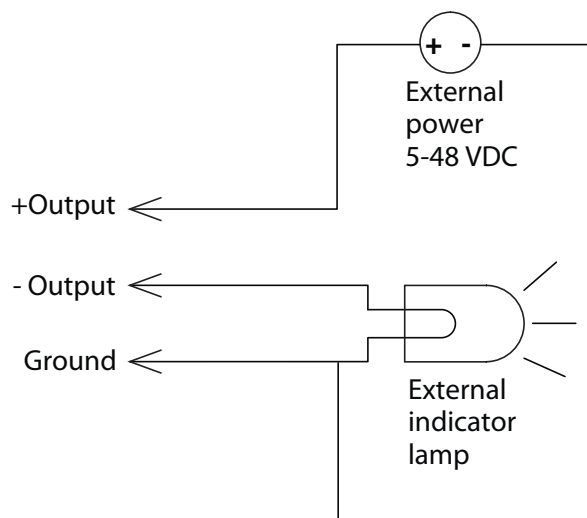
In this method, connect the external indicator lamp to the +Output and +12 VDC pins, and short the corresponding -Output pin to ground as shown.



Switching the Low Side of the Output Load

Switching the High Side Using External Power

To use external power (5 to 48 VDC) to switch the high side, connect the Ground pin to the ground system of the external power supply, and connect the positive side of the external supply to the +Output pin. The external indicator lamp is connected to the corresponding -Output and Ground pins as shown in the next illustration.

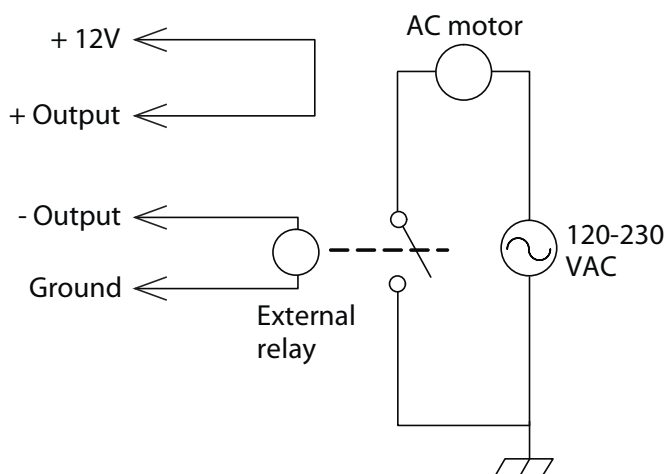


Switching the High Side With External Power

Driving a DC Relay to Control an AC Load

While the IF61 outputs are designed to switch DC loads, they can drive relays that control AC loads. The next illustration shows how to connect such a system to an IF61 output.

Chapter 5 — Using the IF61 GPIO Interfaces



Driving a DC Relay: The external relay provides dry contacts for controlling the AC motor.



Note: In many installations, the relay and AC wiring must be placed in an enclosure that meets local fire code regulations.

Using the Power Interface

The IF61 GPIO interface provides 12 VDC at 0.5A for powering external inputs and loads, eliminating the need for an external DC supply and simplifying the system installation.

The GPIO interface power has an internal thermal fuse that trips if the load exceeds 0.5A. The fuse is self-recovering once the excessive load is removed.

The total load on the GPIO interface power must stay within the 0.5A limit. When you design a system that uses the GPIO interface power, be sure to complete a power budget assessment to ensure that the supply is adequate for the system.

If your system needs more than +12 VDC at 0.5A, you can connect an external power supply to the +12V and Ground pins. The external supply powers the external loads, and that power will be available at all +12V pins on the GPIO port.



A Specifications

This appendix includes physical and electrical specifications for the IF61 and information about the port pin assignments.

IF61 Specifications

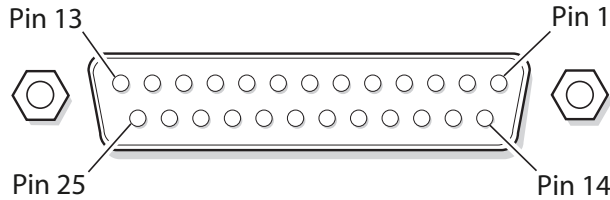
Height	10.7 cm (4.2 in)
Length	34 cm (13.2 in)
Width	23 cm (8.9 in)
Weight	2.6 kg (5.7 lb)
AC electrical rating	~ 100 to 240V, 1.0 to 0.5A, 50 to 60 Hz
Operating temperature	-20°C to +55°C (-4°F to +131°F)
Storage temperature	-30°C to +70°C (-22°F to +158°F)
Humidity (non-condensing)	10 to 90%
Ethernet interfaces	10BaseT/100BaseTx (twisted-pair)
Ethernet compatibility	Ethernet frame types and Ethernet addressing
Ethernet data rate	10 Mbps/100 Mbps
Serial port maximum data rate	115,200 bps
SNMP agent	RFC 1213 (MIB-2), RFC 1398 (dot3)
Linux version	2.6.18.1

RFID Specifications

Protocols Supported	EPCglobal Class 1 Gen 2 ISO 18000-6B Generation 1 ISO 18000-6B Generation 2 Phillips v1.19
Frequency Range	865-868 MHz, 869 MHz, or 915 MHz
Usable channels	1
Output power	
865-867 MHz, 915 MHz	Minimum: 28.5 dBm Typical: 29.5 dBm Maximum: 30.0 dBm
869 MHz	Minimum: 25.5 dBm Typical: 26.5 dBm Maximum: 27.0 dBm
Occupied frequency bandwidth	<250 KHz
Tag data rate	32 kbps/160 kbps
Dispatch rates	
Tag ID rate	70 tags per second
Tag data exchange rate	Reads a tag containing 8 bytes of data within 12 ms. Performs a verified write to a tag at an average rate of 31 ms per byte per tag.
Write range	Up to 70% of the read distance under similar conditions
Transmitter type	90% amplitude modulation index
Frequency stability	<±100 ppm from -25°C to +55°C (-13°F to 131°F)
Number of antennas	Up to 4, electronically switched
Antenna port isolation	22 dB
Antenna connectors	865-867 MHz: SMA 915 MHz: Reverse SMA

Port Pin Assignments

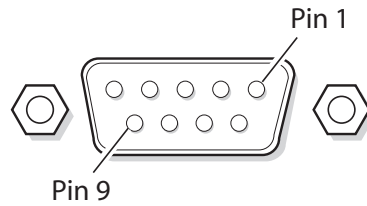
GPIO Port



GPIO Port Pin Assignments

Pin	Description	Active Polarity
1	-Input 1	Low-RTN
2	-Input 2	Low-RTN
3	-Input 3	Low-RTN
4	-Input 4	Low-RTN
5	Ground	
6	Ground	
7	+Output 1	High (10-48V)
8	Ground	
9	+Output 2	High (10-48V)
10	Ground	
11	+Output 3	High (10-48V)
12	Ground	
13	+Output 4	High (10-48V)
14	+Input 1	High (10-36V)
15	+Input 2	High (10-36V)
16	+Input 3	High (10-36V)
17	+Input 4	High (10-36V)
18	12VDC	
19	-Output 1	Low-RTN
20	12VDC	
21	-Output 2	Low-RTN
22	12VDC	
23	-Output 3	Low-RTN
24	12VDC	
25	-Output 4	Low-RTN

Serial Ports (COM1, COM2)



Serial Port Pin Assignments

Pin	Description	Active Polarity
1	NC	
2	Receive data (RXD)	High
3	Transmit data (TXD)	High
4	NC	
5	Signal ground	
6	NC	
7	NC	
8	NC	
9	NC	

Ethernet Port



Ethernet Port Pin Assignments

Pin	Description	Pin	Description
1	LAN_RX+	5	VDC_A
2	LAN_RX-	6	LAN_TX-
3	LAN_TX+	7	VDC_B
4	VDC_A	8	VDC_B



Note: The IF61 does not support power over Ethernet (POE).

Appendix A — Specifications



Index

Symbols

- .NET programming
 - delivering applications to IF61, 55
 - support, described, 57
- \$JAVA_HOME, described, 58
- \$JDBC_HOME, described, 58

Numerics

- 802.11 radio
 - a/b/g mode, selecting, 25
 - choosing network type, 25
 - configuring, 23
 - Enable Medium Reservation, 25
 - Network Mode list, 25
 - Security Level list, 25
 - security, configuring, 37
 - settings, described, 25

A

- About screen, 98
- AC power port
 - described, 5
 - location, 4
- Activate Changes button, 14
- ALE engine. *See* Application Level Events engine
- ALE Store and Forward edgware application, described, 61
- Antenna Timeout setting, 68
- Antenna Tries setting, 67
- ANTTIMEOUT equivalent, 68
- ANTTRIES equivalent, 67
- Application Level Events engine edgware, described, 61
- applications
 - .NET support, 57
 - auto-starting at boot time, 60
 - configuration files, described, 56
 - configuring BRI server, 69
 - delivering to IF61, 55
 - how to develop, 55
 - installing on IF61, 59
 - Java support, 57
 - Java, executing on IF61, 57
 - JavaScript support, 59
 - starting at boot time, 57
 - supported formats, 55
 - using with IF61, 54

- Automount CIFS/SMB check box, 29
- Automount NFS check box, 29
- auto-run file
 - configuring with Workbench, 77
 - JavaScript, at boot time, 77
- Auto-Start check box, for applications, 60
- AUTOSTART, in configuration file, 56
- auto-starting applications at boot time, 56, 60
- Avalanche. *See* Wavelink Avalanche

B

- Basic Reader Interface
 - attribute equivalents for BRI Attribute settings, 64
 - attributes, changing, 63
 - BRI Commands screen, in Developer Tools, 74
 - described, 63
 - external connections, enabling, 70
 - script files, loading and running with Developer Tools, 74
 - sending commands with Developer Tools, 73
 - TCP Port setting, for BRI server, 70
- blue LED, described, 7
- Bonjour service advertisement, enabling, 32
- booting the IF61
 - applications, starting at boot time, 57
 - auto-running JavaScript, 77
- bracket, mounting, described, 15
- BRI Commands screen, 74
- BRI server
 - BRI TCP Port, 70
 - configuring, 69
 - Enable External BRI Connections, 70
 - Enable Logging, 70
 - log, enabling and viewing, 70
 - logfile command event descriptions, 71
 - settings, described, 70
 - using with Intermec Ready-To-Work indicator, 7
- BRI TCP Port setting, for BRI server, 70
- BRI. *See* Basic Reader Interface

C

- cable access door, removing, 4
- cautions, described, xi
- CDC/Foundation profile, 57
- Certificate Details screen, illustrated, 50
- certificates
 - described, 49
 - installing and uninstalling, 50
 - viewing, 50
- changes, saving, 14
- CIFS. *See* Common Internet File System.
- CMDLINE, in configuration file, 56
- Common Internet File System
 - enabling service, 32
 - file sharing, 92
 - shares, enabling, 27, 29
- configuring the IF61
 - applications, starting at boot time, 57
 - BRI server, 69
 - connecting with communications program, 9
 - default configuration, restoring, 100
 - DHCP settings, 22
 - DNS settings, 27
 - Ethernet link speed, 9
 - Ethernet settings, 20
 - firmware, upgrading, 108
 - Intermec Settings, using, 88
 - IP address, 9
 - network settings, 20, 27
 - password server, 33
 - RFID services, 63
 - RFID settings, 63
 - saving changes, 14
 - security, 30
 - serial port connection, 96
 - setting IP address, described, 9
 - SNTP settings, 27
 - SYSLOG destination, 27
 - user name and password, setting, 33
 - using web browser interface, 11
 - viewing software versions, 98
 - web service, 82

- connecting IF61 to network, 16

D

- date and time
 - setting with web browser interface, 17
 - SNTP client settings, 27
- default configuration, restoring, 100
- default login, changing, 35
- defaults, restoring, 100
- Dense Reader Mode setting, 68
- Developer Tools, 73
 - Auto Start, 77
 - BRI Commands, 74
 - enabling, 60
 - GPIO, testing, 73
 - JavaScript files, working with, 76
 - Workbench, 76
- developing applications
 - .NET support, 57
 - access services, controlling, 30
 - auto-running JavaScript files at boot time, 77
 - guidelines, 55
 - Java support, 57
 - JavaScript support, 59
 - Mono support, 57
 - SQL server support, 58
 - starting at boot time, 57
 - testing with Developer Tools, 73
 - using with IF61, 54
 - with Intermec RFID Resource Kit, 54
- Device Configuration web service, 82
- DHCP settings, configuring, 22
- diagnostics
 - BRI server event log, viewing, 70
 - events log, viewing, 97
- Display Advanced Radio Parameters, 24
- DNS
 - server IP address, setting, 28
 - settings, configuring, 27
 - suffixes, setting, 28
- Dynamic WEP/802.1x security
 - enabling mixed cell use, 41
 - parameters, described, 41

Index

E

edgeware
 auto-starting at boot time, 60
 Developer Tools, described, 61
 enabling in web browser interface, 60
 updates, locating, 107
electrical specifications, 122
Enable 802.11 Radio check box, 25
Enable DHCP check box
 802.11 radio, 26
 Ethernet, 22
Enable External BRI Connections
 setting, 70
Enable External USB check box, 102
Enable FTP Server check box, 32
Enable Help check box, 14
Enable Logging check box, for BRI
 server, 70
Enable Medium Reservation check box, 25
Enable mixed cell check box
 dynamic WEP, 41
 static WEP, 39
Enable RADIUS check box, 35
Enable Serial Configuration check box, 36,
 37
Enable SSH Server check box, 32
Enable Telnet Server check box, 32
Enable Web Server check box, 32
environmental requirements, 16
EPCglobal Class 1 Gen 2
 certification, 2
 tags, choosing in BRI Attribute
 settings, 64
Ethernet
 IF61 in wired network, illustrated, 3
 link speed, configuring, 9
 port
 described, 5
 location, 4
 pin assignments, 125
 settings, configuring with web browser
 interface, 20
 troubleshooting problems, 105
 events log, viewing in Maintenance
 menu, 97
 exporting files, 91
 external controls, using with IF61, 114

F

Field Separator setting, 65
Field Strength setting, 68
fields, in tags, separating, 65
FIELDSEP equivalent, 65
FIELDSTRENGTH equivalent, 68
files, importing and exporting, 91
 using CIFS shares, 92
 using FTP, 91
firmware, upgrading, 108
 auto-loading from USB devices, 102
 Avalanche software package, 112
 installing upgrade file on IF61, 110
 overview, 108
 SmartSystems Server, 111
 upgrade file, configuring, 108
 web browser interface, 110
Forced Client Termination, 72
fragmentation threshold, 25
front panel ports
 accessing, 4
 described, 5
FTP server
 access, enabling or disabling, 30
 allowing access, 32
 default login and password, 32
 importing and exporting files, 91

G

general purpose input/output interfaces
 accessing, 114
 described, 114
 Developer Tools, testing with, 73
 inputs, using, 115
 isolated input, 116
 open collector input, 116
 output, switching high side using
 external power, 119
 output, switching the high side, 118
 output, switching the low side, 118
 outputs, using, 117
 port location, 4
 port pin assignments, 124
 power, using, 120
 powered input, 115
 relay, driving to control AC load, 119
 WRITEGPIO equivalents, 74

GPIO. *See* general purpose input/output interfaces

H

Help screen, illustrated, 14
 help text, in web browser interface, 14
 hostname, 28
 HyperTerminal, using to configure IF61, 9

I

ID Report check box, 65
 ID Timeout setting, 67
 ID Tries setting, 67
 IDREPORT equivalent, 65
 IDTIMEOUT equivalent, 67
 IDTRIES equivalent, 67
 IF61
 .NET support, 57
 applications, developing, 55
 applications, starting at boot time, 57
 connecting to network, 16
 connecting with communications program, 9
 default configuration, restoring, 100
 described, 2
 developer access, controlling, 30
 DHCP state, described, 9
 dimensions, 122
 environmental requirements, listed, 16
 Ethernet network, described and illustrated, 3
 files, importing and exporting, 91
 using FTP, 91
 via CIFS shares, 92
 firmware, upgrading, 108
 installing, 15
 IP address, setting, 9
 Java support, 57
 JavaScript support, 59
 locating with LEDs, 99
 maintaining, 97
 managing, 82
 mounting location, choosing, 15
 overview, 2
 rebooting via web browser interface, 101

related documents, list of, xiii
 RFID settings, configuring, 63
 SNMP, managing with, 84
 specifications, 122
 troubleshooting, 103
 using securely, 18
 importing files, 91
 indicator lamps, external
 testing with IF61, 73
 using with IF61, 114
 Initial Q setting, 67
 Initialization Tries setting, 67
 initialize tags setting, 67
 INITIALQ equivalent, 67
 INITTRIES equivalent, 67
 input interface
 isolated, 116
 open collector, 116
 powered, 115
 signal descriptions, 115
 Install User Application screen, 59
 installing
 applications, 59
 edgware, 62
 IF61, 15
 RFID antennas, 16
 Intermec
 Global Sales and Service, xi
 Knowledge Central, xi
 manuals, how to download from web, xiv, 107
 Product Support, what to know when calling, 107
 Settings, application, 88
 SmartSystems Foundation, 87
 IP address
 802.11 radio, 26
 Ethernet, 22
 setting with communications program, 9
 setting with web browser interface, 20
 IPv6 settings
 802.11 radio, 26
 Ethernet, 23
 ISO6B tags, choosing, 64

Index

J

- J2SE support, 57
- Java programming
 - \$JAVA_HOME, 58
 - \$JDBC_HOME, 58
 - delivering applications to IF61, 55
 - IF61 support, 57
 - jar files, running, 57
 - JIT compiler, enabling, 58
 - JVM name, 58
 - libraries, described, 57
 - running applications on IF61, 57
 - SQL server support, 58
- Java runtime executable on IF61,
 - described, 58
- JavaScript
 - files, testing with Workbench, 76
 - support, 59

L

- LBT Channel setting, 68
- LBT Scan Enable setting, 68
- LEDs
 - described, 6
 - Intermec Ready-To-Work Indicator, 6
 - location, 6
 - power, 6
 - RFID Transmit, 7
 - Tag ID, 7
 - using to locate the IF61, 99
 - wired LAN, 6
 - wireless, 6
- Link Local IP Address, 23
- Linux shell, accessing, 93
 - communications program, 95
 - secure interface, 93
 - Secure Shell (SSH) connection, 93
 - Telnet connection, 94
- Listen Before Talk algorithm,
 - described, 68
- LLRP. *See* Low-Level Reader Protocol
- location, choosing for IF61, 15
- Lock Tries setting, 65
- LOCKTRIES equivalent, 65
- login screen, 12
- login, changing default, 35
- Low-Level Reader Protocol, 71

- configuring settings, 71
- settings, described, 72

M

- maintaining the IF61, 97
- Maintenance menu, 97
 - events log, viewing, 97
 - locating the IF61, 99
 - using LEDs to locate the IF61, 99
- managing the IF61
 - defaults, restoring, 100
 - developer access, controlling, 30
 - Device Configuration web service, 82
 - firmware, upgrading, 108
 - methods, 82
 - security, configuring, 30
 - SmartSystems Foundation, 87
 - SNMP, 84
 - using securely, 18
 - Wavelink Avalanche, 89
- manuals, Intermec, how to download from
 - web, xiv, 107
- Mono, support for .NET applications, 57
- motion sensors, external
 - testing with IF61, 73
 - using with IF61, 114
- mounting bracket, 15
- mounting location, choosing, 15

N

- network
 - configuring settings, 20
 - connecting IF61 to, 16
 - IF61 illustrated in, 2
 - Network Mode, for 802.11 radio, 25
 - restrictions on choosing mode, 27
 - NFS volumes, enabling, 27, 29
 - No Tag Report check box, 66
 - NOTAGRPT equivalent, 66
 - NOTAGS message, enabling or
 - disabling, 66
 - notes, described, xi
- ### O
- OSGi support, 57
 - output interface
 - driving external DC relay, 119
 - high side switching, 118

- output interface (*continued*)
 - high side switching with external power, 119
 - low side switching, 118
 - signal descriptions, 117
- overview of the IF61, 2
- P**
- password settings, described, 36
- Password, setting on IF61, 36
- patent information, xiv
- Phillips 1.19 tags, choosing, 64
- pin assignments, for ports, 124
- port pin assignments
 - Ethernet, 125
 - GPIO, 124
 - serial, 125
- ports
 - AC power, 5
 - Ethernet, 5
 - front panel, accessing, 4
 - front panel, described, 5
 - GPIO, 5
 - pin assignments, 124
 - serial, 5
 - top panel, described, 8
- power interface, 120
- Power LED, 6
- power port, described, 5
- problems with IF61, solving, 103
- Product Support, calling Intermec, 107
- proxy server, using to access Internet, 11
- R**
- radio. *See* 802.11 radio
- RADIUS
 - authentication server, described, 33
 - enabling, 35
 - settings, described, 35
- RDTRIES equivalent, 65
- Read Tries setting, 65
- reader module, changing settings, 63
- reader-initiated connections, configuring for LLRP, 72
- Read-only Password setting, 36
- Ready-to-Work indicator, described, 7
- rebooting the IF61, 101
- Report Timeout setting, 66
- RFID
 - antenna port locations, 8
 - applications, using with IF61, 54
 - connecting directly to reader module, 104
 - Developer Tools, 73
 - edgeware, enabling, 60
 - IF61 settings, described, 64
 - Java support, 57
 - JavaScript support, 59
 - module, configuring, 63
 - Resource Kit, described, 54
 - specifications, 123
 - troubleshooting problems, 103
- RFID Transmit LED, 7
- Router entry field
 - 802.11 radio, 26
 - Ethernet, 22
- RUNAFTERINSTALL, in configuration file, 56
- running Java applications on IF61, 57
- S**
- safety information, xi
- SAP device controller edgeware, described, 61
- Secure Server Enable check box, 72
- secure shell access, enabling, 32
- secure web browser interface, using, 11
- securely using the IF61, 18
- security
 - access services, controlling, 30
 - certificates, described, 49
 - configuring, 30
 - default login, changing, 35
 - password server, using with IF61, 33
 - supported methods, 30
 - wireless network, configuring, 37
 - WPA Enterprise (802.1x), 43
 - WPA Personal (PSK), 41
 - WPA2 Enterprise (802.1x), 47
 - WPA2 Personal (PSK), 45
- Security Level, for 802.11 radio, 25
- Select Tries setting, 66
- SELTRIES equivalent, 66
- serial connection to IF61, 96

Index

- serial port
 - access, enabling for configuration, 36
 - connecting to IF61, 96
 - location, 4
 - pin assignments, 125
 - restoring defaults via serial
 - connection, 101
 - SESSION equivalent, 67
 - Session setting, 67
 - Simple Network Time Protocol (SNTP)
 - client settings, configuring, 27
 - SmartSystems Foundation, Intermec, using
 - to manage IF61, 87
 - SMB shares, enabling, 32
 - SNMP
 - Community settings, described, 85
 - parameters, described, 85
 - using to manage IF61, 84
 - SNMPv3
 - enabling, 84
 - settings, described, 85
 - SNTP client settings, configuring, 27
 - specifications
 - electrical and physical, 122
 - RFID, 123
 - SQL server, driver for IF61, 58
 - SSH (Secure Shell) connection, 93
 - SSID (Network Name) entry field, 25
 - Start button, for applications, 61
 - startup file
 - configuring JavaScript, 77
 - editing, 79
 - uploading from PC, 79
 - Static WEP security
 - enabling mixed cell use, 39
 - parameters, described, 39
 - Stop button, for applications, 61
 - Subnet Mask entry field
 - 802.11 radio, 26
 - Ethernet, 22
 - support, calling Intermec, 107
 - Sync File Systems button, 102
 - SYSLOG destination
 - configuring, 27
 - defined, 29
 - SYSLOG server, 29
- ## T
- Tag ID LED, 7
 - Tag Types setting, 64
 - tags, RFID
 - choosing Gen 2 type, 64
 - choosing ISO type, 64
 - ID reporting, enabling or disabling, 65
 - TAGTYPE equivalent, 64
 - TCP/IP settings, configuring, 20
 - Telnet
 - access, enabling or disabling, 30
 - accessing Linux shell, 94
 - allowing access, 32
 - connecting to the IF61, 94
 - default login and password, 32
 - time and date
 - setting with web browser interface, 17
 - SNTP client settings, 27
 - Time screen, 17
 - Timeout Configuration mode,
 - enabling, 66
 - TIMEOUTMODE equivalent, 66
 - top panel ports, described and illustrated, 8
 - troubleshooting the IF61, 103
 - connecting directly to RFID reader
 - module, 104
 - connectivity problems, 105
 - default configuration, restoring, 100
 - Intermec Product Support, calling, 107
 - Maintenance menu, viewing, 97
 - RFID problems, 103
 - turning off help text, 14
- ## U
- Uninstall button, for applications, 61
 - Universal Plug and Play
 - advertisement, enabling, 32
 - service, 31
 - Unsecure Server Enable check box, 72
 - Unselect Tries setting, 66
 - upgrade files, where to find, 108
 - Upgrade Package utility, 108
 - upgrading firmware, 108
 - USB devices, managing, 101
 - USB screen, illustrated, 102
 - User Storage Area list, 102
 - userapp.conf, 56

Username setting, for passwords, 36

W

warnings, described, xi

warranty information, xi

Wavelink Avalanche, using to manage IF61, 89

web browser interface, 11

802.11 radio, 23

applications, installing, 59

BRI server, changing settings, 69

date and time, setting, 17

Developer Tools, 73

DNS settings, 27

enabling, 32

help text, disabling, 14

IF61 default settings, restoring, 100

IP address, setting, 20

login screen, 12

Maintenance menu, 97

reader settings, 63

RFID edgeware, enabling, 60

secure, 12

secure only, enabling, 32

SNMP, enabling, 84

SNTP settings, 27

SYSLOG destination, 27

Wavelink Avalanche, enabling, 89

web service, configuring with, 82

WEP

dynamic, parameters described, 41

static, parameters described, 39

WEP keys, setting, 39

Wired LAN LED, 6

Wireless LAN LED, 6

wireless network

security, configuring, 37

settings, configuring, 23

settings, described, 25

See also 802.11 radio

Workbench, in Developer Tools

remote startup files, editing, 79

running a file at boot time, 77

WPA Enterprise (802.1x) security

configuring, 43

parameters, described, 45

WPA Personal (PSK) security

configuring, 41

parameters, described, 43

WPA2 Enterprise (802.1x) security

configuring, 47

parameters, described, 49

WPA2 Personal (PSK) security

configuring, 45

parameters, described, 47

Write Tries setting, 65

WRTRIES equivalent, 65

WSDL document, downloading, 82

www.intermec.com, accessing from IF61

web browser interface, 107

Index



Worldwide Headquarters

6001 36th Avenue West
Everett, Washington 98203
U.S.A.

tel 425.348.2600

fax 425.355.9551

www.intermec.com

IF61 Fixed Reader User's Manual



P/N 935-011-003