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

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 and click **Service & Support**. The Intermec Global Sales & Service page appears. From the **Service & Support** menu, move your pointer over **Support**, and 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 web site at www.intermec.com to download PDF versions of our current manuals. To order printed versions of the Intermec manuals, contact your local Intermec representative or distributor.

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.

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	• 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	• 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, from the Intermec web site, click **Contact**.

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.

Related Documents

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

Document Title	Part Number
IF61 Fixed Reader Quick Reference Guide	930-190-xxx
Basic Reader Interface Programmer's Reference Manual	937-000-xxx

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

To download documents

1. Visit the Intermec web site at www.intermec.com.
2. Click **Service & 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
- Configuring the IF61 (Setting the IP Address)
- Saving Configuration Changes
- 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).

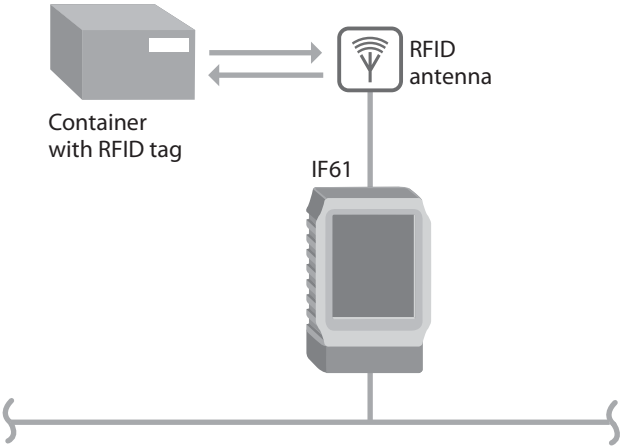
The IF61 Fixed Reader uses an EPCglobal Gen 2-certified IM5 Module (915 MHz RFID frequency band).

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 network as shown in the next illustration.

IF61 in a Wired Ethernet Network

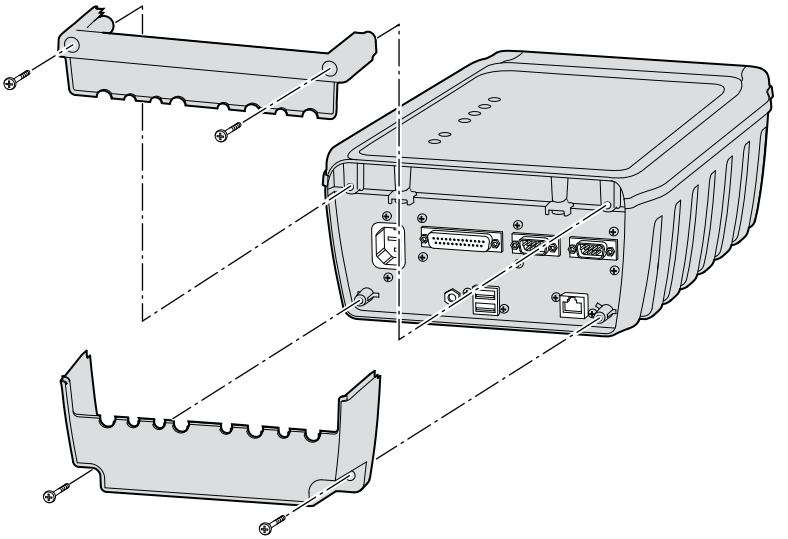


Understanding the Network and Power Ports

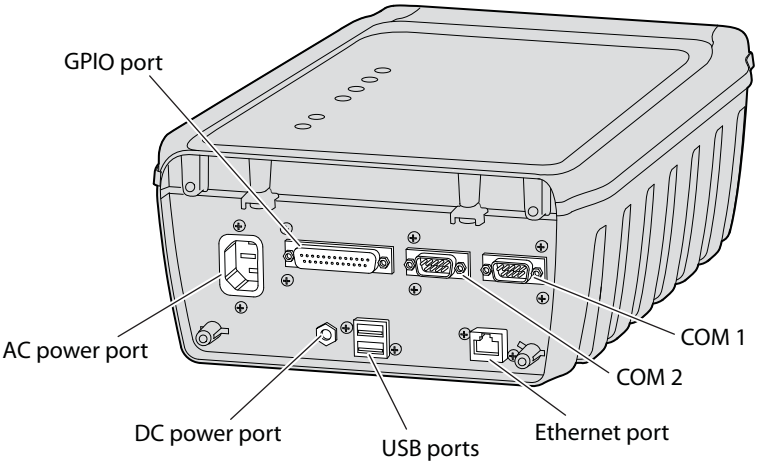
To access the IF61 network and power ports, you need to remove the cable cover.

To remove the cable cover

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



Removing the IF61 Cable Cover



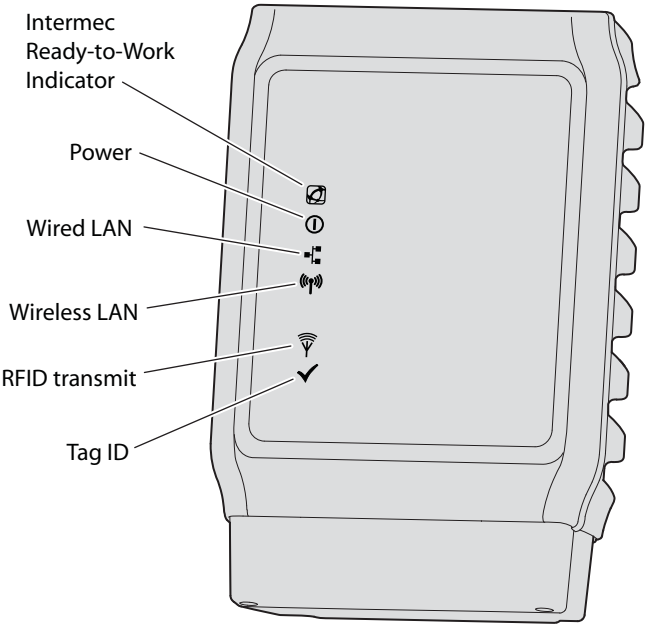
IF61 Port Descriptions

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 108.
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 93.
DC power	Not used.

For more information, see "Port Pin Assignments" on page 118.

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	Not used.

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.

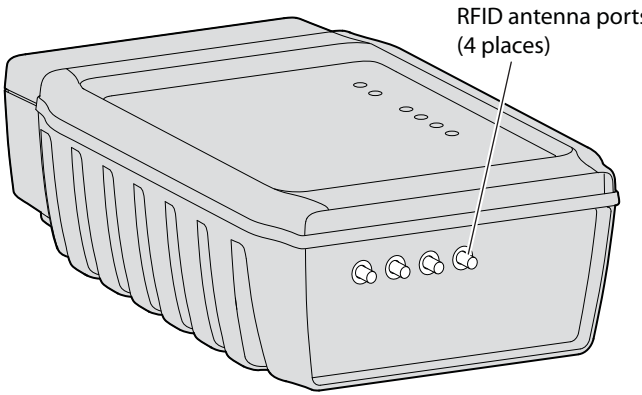
Ready-to-Work Indicator Status Descriptions

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 46.

For more information on the BRI server, see "Configuring the BRI Server" on page 58.

Understanding the Top Panel Ports

Connect RFID 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.

Configuring 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 10.

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, you 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 10.

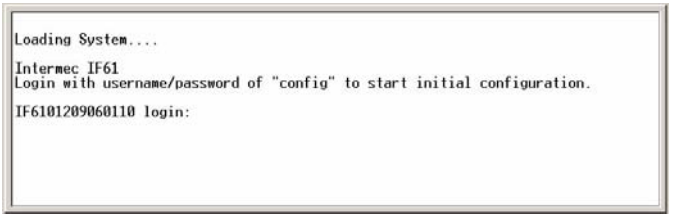
Assigning an Initial IP Address

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

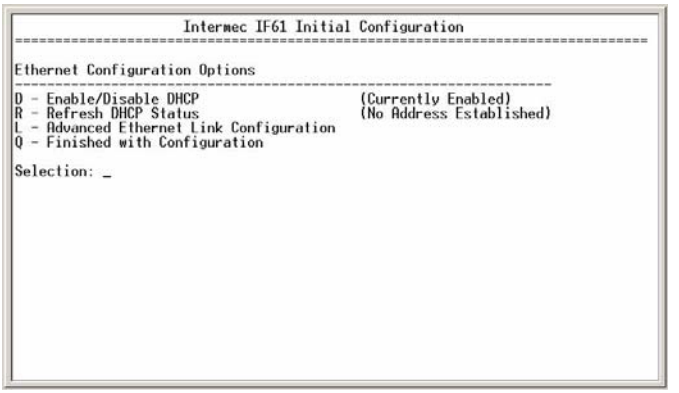
Note: If configuration via a serial connection has been disabled on the IF61, you need to restore default settings before you use this procedure. For more information, see "Using a Communications Program" on page 86.

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 87.

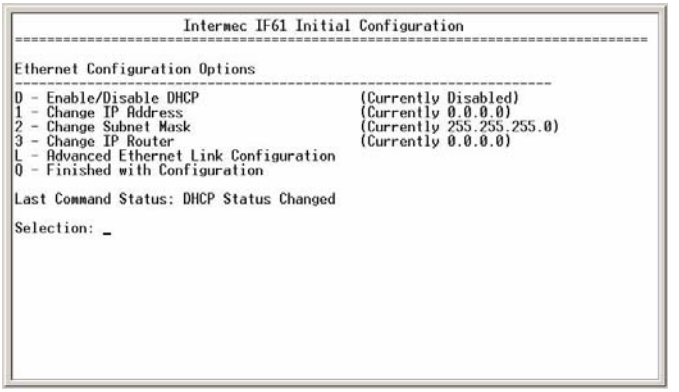


2 Type `config` and press **Enter**, and then type `config` again in the **Password** field and press **Enter**. The IF61 Initial Configuration screen appears.



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.



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. You can now continue to configure the IF61 through the web browser interface. For help, see "Using the Web Browser Interface" on page 10.

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 15.

Using the Web Browser Interface

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

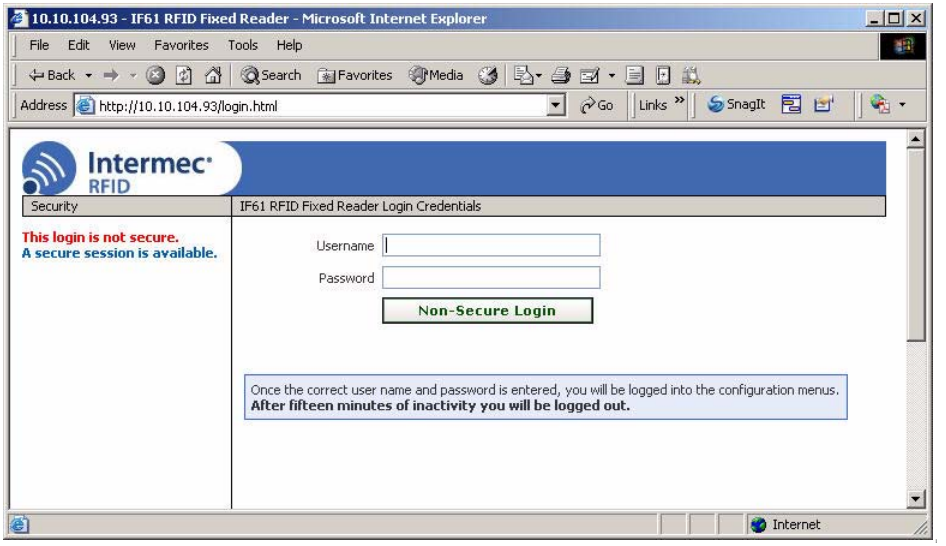
To use the web browser interface, the IF61 must be connected to your wired network. For help, see "Connecting the IF61 to Your Network" on page 15.

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.

To use the IF61 web browser interface

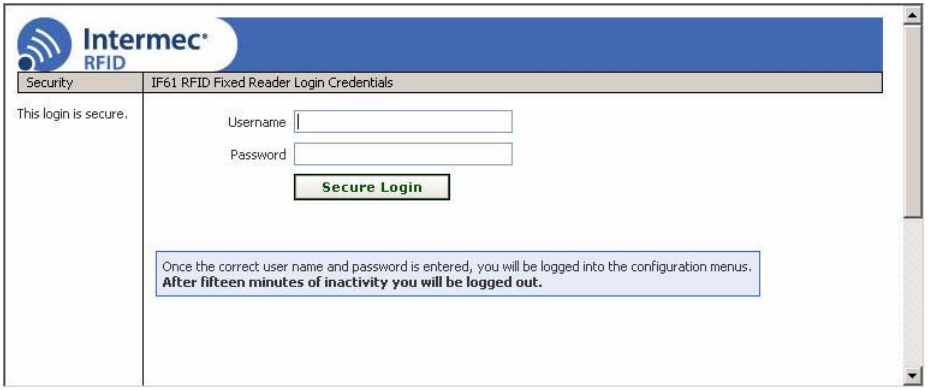
1. Determine the IP address of the IF61. If a DHCP server assigned the IP address, you need to get the IP address from that server.
2. Start the web browser.
3. In the browser address field, enter the IP address, and press **Enter**. The IF61 login screen appears.



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

Note: If a security alert message appears:

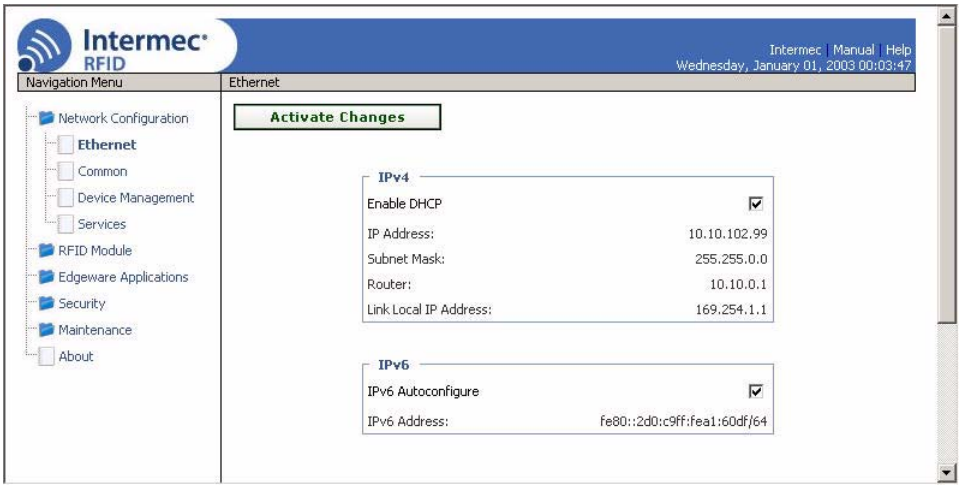
- Click **Yes** to continue to the secure login screen.
- Click **No** to cancel.
- Click **View certificate** to see the security certificate before continuing.



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 28.

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.

For help with configuring RFID reader settings, see "Configuring RFID Settings" on page 52.

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.

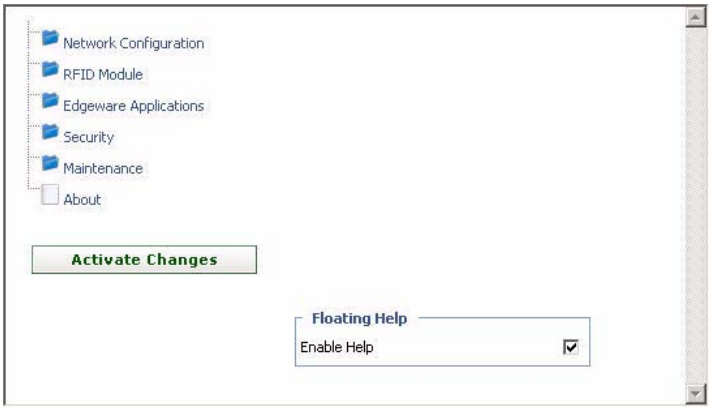
Disabling Help in the Web Browser Interface

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.

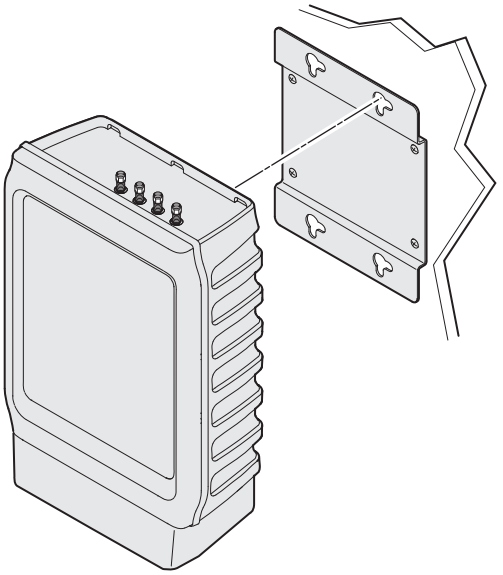
3 Click **Activate Changes** to save your changes and immediately make them active. The Help text is disabled.

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	-20ºC (-4ºF)	55ºC (131ºF)
Storage temperature	-30ºC (-22ºF)	70ºC (158ºF)
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 14.
2. Remove the cable cover. For help, see "Understanding the Network and Power Ports" on page 3.
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 7.

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. Connect the AC power cord to the power port on the IF61.

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

6. Install the bottom half of the cable cover and route the cables through the openings.
7. Install the top half of the cable cover. Make sure the cables are not caught in the seam.

8 Place the IF61 in its mounting location. For help, see "Choosing a Mounting Location" on page 14.

9 Connect the Ethernet cable to your network.

10 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 10.

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 10.

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 45.

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 10.
- limit developer access to the IF61 by enabling or disabling access services such as FTP, Telnet, or Common Internet File System (CIFS) shares. For help, see "Controlling Access Services" on page 26.
- configure and use network security methods, or disable basic configuration through the serial port. For help, see "Configuring Security" on page 25.

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 Ethernet Settings
- Configuring Common Network Settings
- Configuring Security
- About 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

To configure network settings on the IF61, you use the IF61 web browser interface. For help, see "Using the Web Browser Interface" on page 10.

You can also configure network settings by:

- using a communications program to access the IF61. If you choose this method, you can only configure basic network settings such as the IP address, subnet mask, and router. For help, see "Assigning an Initial IP Address" on page 8.
- using Intermec Settings from within the Intermec SmartSystems™ Console. For help, see "Using SmartSystems Foundation" on page 79.
- using the Wavelink Avalanche client management system to access the IF61. For help, see "Using Wavelink Avalanche" on page 80.

Configuring Ethernet Settings

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

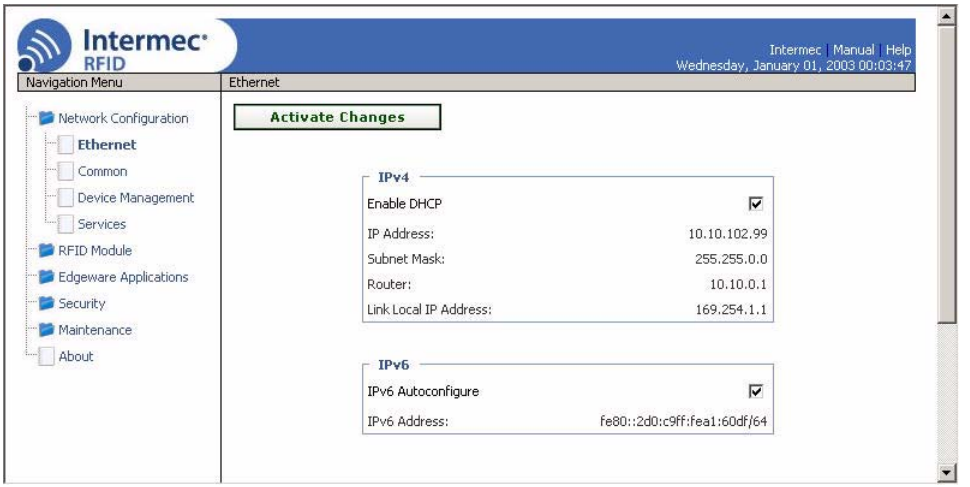
- DHCP mode
- IP address, subnet mask, and router (if DHCP is disabled or if you need to assign a static IP address)

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

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:



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

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.

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 23.

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

Ethernet Setting 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 Setting 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. Default is 169.254.1.1.
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 Common Network Settings

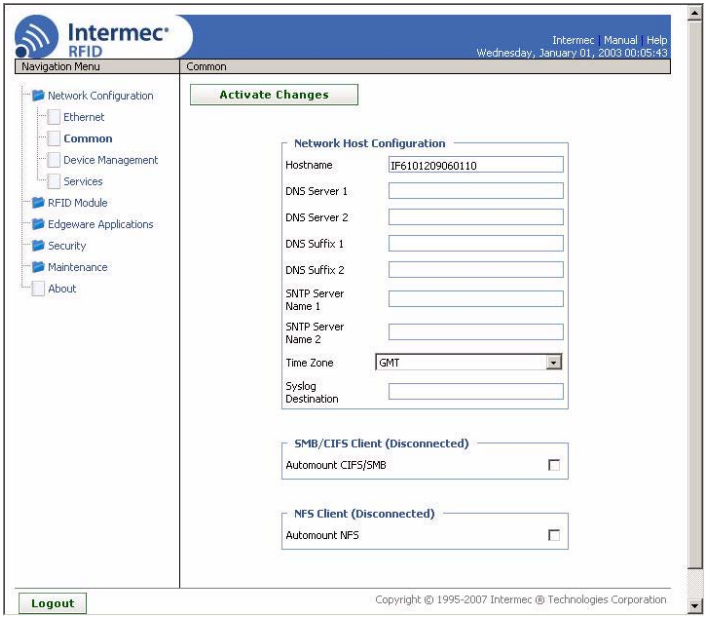
Common network settings are configuration items that apply to all network connections.

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.



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	Enter the IP address of a domain name server that the IF61 uses to resolve DNS names.
DNS Server 2	Enter the 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 16.
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: • 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: • 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:

- 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 28.
- 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 28.
- disable serial port access to the IF61. For help, see "Disabling Access Via the Serial Port" on page 32.

For general information on securely using the IF61, see "Using the IF61 Securely" on page 17.

Controlling Access Services

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

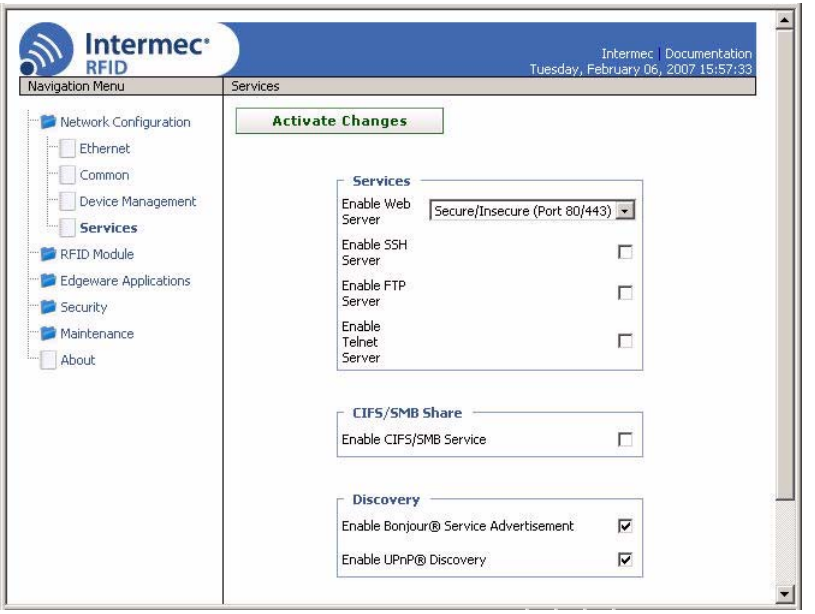
You can control how developers access the IF61 by enabling or disabling these services:

- 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	Enables access to the IF61 via the web browser interface. 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. Choose **Secure Only** to allow only the secure web interface through port 443. Choose **Disable** to disable web browser access. If you disable browser access to the IF61, you may need to access the IF61 via a communications program.
Enable SSH Server	Enables Secure Shell (SSH) access to the Linux system console using the same login and password as the web browser interface (default is `intermec`).

Developer Access Method Descriptions (continued)

Method	Description
Enable FTP Server	Enables access to the IF61 via its FTP server. For more information, see "Using the IF61 FTP Server" on page 82.
Allow Telnet Shell Access	Enables access to the Linux system console via standard Telnet, using the same login and password as the web browser interface. Default is `intermec`.
Enable CIFS/ SMB Service	Enables the Common Internet File System service, which creates a file sharing connection from a Windows PC to the /home/developer directory on the IF61. When you enable the CIFS/SMB service, entry fields for a username and password appear. Enter these settings and then click **Activate Changes**.
Enable Bonjour Service Advertisement	Enables the IF61 to advertise services and be discovered by Bonjour zero-configuration networking.
Enable UPnP Discovery	Enables the IF61 to be discovered by Universal Plug and Play protocols.

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."

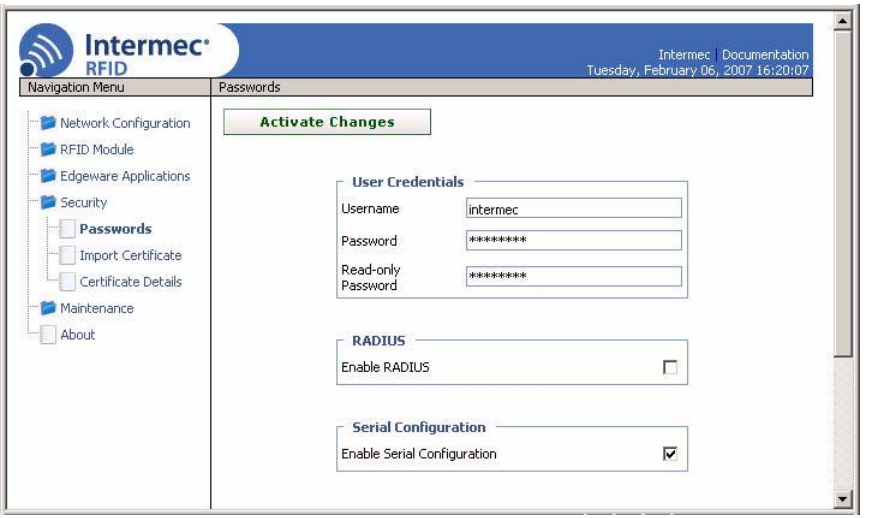
- If you do not want to use a password server, you should change the default login user name and password, and create a read-only password. For help, see "Changing the Default Login" on page 31.

Configuring the IF61 to Use a Password Server

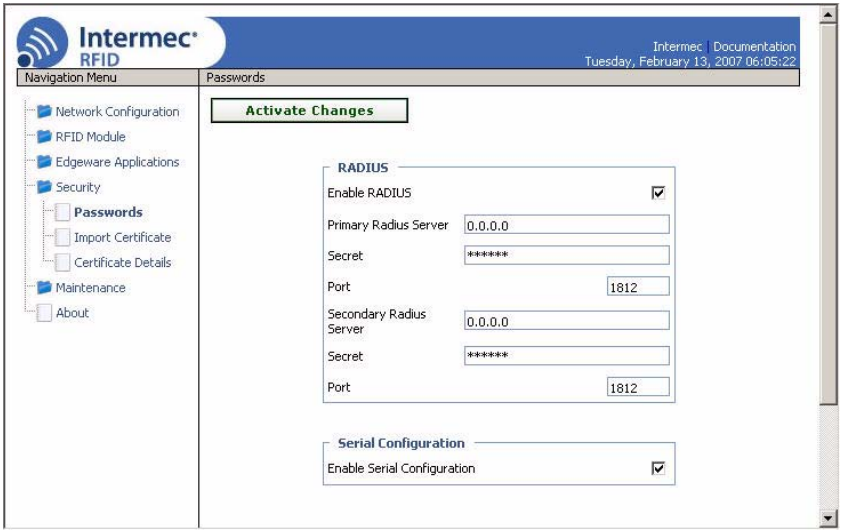
If you use a password server to manage users who log in to this IF61, you need to tell the IF61 how to communicate with the password server and then you need to configure the password server.

To configure the IF61 to use a password server

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



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



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

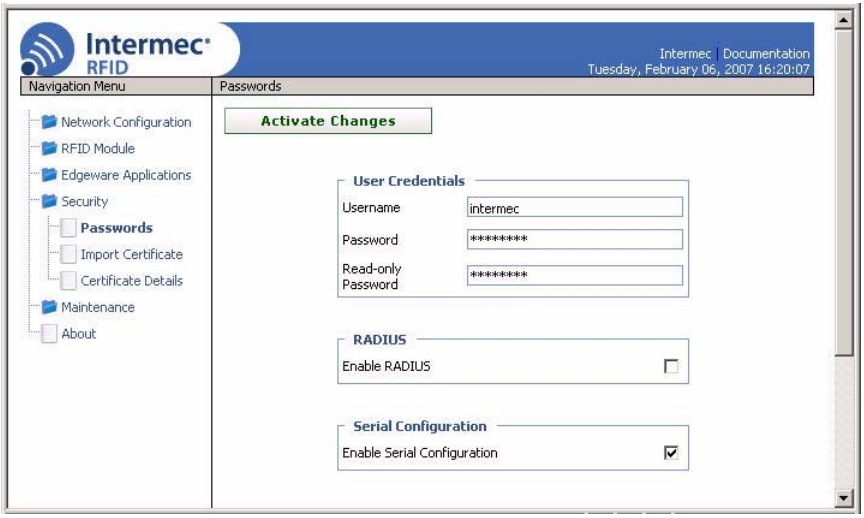
Type	Description
Enable RADIUS	Enables RADIUS authentication for this IF61.
Primary Radius Server	IP address or DNS name of the RADIUS server. If this field is blank, the RADIUS client does not use this entry.
Secret	Secret key for this RADIUS server.
Port	Port number of the primary RADIUS server. Default 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.



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

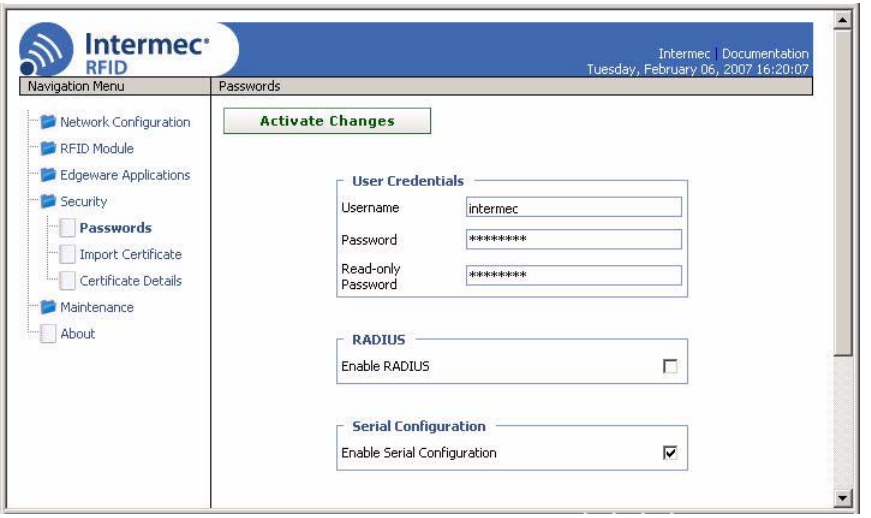
Parameter	Description
Username	Enter the user name you need to use to log in to this IF61. The user name can be from 1 to 32 characters long. You must always specify a user name. Default is “intermec”.
Password	Enter the password you need to use to log in to this IF61. This password gives you read and write access to the IF61 configuration. The password can be from 8 to 32 characters long. You must always specify a password. Default is “intermec”.
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 “intermec”. 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 25.

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 8. 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.

About 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.

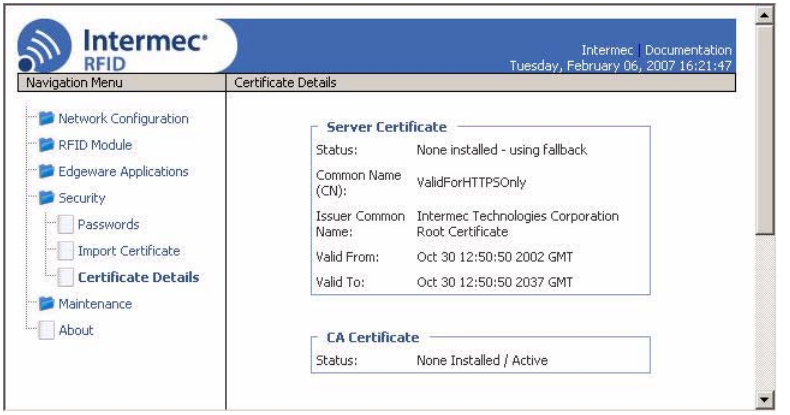
Note: To install or uninstall certificates, you need to access the IF61 via a secure web browser. For help, see "Using the Web Browser Interface" on page 10.

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.

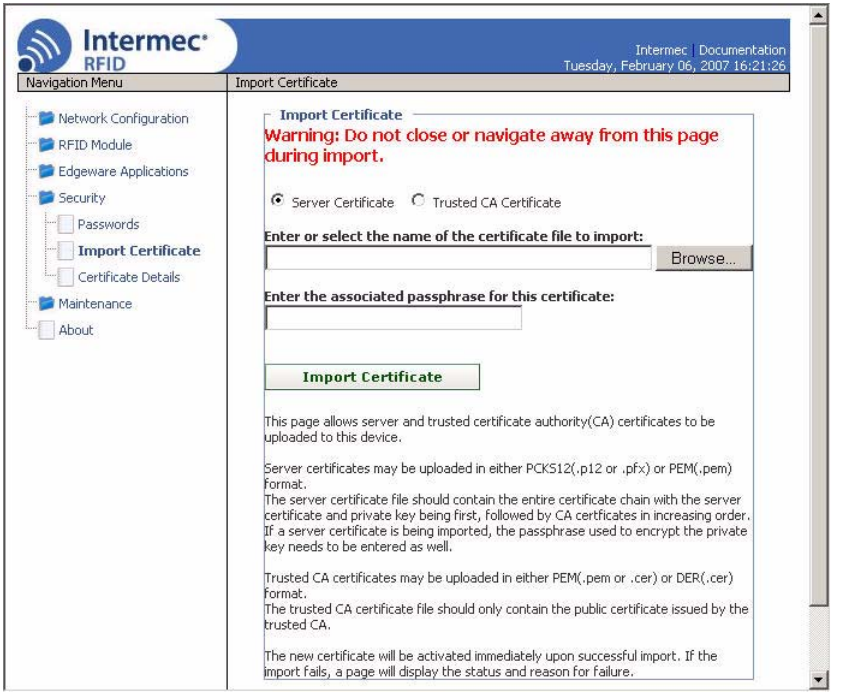
Installing and Uninstalling Certificates

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 10.

To install or uninstall certificates

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



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.

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
- Running Applications at Boot Time
- About IF61 Edgeware
- About the IF61 RFID Architecture
- Configuring RFID Settings
- Configuring the Data Collection Engine
- Using the Diagnostics Tool
- Using the JavaScript Tool

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

RFID Applications and the IF61

The IF61 supports Java and .NET applications. Your application communicates with the IF61 through the Basic Reader Interface (BRI) server, and controls the reader by issuing BRI commands.

- For more information on the BRI server, see "Configuring the BRI Server" on page 58.
- For more information on the BRI, see the *Basic Reader Interface Programmer's Reference Manual* (P/N 937-000-xxx).

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. Such an application is also known as edgeware, because the processing is done at the "edge" of the network.

Running your application as edgeware 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 39.

If your application uses the IF61 GPIO interfaces to control external devices such as indicator lamps, running the application as edgeware 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 .NET 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 IDL, go to www.intermec.com/idl.

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 "Configuring RFID Settings" on page 52.

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 45.

Delivering Applications to the IF61

For Java applications:

- Package your Java application (.tar, .tar/gz, or .tar/bz2 format only) and install the file and RFID Java libraries on the IF61 as described in "Installing RFID Applications on the IF61" on page 44. Be sure to specify the class path to the libraries.

  For help with executing Java applications, see "Executing Java Applications" on page 42.

For .NET applications:

- Create a .zip file that includes your application (.exe) and required DLLs, and install the .zip file on the IF61 as described in "Installing RFID Applications on the IF61" on page 44.

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 next 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 45.

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 "Configuring RFID Settings" on page 52.

`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.

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.

IF61 .NET Support

The IF61 supports applications based on .NET Framework 1.1. The IF61 uses Mono 1.2.3 to provide support for .NET applications deployed on the IF61 Linux operating system.

Note: The IF61 does not support ASP.NET or .NET 2.0.

IF61 Java Support

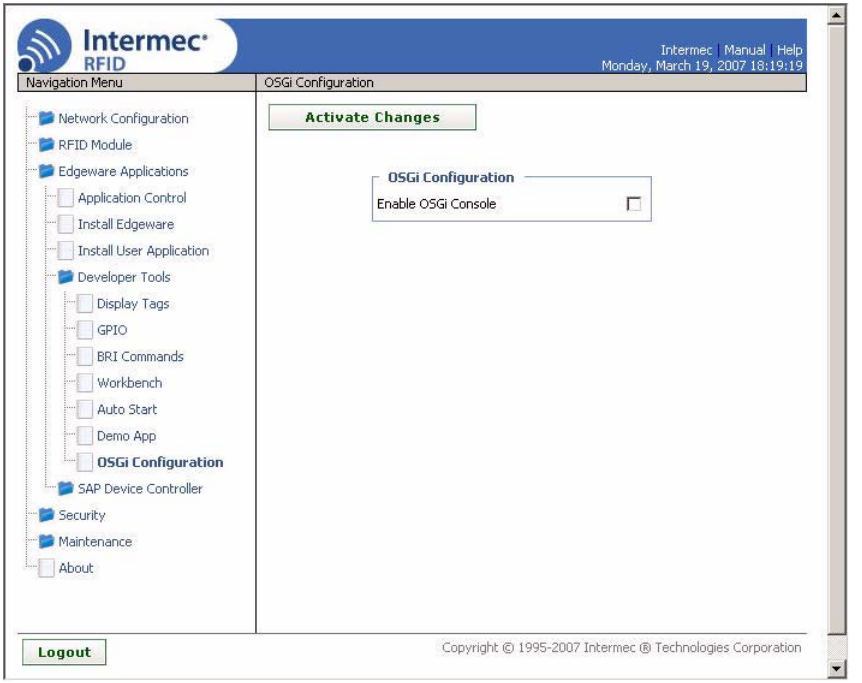
The IF61 comes with a JDBC driver you can use to create applications that write data directly from the IF61 to a remote database. For more information, see "Java Support for Microsoft SQL Server and Sybase" on page 43.

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.

The OSGi console is disabled by default. To enable the console, follow the next procedure.

To enable the OSGi console

1. From the menu, click **Developer Tools** > **OSGi Configuration**. The OSGi Configuration screen appears.



2 Check the Enable OSGi Console check box.

3 Click **Activate Changes**. The console is enabled.

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:

- 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 software or proof-of-concept applications as well as production RFID edgeware.

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 70.

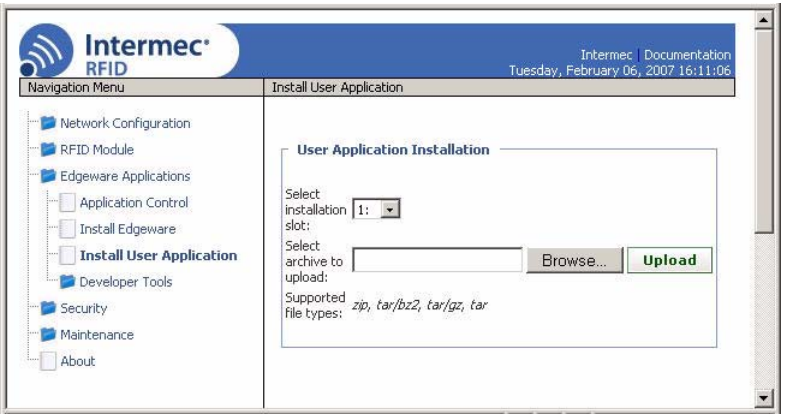
Installing RFID Applications on the IF61

The IF61 provides up to 160 MB of memory for your applications. Depending on the amount of memory each application uses, you can install up to 10 applications on the IF61. 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 applications on the IF61

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



2 Choose an installation slot from the drop-down list.

3 Click **Browse** and follow the prompts to navigate to the location of the application file.

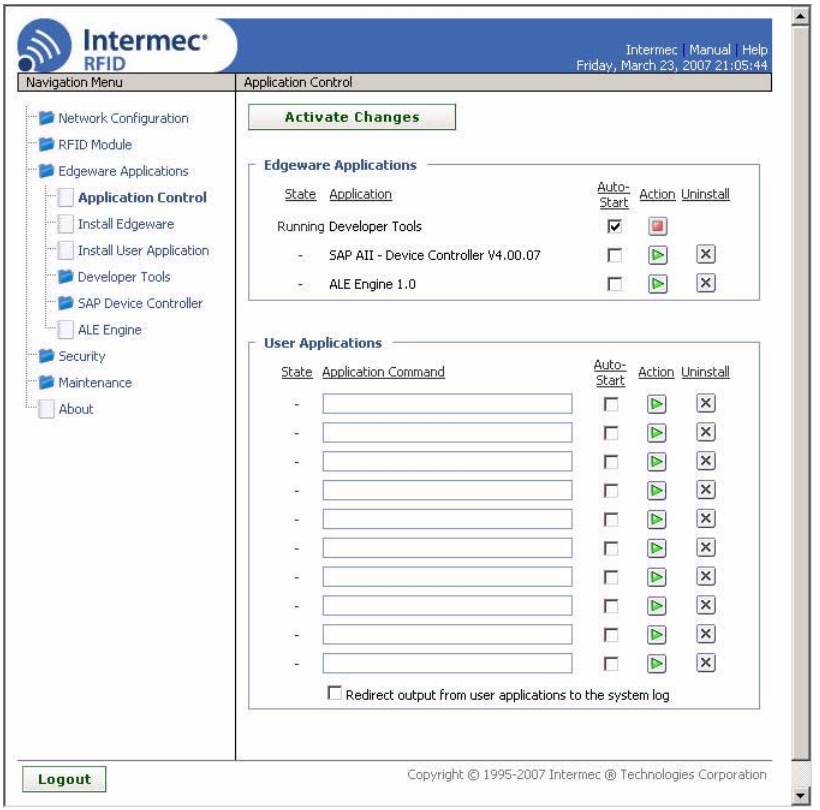
4 Click **Upload**. The application is uploaded to the IF61 in the installation slot you chose.

Managing Applications

To maximize IF61 resources, you can start, stop, or uninstall IF61 edgeware 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 **Edgeware Applications > Application Control**. The Application Control screen appears.



The Edgeware Applications section lists all installed edgeware. In this screen, you can:

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

2 Choose one of the options:

- 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.

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

About the IF61 Edgeware Applications

The IF61 includes these edgeware applications:

- The Developer Tools (enabled by default). Use the Developer Tools to test your RFID systems and settings. For more information, see "About the Developer Tools" on page 61.
- 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 Appendix B, "Configuring and Using the SAP Device Controller."
- 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 "About the IF61 ALE Engine" on page 48.

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.

You can uninstall the SAP device controller or the ALE Engine. For help, see the previous section, "Enabling or Disabling Applications."

Intermec may provide firmware upgrades for installed edgeware. For help with locating IF61 upgrades at www.intermec.com, see "Accessing Intermec Web Pages" on page 99. To install upgrades, see the next section.

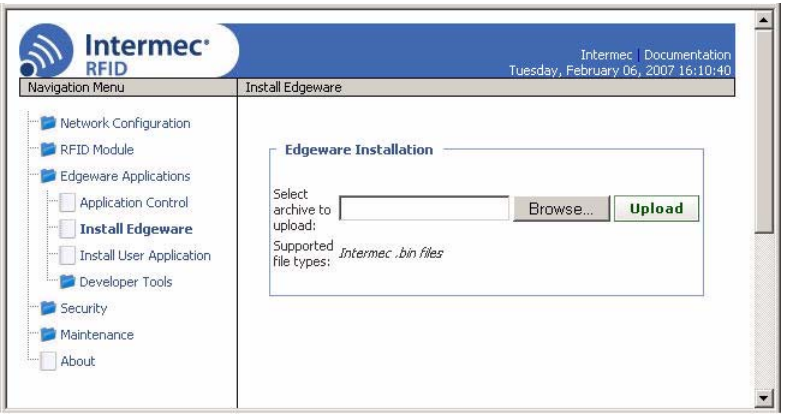
Upgrading or Installing Edgeware Applications

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 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 45.

About the IF61 ALE Engine

The EPCglobal ALE standard specifies methods by which large volumes of tag data can be processed into "events" that can be easily managed by applications. Processing can include reading tag IDs from one or more data sources, accumulating data over a specified time period, filtering data to eliminate duplication of tags, counting and grouping tag IDs to reduce the total volume of data, and reporting data.

The IF61 ALE engine supports version 1.0 of the EPCglobal ALE standard. For more information on the standard, see www.epcglobalinc.org/standards.

The default installation directory for the IF61 ALE engine is /home/developer/edgeware/ale.

On the IF61, the default logical reader is specified as "LocalAntenna*n*," where *n* is the number of the IF61 RFID antenna port. For example, "LocalAntenna1" is the antenna connected to RFID antenna port 1. All readers default to a polling value of 1 second.

The default configuration file is ale.conf. All settings are case sensitive.

About the ALE Configuration File

The ale.conf file is placed in the /home/developer/edgeware/ale/conf directory and can be edited directly through the web browser interface page. For more information on editing the file, see the next section, "Changing the ALE Configuration File."

Host applications can also use file transfer mechanisms such as FTP to update this file remotely.

The syntax for specifying a reader in the configuration file is:

```
Address="host:port"
PollingInterval=<number of seconds>
Command=<BRI command or commands resulting in a tag
report>
```

The configuration file is as follows:

```
[config]
;IP Port number to which ALE listens
ALE_ServerPort=8512
```

```
;Maximum number of characters in any
;ALE identifier (ECSpec Name, ReaderName, etc)
ALE_MaxIdentifierLength=128

;Number of threads servicing incoming ALE requests
ALE_RequestServerThreads=10

;Number of threads servicing outgoing ALE notifications
ALE_NotificationThreads=10

;ALE Version string returned by the ALE GetStandardVersion() API
ALE_Version="1.0"

;Version string returned by the ALE GetVendorVersion() API
ALE_VendorVersion=""

;ALE ID string returned in ECReports
ALE_ID="Intermec ALE"

;String prefix for temporary ECSpec created for Immediate()
;and Poll() API calls
; Note: an integer value will be appended to this string to form a
; unique identifier for the temporary ECSpec.
ALE_ImmediateSpecName="___INTERMEC___IMMEDIATE___"

;ALE schema version returned in all ALE responses
ALE_SchemaVersion="1.0"

;Maximum backlog (in number of bytes)of unprocessed reader reports
ALE_MaxQueueSize=5000000

;Maximum number of unprocessed reader reports (per reader)
ALE_QueueThreshold=20

;Number of seconds ALE waits for a connection when sending an
;ECReports notification
SOAP_ConnectTimeout=5

;Number of seconds ALE waits for a send when sending an ECReports
;Notification
SOAP_SendTimeout=5

;Number of seconds ALE waits for a response when sending an ECReports
;Notification
SOAP_RecvTimeout=5

;Logical Reader definitions
; Each definition contains the physical readers that comprise the
; Logical Reader
; Multiple physical readers can be specified under each logical
; reader
```

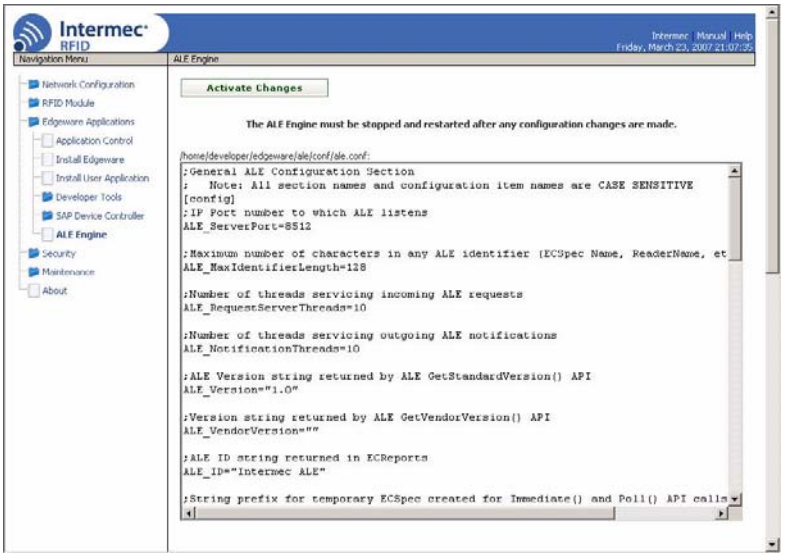
```
[LogicalReaders\LocalAntenna1]
physAntenna1="First Antenna"

[LogicalReaders\LocalAntenna2]
physAntenna2="Second Antenna"

[LogicalReaders\LocalAntenna3]
physAntenna3="Third Antenna"

[LogicalReaders\LocalAntenna4]
physAntenna4="Fourth Antenna"


;Physical Reader Definitions
;  ReaderType=BRI
;     --BRI is the only reader type currently
;           supported by Intermec ALE Engine
;  Address="ipaddr:port"
;     -- IP address (or hostname) and IP port
;           of the BRI port on this reader
;  Command="..."
;     -- BRI command for reading on this physical antenna
;  PollingInterval=integer_milliseconds
;     --Integer number of milliseconds between
;           polling cycles
;  GpioMonitor=[0|1]
;     -- 1== Monitor this reader for GPIO trigger notifications

[PhysicalReaders\physAntenna1]
ReaderType=BRI
Address="localhost:2189"
Command="attrib ants=1;READ"
PollingInterval=1000
GpioMonitor=1

[PhysicalReaders\physAntenna2]
ReaderType=BRI
Address="localhost:2189"
Command="attrib ants=2;READ"
PollingInterval=1000

[PhysicalReaders\physAntenna3]
ReaderType=BRI
Address="localhost:2189"
PollingInterval=1000
Command="attrib ants=3;READ"

[PhysicalReaders\physAntenna4]
ReaderType=BRI
Address="localhost:2189"
PollingInterval=1000
Command="attrib ants=4;READ"
```

Changing the ALE Configuration File

You can access and make changes to the ALE configuration file from the web browser interface as described next.

To edit the ALE configuration file

1 From the menu, click **Edgeware Applications** > **ALE Engine**. The ALE Engine screen appears.



2 Click in the text editor and make changes as necessary.

3 Click **Activate Changes**. Your changes are saved and will be made active the next time the ALE Engine is restarted.

If the ALE Engine is currently running and you want to make the changes active immediately:

a From the menu, click **Edgeware Applications** > **Application Control**. The Application Control screen appears.

b In the Edgeware Applications section, click for the ALE Engine 1.0 to stop the engine.

c Click **Activate Changes**.

d Click and then click **Activate Changes**. The ALE Engine is started and your changes are active.

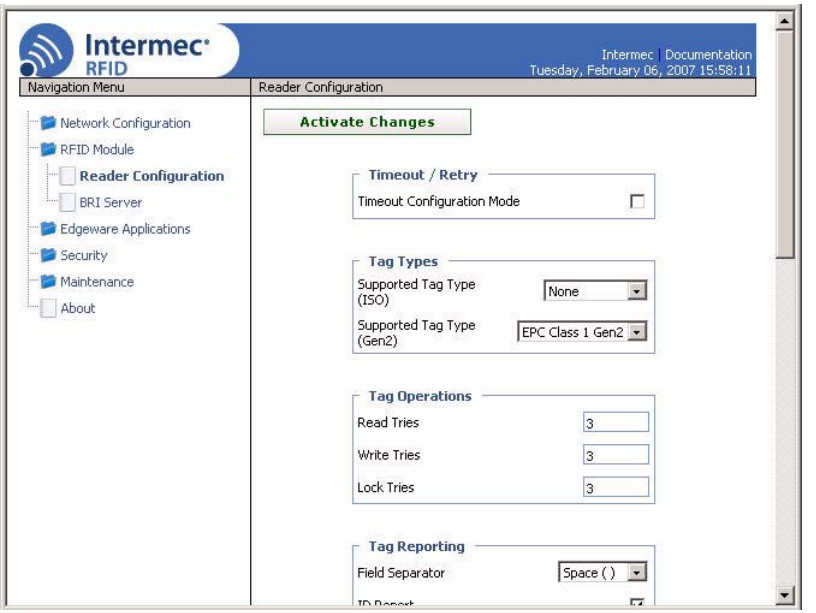
Configuring RFID Settings

This section explains how you use the web browser interface to change the settings for the IF61 RFID module. As you develop and test your application, you can configure the RFID settings for best system performance.

When you use the Diagnostics tool to display tags, the IF61 RFID module uses settings from the Reader Configuration screen. For help, see "Displaying Tags" on page 62.

To change RFID module settings

1 From the menu, click **RFID Module**. The Reader Configuration 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 RFID Module Settings

This section explains the RFID module settings. Most settings have BRI attribute equivalents. For more information, see the *Basic Reader Interface Programmer's Reference Manual* (P/N 937-000-xxx).

Timeout Configuration Mode

Enables a timeout mode. Instead of specifying the number of antenna or ID tries, you specify a 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.

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 **Save 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 timeout in the entry fields and then click **Save Changes**.

Supported ISO Tag Type

Sets the type of ISO tag for RFID operations. See the next table for more information. Default is None.

This setting is equivalent to the TAGTYPE BRI attribute.

ISO Tag Type Descriptions

Tag Type	Description
ISO6B/G1	ISO6B Generation 1
ISO6B/G2	ISO6B Generation 2
Phillips v1.19	Phillips v1.19
None	Disables ISO tag operations

Supported Gen2 Tag Type

Enables or disables Gen 2 tag support for RFID operations. Choose **EPC Class 1 Gen 2** (default) to enable Gen 2 support, or **None** to disable Gen 2 support.

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 will be read until the Read is successful. Valid range is 1 (default) to 254.

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 will be written to until the Write is successful. Valid range is 1 (default) to 254.

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 (default) to 254.

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 either space ( ) or comma (,). 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.

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. The maximum value is 65000 (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. The maximum value is 65000 (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 ETSI 302-208 channel scanning when the Listen Before Talk algorithm is enabled.

When this check box is checked, the LBT algorithm looks for a free transmit channel among the 10 available ETSI 302-208 channels. When this check box is not checked, the transmit channel is set by LBT Channel.

LBT Channel

(Supported only by 865 MHz readers) Sets the default transmit channel (of the 10 ETSI 302-208 channels) when the Listen Before Talk algorithm is enabled. Range is 1 to 10. Default channel is 5. This setting is used only when the LBT Scan Enable check box is not checked.

Enable Antenna Port *n*

Enables or disables the antenna connected to antenna port *n*. Check the check box to enable that antenna. Antenna Port 1 is enabled by default.

If more than one antenna is enabled, the antennas always fire in sequence numerically (1, 2, 3, 4). To change this sequence, you need to set the ANTS BRI attribute. For more information, see the BRI programmer's reference manual.

Field Strength

Sets the RF power level (measured as a percentage of maximum power) for all antennas. Valid range is 0 to 100 (default is 100).

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.

Configuring the BRI Server

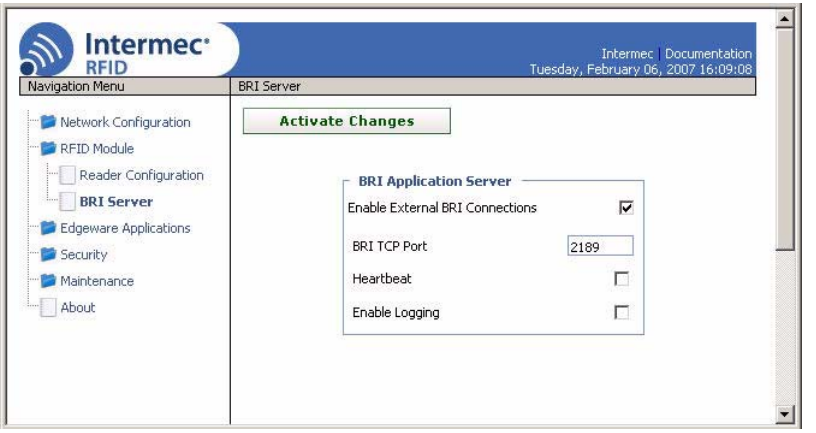
The IF61 BRI server handles communication between your application and the RFID module.

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 help, see "About the Intermec Ready-To-Work Indicator" on page 6.

You can configure the BRI server for your application. For help, see the next procedure.

To configure BRI server settings

1 From the menu, click **RFID Module** > **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.
Heartbeat	Enables/disables an asynchronous heartbeat event (EVT: HEARTBEAT BRI STRING). When enabled, the IF61 sends the heartbeat event every 30 seconds, enhancing the IF61's ability to detect TCP sessions that were not closed cleanly.
Enable Logging	Enables/disables logging of BRI server events. When you enable logging, you can also view and save a list of BRI server statistics, which can be helpful when testing your RFID system. 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.

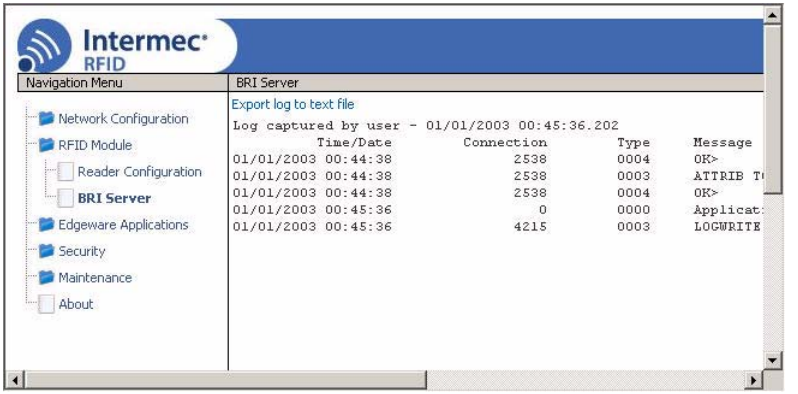
To enable BRI server logging and view the logfile

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

2 Check the **Enable Logging** check box.

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

4 Click **Display Log**. The BRI Server Log screen appears with a list of server events. For more information on server events, see the next table.



5 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 Server 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: 0 = BRI client connection status 1 = Received data from reader module 2 = Transmitted data to reader module 3 = Received data from BRI client 4 = Transmitted data to BRI client Types 1 and 2 are suffixed by the message checksum value used by the reader module to detect errors.
Message	Text of the message, including responses.

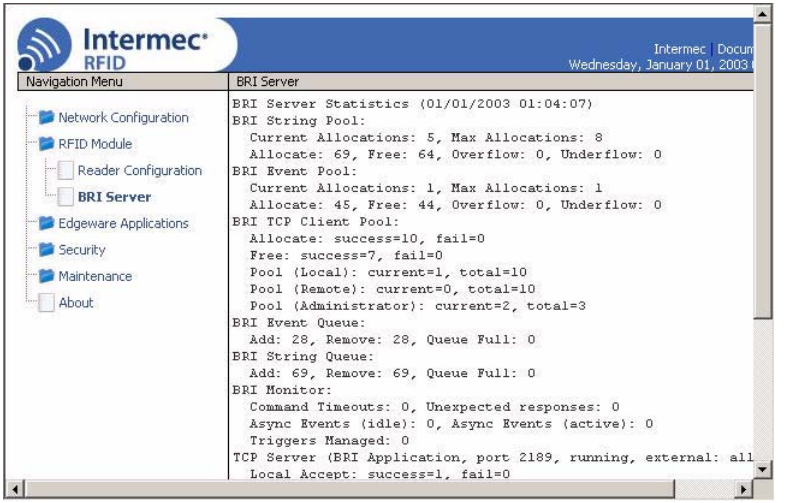
Viewing BRI Server Statistics

After you enable logging, you can use the web browser interface to view a list of BRI server statistics.

To view BRI server statistics

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

2 Click **Display Statistics**. The list of BRI server statistics appears.



3 To save the list, choose **File** > **Save As** in the browser menu. Follow the prompts to save the list to your desktop PC as a .txt file. Because the entire web page is saved, there will be other information in addition to the list of statistics.

About the Developer Tools

You can use the Developer Tools to test and fine-tune your RFID system. The Developer Tools support these features:

- Continuous tag reading, including tag ID reporting. For help, see the next section, “Displaying Tags.”
- General purpose input/output (GPIO) testing. For help, see “Testing the GPIO Interfaces” on page 63.
- 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 67.
- Editing and testing JavaScript files. For help, see “Using the Workbench” on page 68.

Note: To use the Developer Tools, you need to enable the IF61 Developer Tools. For help, see "About the IF61 Edgeware Applications" on page 46.

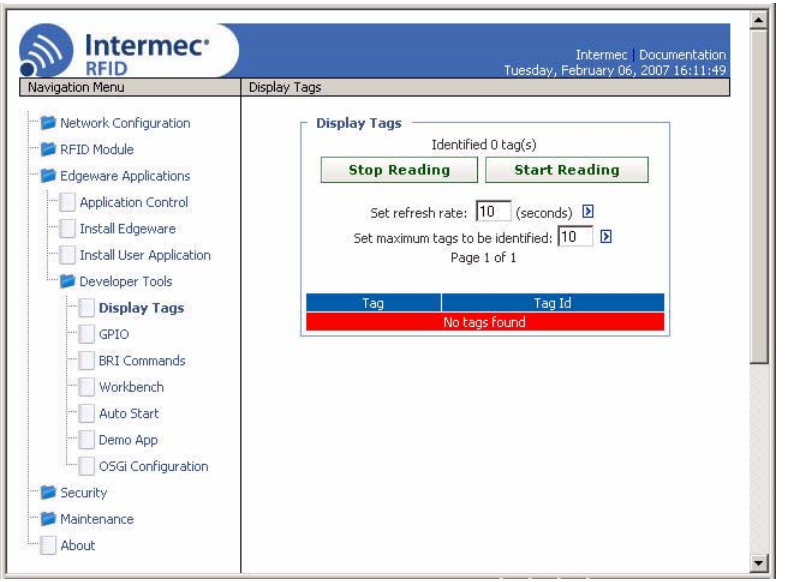
Displaying Tags

You can use the Display Tags tool to execute read cycles on the IF61. This procedure may be useful when you are testing antenna locations or tag placement.

Note: The read cycle is based on the settings listed in the RFID Module screen. For help, see "Configuring RFID Settings" on page 52.

To display tags and tag IDs

1 From the menu, click **Edgeware Applications** > **Developer Tools**. The Display Tags screen appears.

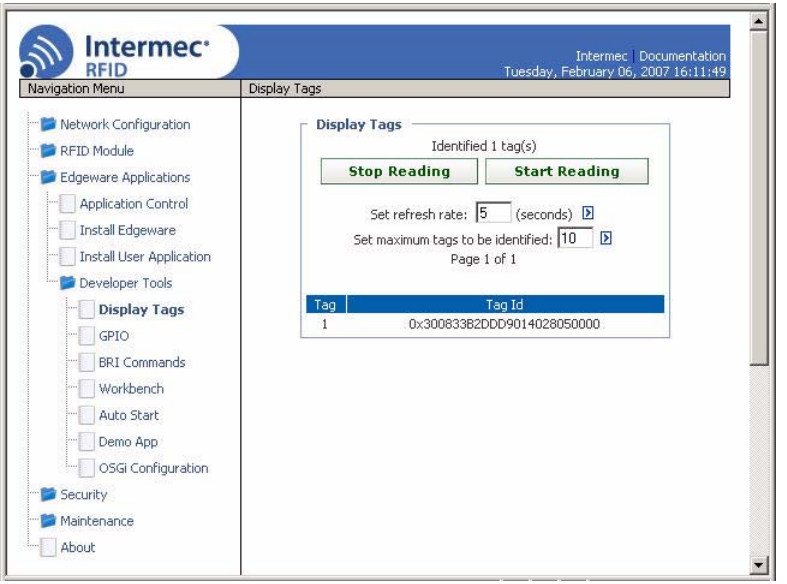


- In the **Set refresh rate** entry field, enter the number of seconds for the read cycle, and then click ▷. The default is 10.

- In the **Set maximum tags to be identified** entry field, enter the maximum number of tags to identify during each read cycle, and then click ▶. The default is 10.

2 Click **Start Reading**. The IF61 looks for RFID tags within range of the connected antennas.

When the IF61 finds readable tags, the tag IDs appear in the list in the order in which they were read.



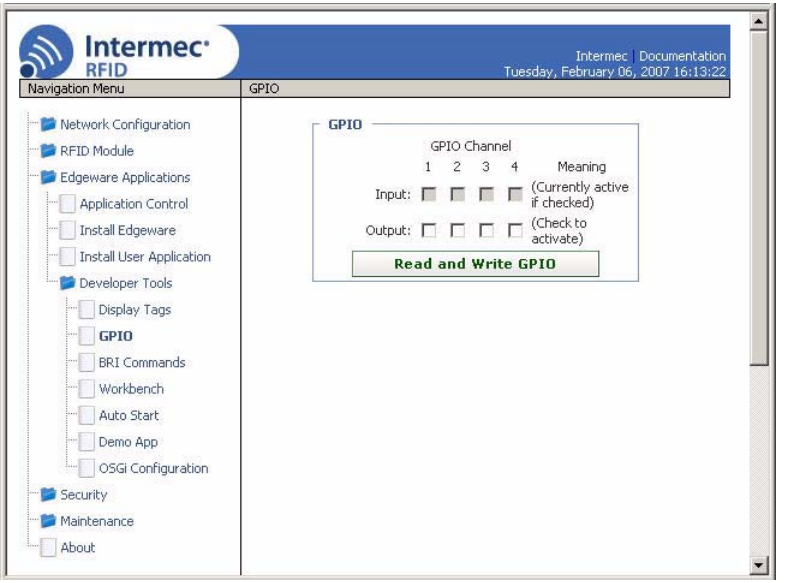
3 Click **Stop Reading** to end the read cycle.

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 **Edgeware Applications** > **Developer Tools** > **GPIO**. The GPIO screen appears.



When this screen appears, the four IF61 GPIO interfaces are turned off (equivalent to sending the BRI command `WRITEGPIO=0`).

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 (equivalent to `WRITEGPIO=15`), and its associated GPIO input is turned on.

   If a check box is not checked, that GPIO output is turned off and its associated GPIO input is turned off.

3 Click **Read and Write GPIO**. The GPIO interface state is changed.

Using the GPIO Demo Application

The IF61 includes a demo application you can use to test your GPIO input and output interfaces and verify that the controls behave as expected.

Basically, the demo application works this way:

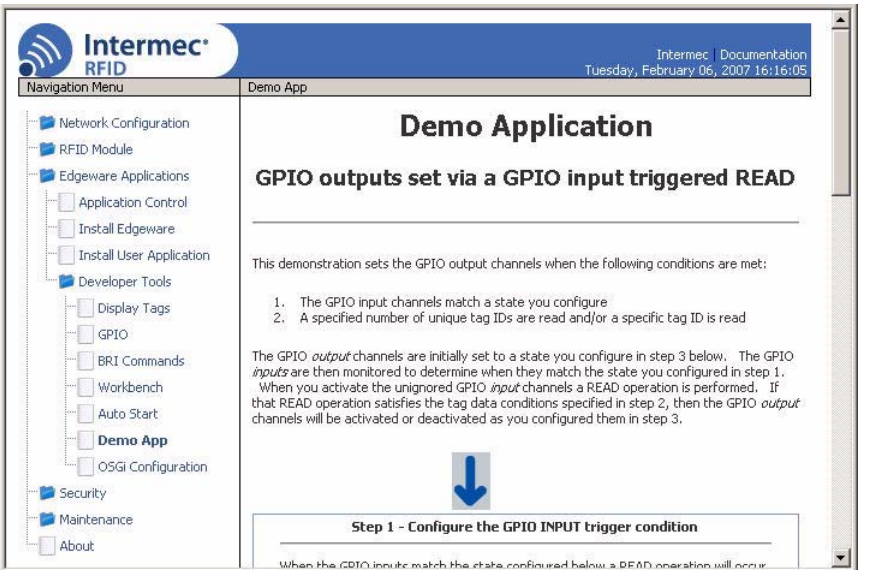
First, you set which GPIO input channels are monitored. The IF61 will read tags when the specified input channels are activated (for example, when a motion sensor connected to GPIO input 1 is triggered).

Next, you set the conditions under which the GPIO output state should change. You can specify a quantity of tags read, a specific tag ID, or both. When the conditions are met, the GPIO output state changes.

Finally, you set which GPIO outputs are to be triggered. For purposes of the demo application, you set both the initial and target states of the output channels (for example, if a light fixture connected to GPIO output 2 is initially OFF and then turns ON after the read conditions are met).

To use the GPIO demo application

1 From the menu, click **Edgeware Applications** > **Developer Tools** > **Demo App**. The GPIO demo application screen appears.



2 In the Step 1 box, click the **Perform a READ when these are activated** button for the GPIO input channels you want to test. Input 1 is selected by default.

3 In the Step 2 box, enter the number of unique tag IDs to read that triggers a change in the output state, or enter a specific tag ID that triggers the change.

4 Click the **Evaluate** button for the values you defined in step 3. When you run the demo, the IF61 changes the output state when the predefined number of unique tag IDs are found, or when the specified tag ID is found.

Or, click the **Ignore** button if you want the demo application to ignore one or the other of the defined values. This feature is useful if you want to test the demo for only one of the defined values.

Note: To run the demo application, you must choose **Evaluate** for at least one of the two values.

5 In the Step 3 box, click one of the **GPIO output INITIAL state** option buttons for each of the GPIO output lines:

- Click the **Start with this channel activated** button for each GPIO output channel that should be "on" when the demo application starts (for example, if a light connected to that output should be ON before the output channel state is changed).
- Click the **Start with this channel deactivated** button for each GPIO output channel that should be "off" when the demo application starts.

6 Click one of the GPIO output TARGET state option buttons for each of the GPIO output lines:

- Click the **Activate this output channel** button for each GPIO output channel that should be turned "on" when the demo application changes the IF61 output state.
- Click the **Deactivate this output channel** button for each GPIO output channel that should be turned "off" when the demo application changes the IF61 output state.

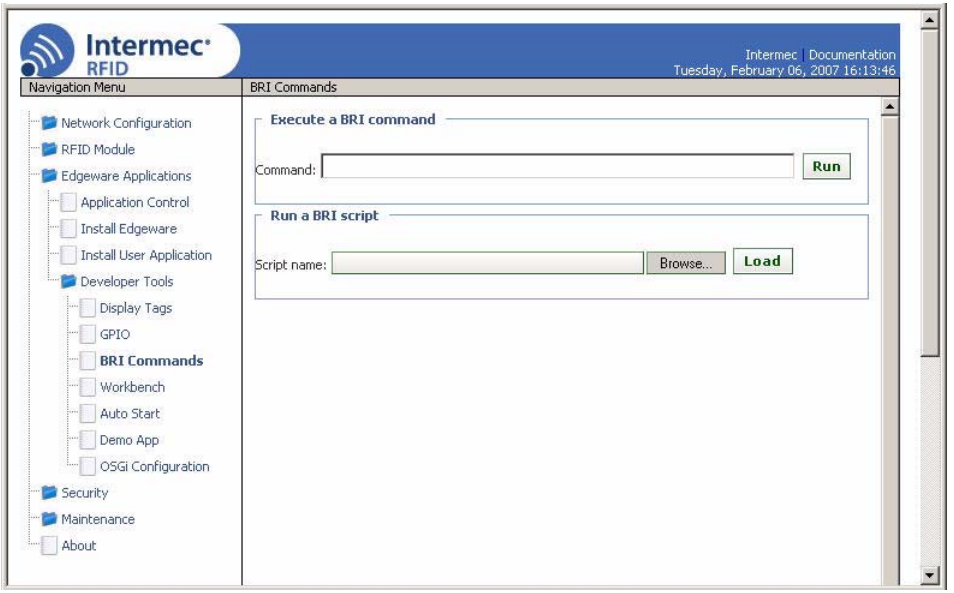
7 Click **Start Demo** to run the demo application.

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.

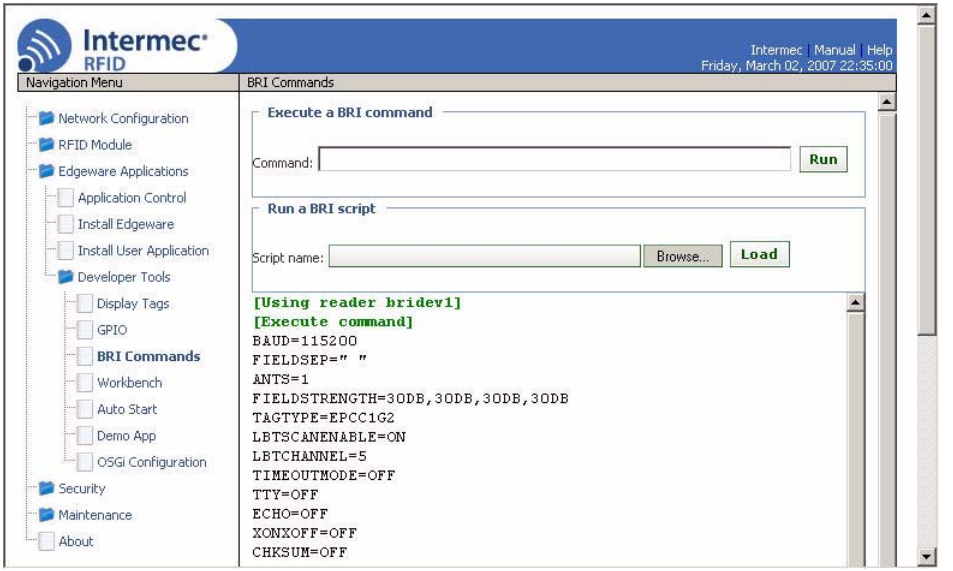
To send BRI commands

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.
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.

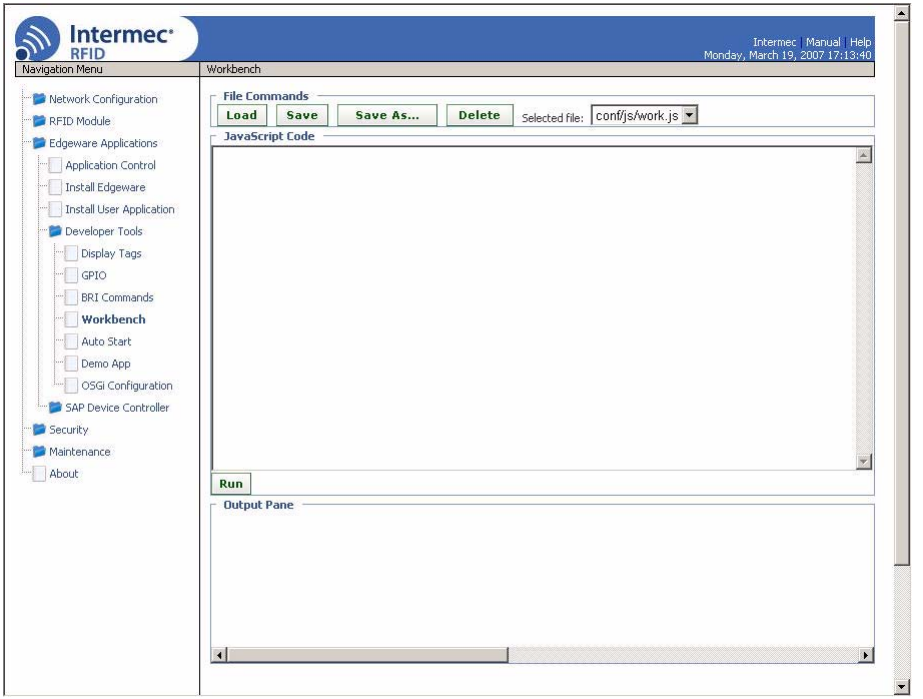
Using the Workbench

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 **Edgeware Applications** > **Developer Tools** > **Workbench**. The Workbench screen appears.



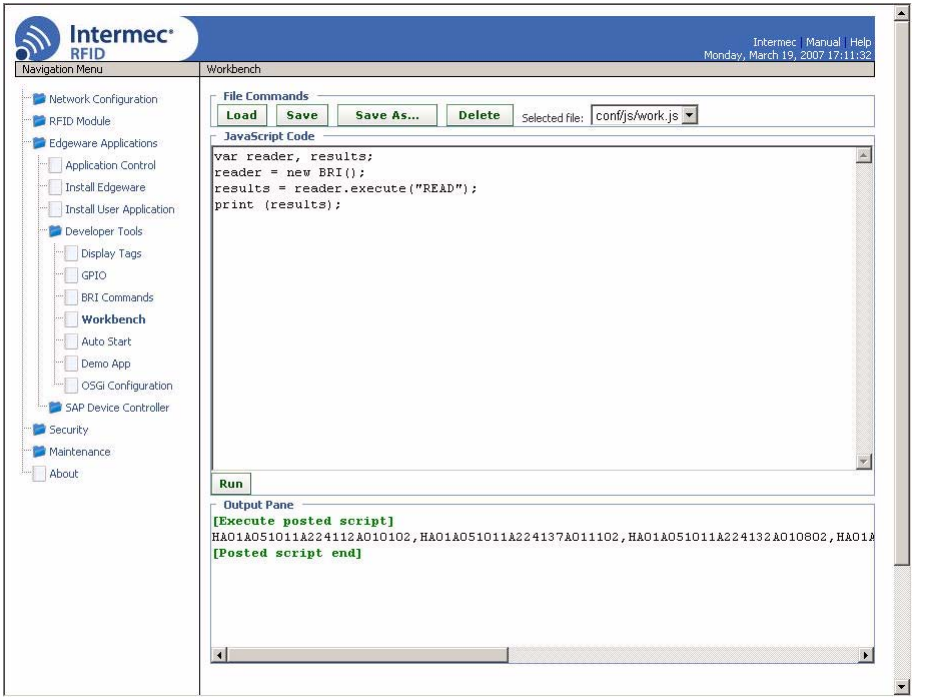
2 Click in the JavaScript Code box to enter code. You can also paste text copied from Notepad or another application. Copy the text from the other application and choose **Edit** > **Paste** in the browser menu.

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

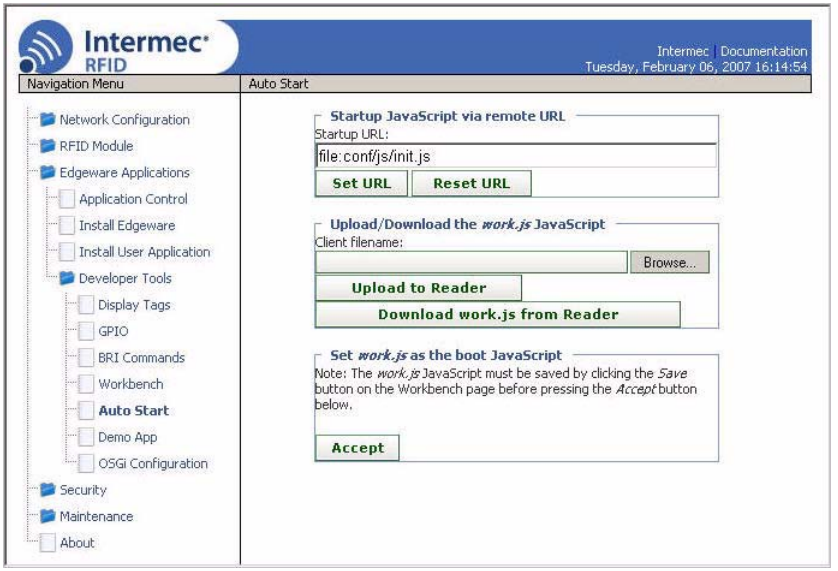
Note: For help with configuring the IF61 to run other executables or scripts when the IF61 boots, see "Auto-Starting Applications at Boot Time" on page 39.

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

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's 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.

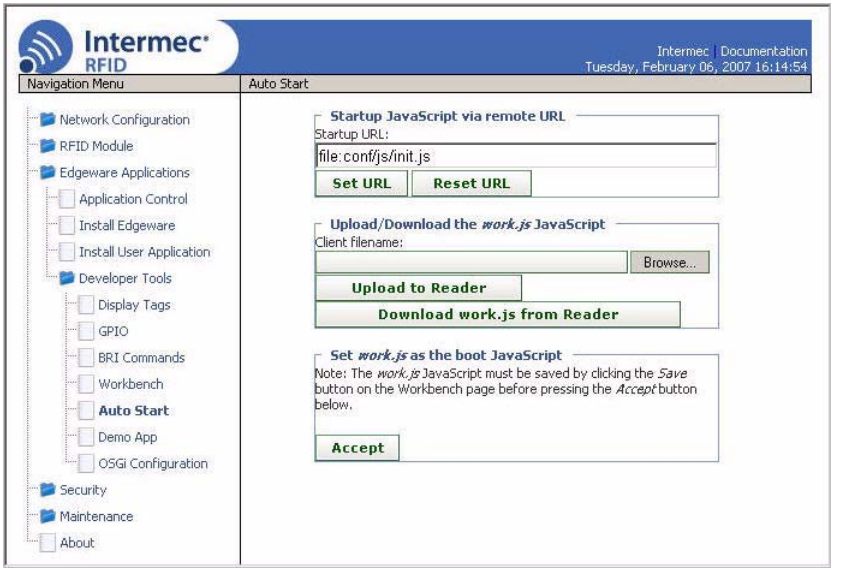
To reset the URL to the default (file:conf/js/init.js), click **Reset URL**.

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 68.

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 Simple Network Management Protocol (SNMP)
- Using SmartSystems Foundation
- Using Wavelink Avalanche
- Importing and Exporting Files
- Opening Connections to the Linux Shell
- 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 10. This manual assumes you are using this method for all procedures.
- an SNMP management station. For help, see the next section.
- the Wavelink Avalanche client management system. For help, see "Using Wavelink Avalanche" on page 80.
- the Intermec SmartSystems Console. For help, see "Using SmartSystems Foundation" on page 79.

Using Simple Network Management Protocol (SNMP)

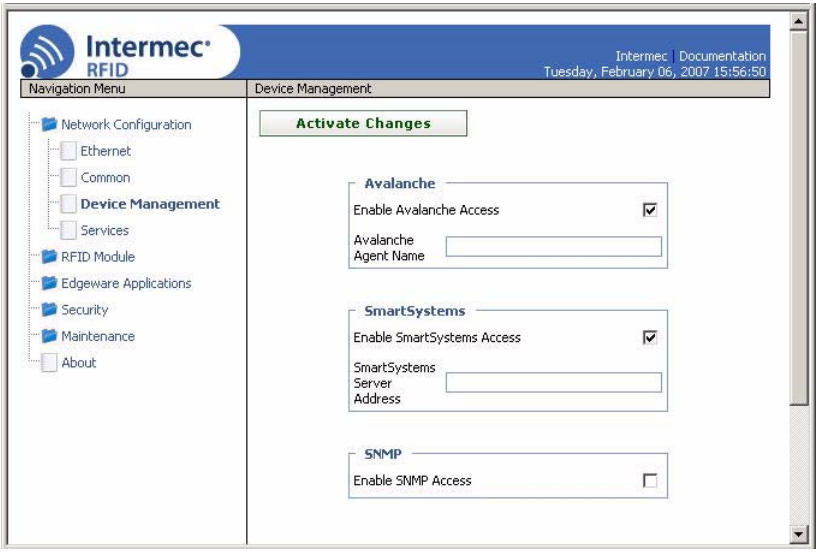
You can access and manage the IF61 from a Simple Management Network Protocol (SNMP) station. Contact your Intermec representative for a copy of the management information base (MIB).

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

- enable SNMP access to the IF61. By default, SNMP access is disabled.
- 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.



2 Check the **Enable SNMP Access** check box. A list of SNMP configuration items appears.

3 Configure SNMP settings for your network. For help, see the next table.

4 Click **Activate Changes** to save your changes and immediately make the changes active.

SNMP Community Parameter Descriptions

Parameter	Description
Enable SNMP Access	Check this check box to enable SNMP access to the IF61. SNMP access is disabled by default.
SNMP Community (Read-Only)	Password for read-only access. Range is 1 to 15 characters, case-sensitive. Default is `public`.
SNMP Community (Read/Write)	Password for read/write access. Range is 1 to 15 characters, case-sensitive. Default is `private`.
SNMP Trap Target 1	Authoritative name for trap target 1.
SNMP Trap Target 2	Authoritative name for trap target 2.
SNMPv3 Username (Read-Only)	User name for SNMPv3 read-only access. Default is `readonly`.

SNMP Community Parameter Descriptions

Parameter	Description
SNMPv3 Password (Read-Only)	Password for SNMPv3 read-only access. Default is `intermec`.
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**.
SNMPv3 Username (Read/Write)	User name for SNMPv3 read/write access. Default is `intermec`.
SNMPv3 Password (Read/Write)	Password for SNMPv3 read/write access. Default is `intermec`.
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**.

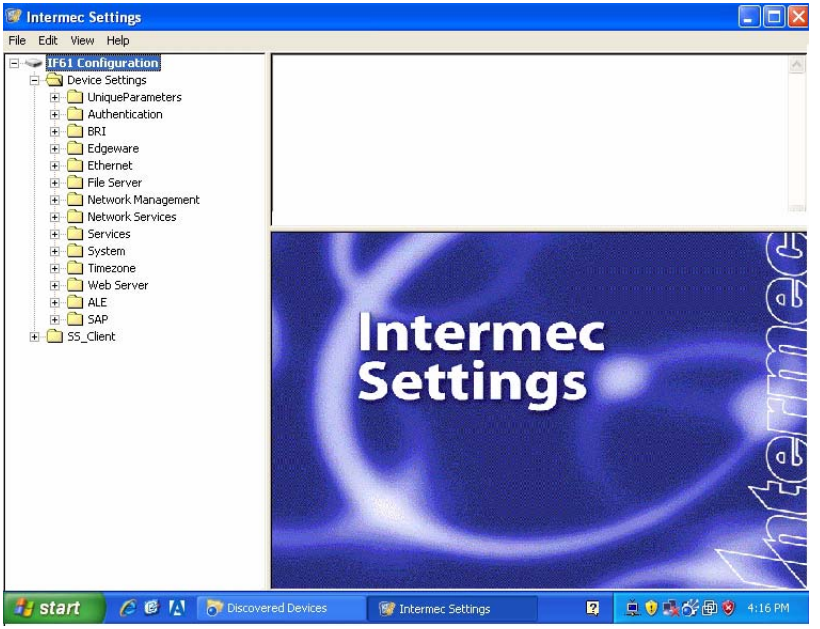
Using SmartSystems Foundation

The IF61 ships with a SmartSystems™ Client, which means you can manage it from a central host PC using Intermec'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**.

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:

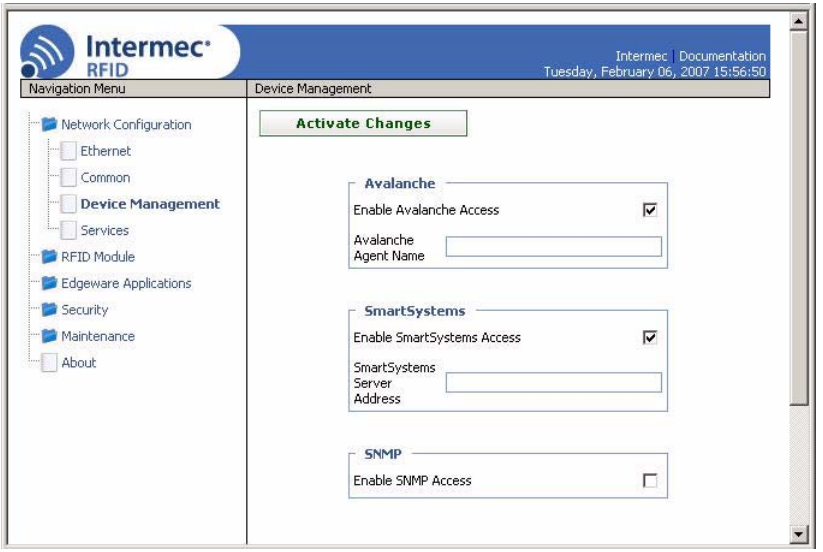
- Software packages are groups of files for an application that resides on the device.
- Software collections are logical groups of software packages.

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.



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 100.
- For help with installing applications, see "Installing RFID Applications on the IF61" on page 44.

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."
- enable Common Internet File System (CIFS) file sharing on the IF61. For help, see "Using CIFS File Sharing" on page 83.
  - For help with enabling CIFS, see "Configuring Common Network Settings" on page 23.
- auto-mount a Network File System (NFS) share at boot time. For help, see "Controlling Access Services" on page 26.

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 26.

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.

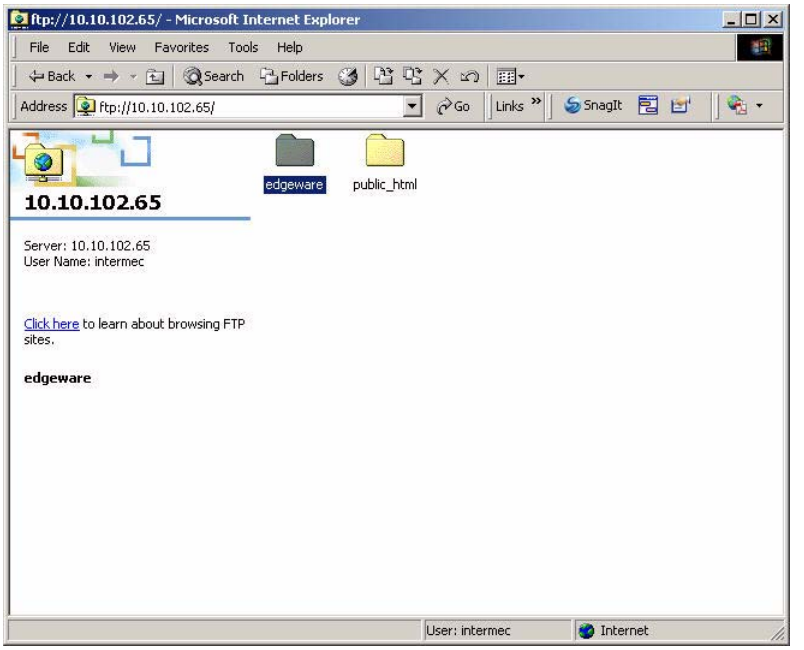
To access the IF61 via FTP

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.
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.



You can access the edgeware directory via FTP. Applications installed through the web browser interface can be found in the edgeware/userapp*n* directory, where *n* is the number of the installation slot minus 1 (for example, if you installed an application in slot 3, the application is in the edgeware/userapp2 directory).

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.

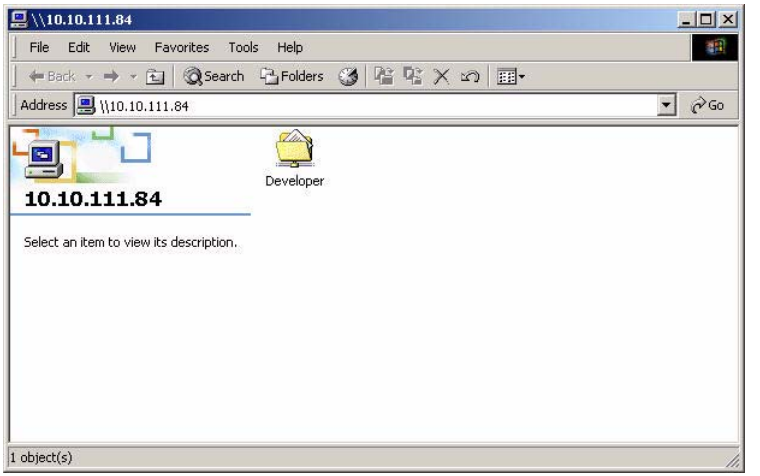
To access the IF61 directories via CIFS file sharing

1 Enable CIFS file sharing on the IF61. For help, see "Configuring Common Network Settings" on page 23.

2 On your desktop PC, choose **Start** > **Run**. The Run dialog box appears.

3 Enter the IP address of the IF61 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`.



If the IF61 uses a static IP address, you can also map a drive on your desktop PC to the IF61. 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 85.

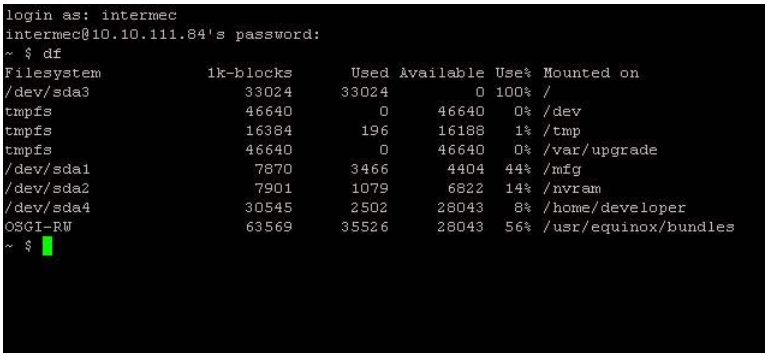
- You can open a connection through a communications program such as HyperTerminal. For help, see "Using a Communications Program" on page 86.

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 26.

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`).



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

Opening a Telnet Connection

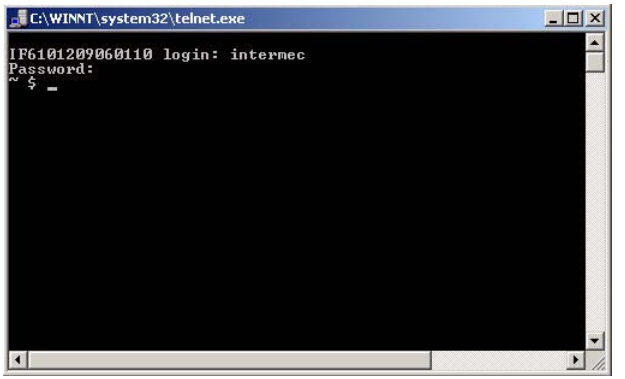
Follow the next procedure to open a Telnet connection to the IF61 for access via the Linux shell.

To open a Telnet session, you need to enable Telnet shell access to the IF61. For help, see "Controlling Access Services" on page 26.

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



Using a Communications Program

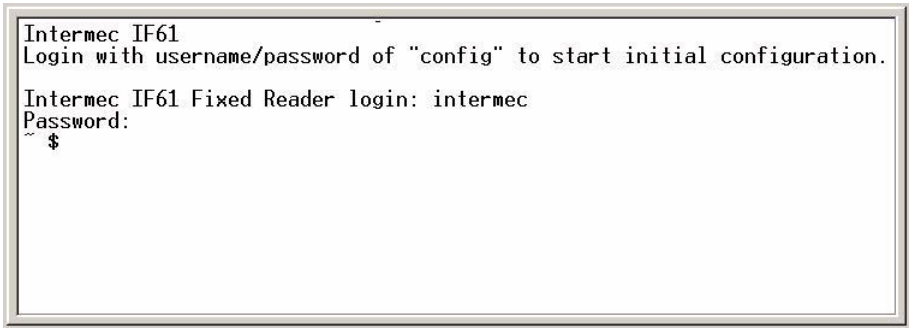
Note: For more secure access to the IF61, use a Secure Shell (SSH) connection. For help, see "Opening a Secure Shell (SSH) Connection" on page 85.

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

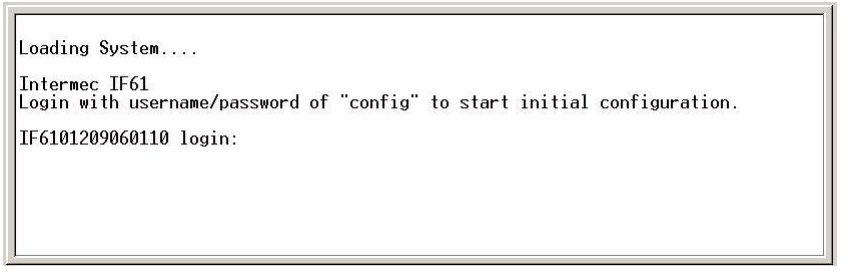
1 Connect the null-modem cable from the serial port on the IF61 to a serial port on your PC.

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

Bits per second	115200
Flow control	None

3 Connect the IF61 to AC 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.



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 8.
- 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 92.
- You can access the Linux shell. For help, see "Accessing the IF61 via the Linux Shell" on page 84.

Maintaining the IF61

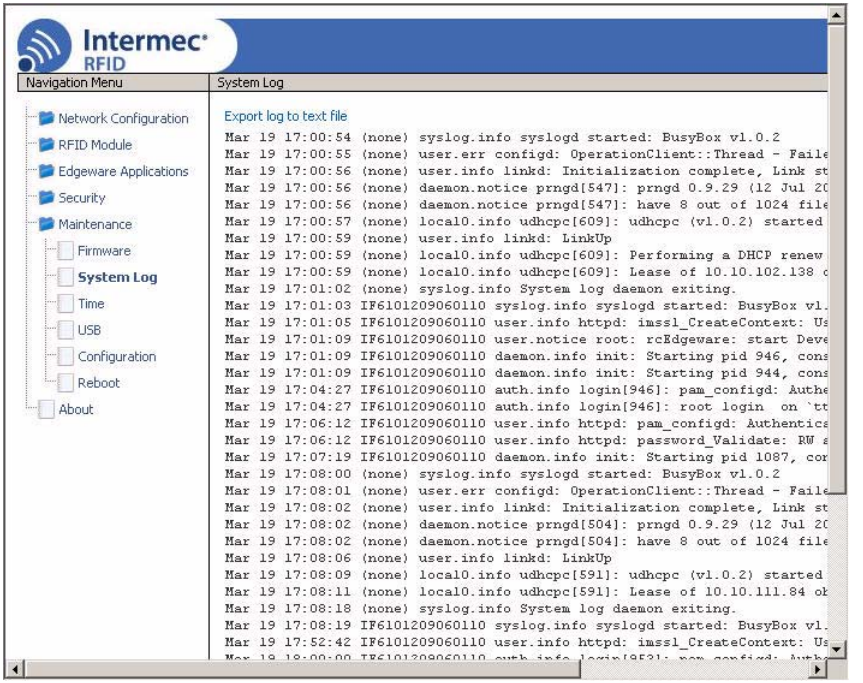
The Maintenance menu lets you view IF61 parameters and statistics, including a list of logged events. You may need this information if you need to call Intermec Product Support.

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.



2 To save the list, click **Export log to text file**. The log is saved as Syslog.log and appears in the browser window.

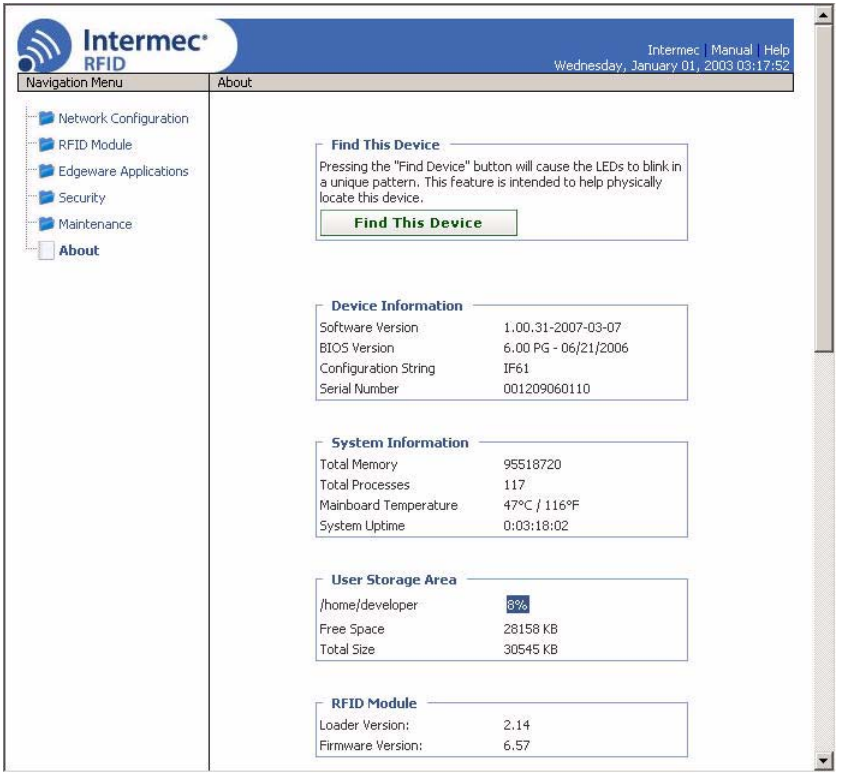
3 Choose **File** > **Save As** and follow the prompts to save the log file to your desktop PC.

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 **Maintenance** > **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: Total space and space used in the /home/developer directory.
- 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

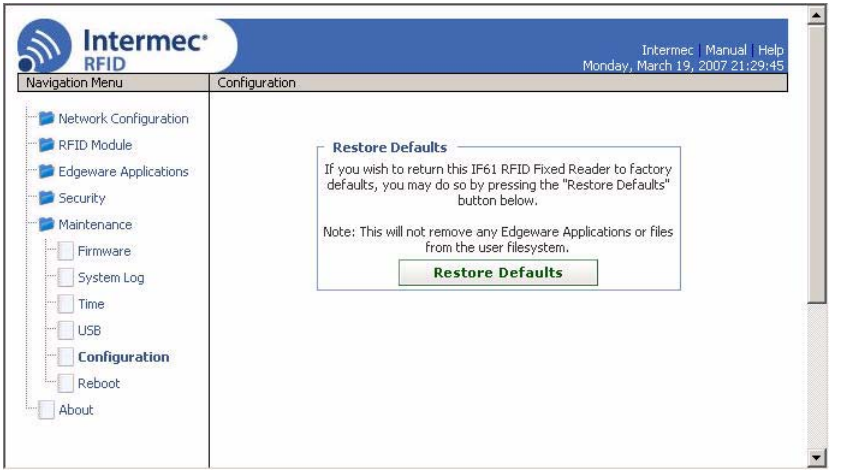
Note: Restoring default settings as described in this section does not affect applications or security certificates you have installed.

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 92.

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.

   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 87.

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.

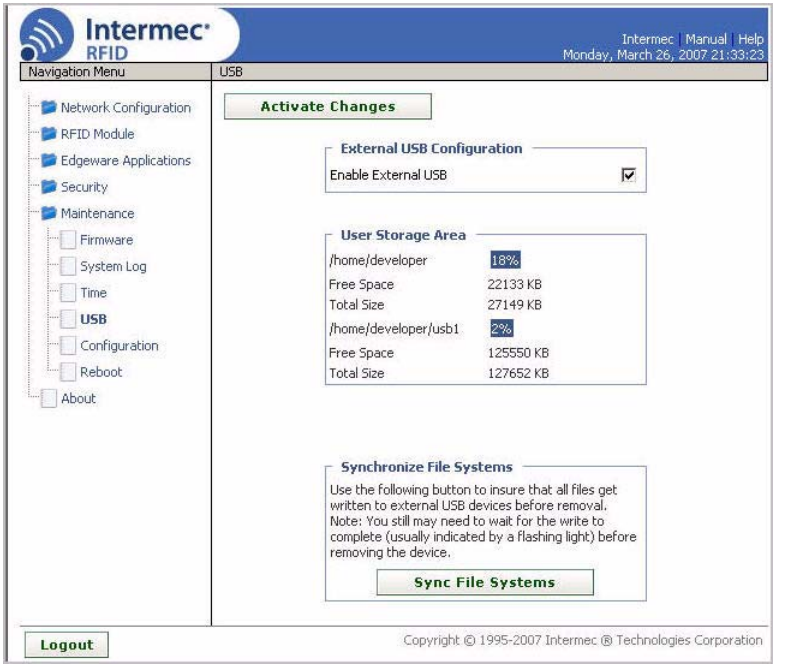
2 Click **Reboot** to reboot the IF61. You may need to login again after the IF61 reboots.

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.

To manage USB devices

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



USB Screen: *In this sample screen, an installed USB drive is shown as /home/developer/usb1.*

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 105.

The User Storage Area box lists the available space on the /home/developer directory where applications are installed. If you have USB drives connected to the IF61, the drives appear in the User Storage Area list as /home/developer/usb1 or /usb2.

2 To disable automatic upgrades or to eject a connected USB device, 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 "Configuring RFID Settings" on page 52.

RFID Problems and Solutions

Problem	Solution
The IF61 is unable to read RFID tags, or seems to read tags slowly or inconsistently.	Check these conditions: • 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. • Terminators must 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 RFID Settings" on page 52.
The IF61 does not respond to your RFID application.	Your application may not be communicating with the IF61 BRI server. Check these conditions: • Make sure that you have disabled the IF61 Developer Tools or SAP Device Controller edgeware. For help, see "About the IF61 Edgeware Applications" on page 46. • 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 58.

RFID Problems and Solutions (continued)

Problem	Solution
The SAP device controller does not connect to the SAP backend module installed on your server.	Check these conditions: • Make sure you have enabled the SAP device controller edgeware on the IF61. For help, see "About the IF61 Edgeware Applications" on page 46. • Check the SAP device controller configuration files and make sure you have the correct information for your SAP system. For help, see "Editing the Configuration Files" on page 126.

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 also need a known good RFID tag.

To connect directly to the IF61 RFID module and verify operation

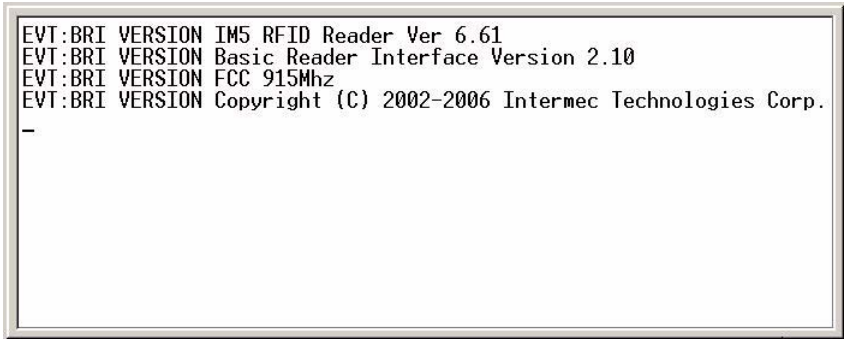
1 Use a communications program (such as HyperTerminal) to open a TCP/IP connection to the IF61 with these parameters:

IP Address IP address of the IF61

Port 2189

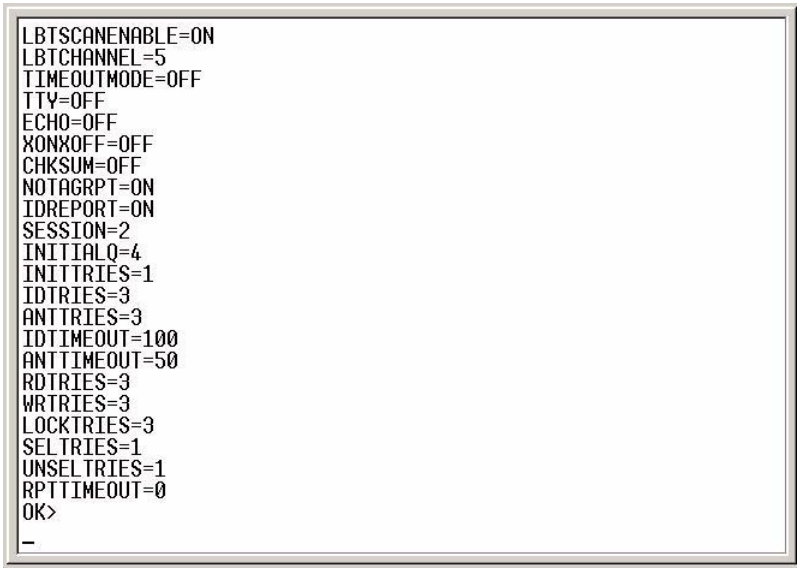
Configure the communications program to echo typed characters locally and to send line feeds with line ends.

2 Press **Enter**. The RFID module boot sequence text appears.



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

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



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

4 (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

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.	**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.	**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 26.
You cannot access the IF61 FTP directory.	Make sure that the IF61 FTP server is enabled. For help, see "Controlling Access Services" on page 26.
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 10.
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 26.

Connectivity Problems and Solutions (continued)

Problem	Solution
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 "Configuring the IF61" on page 8.

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 89.

When you have these answers, call Intermec Product Support at 1-800-755-5505.

Accessing Intermec Web Pages

Periodically, IF61 firmware and edgeware 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 10.
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 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 Firmware Bundle utility from the Intermec web site. For help, see the previous section, "Accessing Intermec Web Pages."
2. Run the Firmware Bundle 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 103.

Configuring the Firmware Upgrade

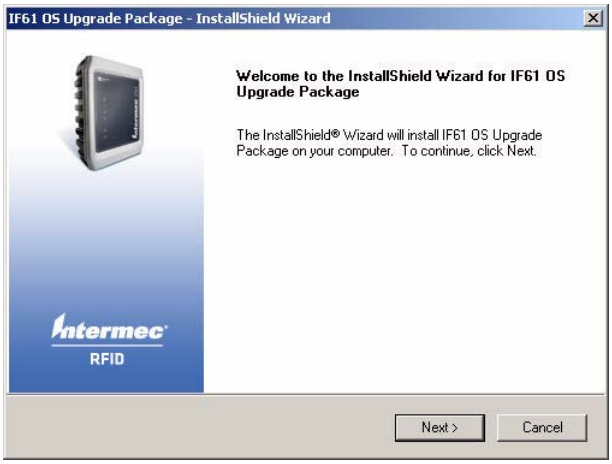
The Firmware Bundle utility configures IF61 firmware upgrades. The configuration you need depends on the method you use to upgrade the IF61:

- 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.

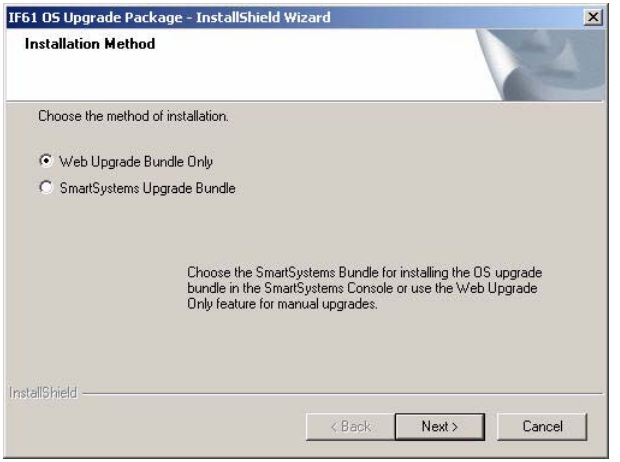
This section explains how to choose the correct configuration.

To configure the firmware upgrade file

1 Double-click the Firmware Bundle 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.

   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 in the directory tree to choose the location.

   c Click **Next**.

   d Click **Install**. The file is installed at the new location.

Note: If you are using SmartSystems Server to upgrade the IF61, do not change the default file location.

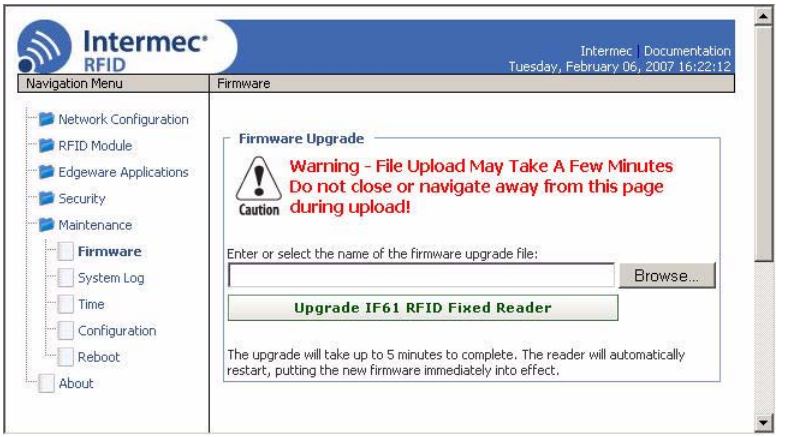
5 Click **Finish** to close the utility.

Installing the Firmware Upgrade

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

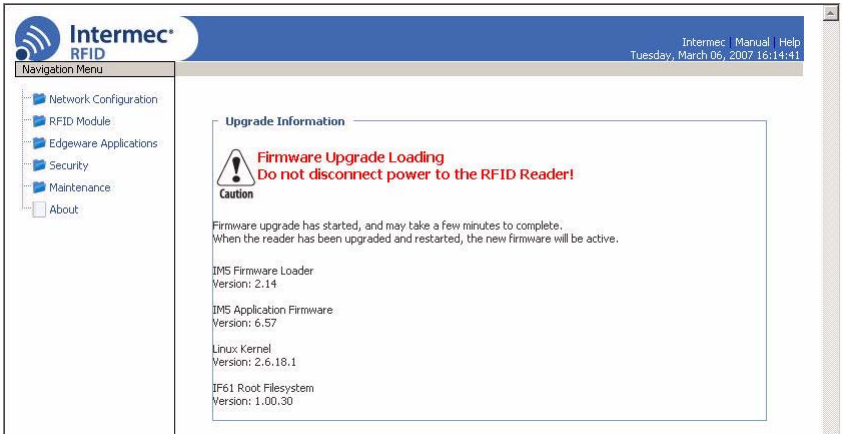
Upgrading from the Web Browser Interface

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.

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 Intermec web site.

Before you can upgrade the IF61, you need:

- SmartSystems Foundation. To download SmartSystems Foundation, go to www.intermec.com/SmartSystems.
- the IF61 upgrade file. For help, see "Configuring the Firmware Upgrade" on page 101.

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 you want 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 93.

1. Follow the procedure for configuring the upgrade file. For help, see "Configuring the Firmware Upgrade" on page 101.
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.

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. For more information, see the Avalanche 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 118.

You can also use the GPIO Terminal Block accessory to connect devices to the IF61 GPIO interfaces. The block provides access to the IF61 GPIO interfaces via standard screw terminals.

GPIO Terminal Block accessory

For more information on the terminal block, 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.

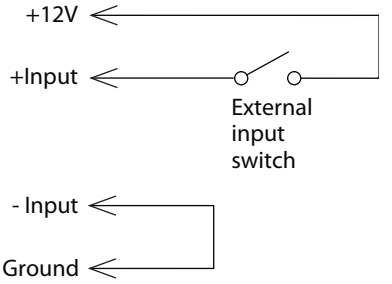
There are three basic ways to connect input controls to the IF61 input interfaces:

- 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

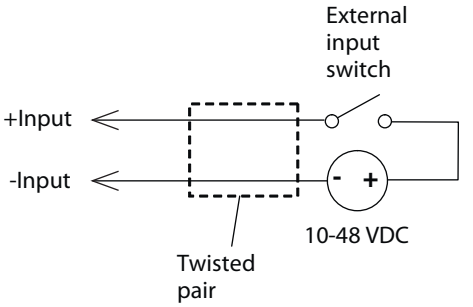
This is the simplest way to connect a control to an IF61 input interface. If the external control device is a switch, you can connect one side of the switch to an IF61 +Input pin, and the other side of the switch to one of the +12 VDC sources. Ground the corresponding -Input pin as shown in the next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

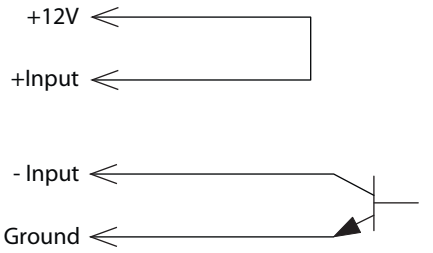


Isolated Input Interface

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.

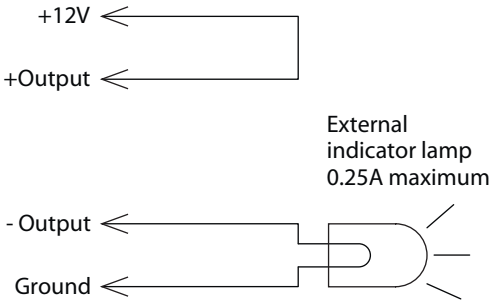
In a typical application, the outputs control indicator lamps that signal good reads or errors. The basic methods for connecting external devices to the GPIO outputs include:

- 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.

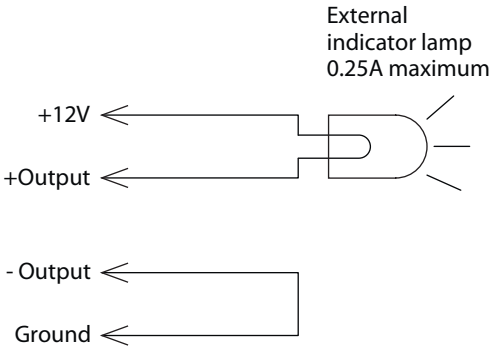


Switching the High Side

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.

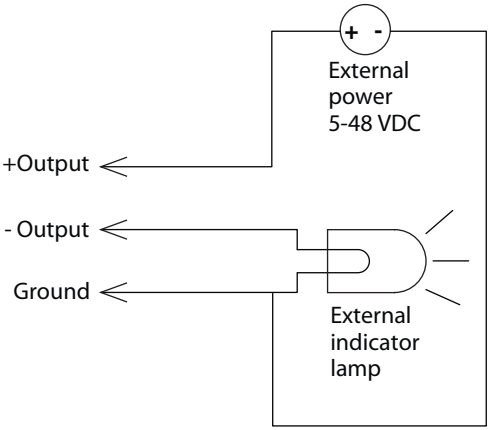
In this method, connect the external indicator lamp to the +Output and +12 VDC pins, and short the corresponding -Output pin to ground as shown.



Switching the Low Side of the Output Load

Switching the High Side Using External Power

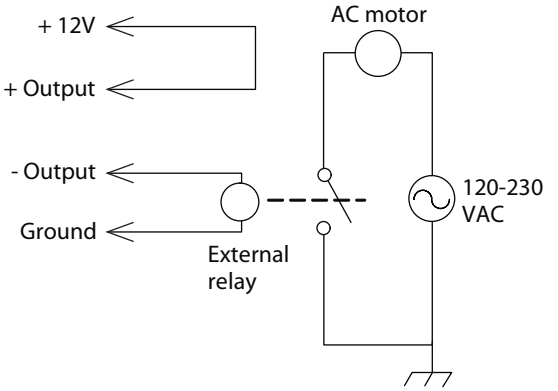
To use external power (5 to 48 VDC) to switch the high side, connect the Ground pin to the ground system of the external power supply, and connect the positive side of the external supply to the +Output pin. The external indicator lamp is connected to the corresponding -Output and Ground pins as shown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



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

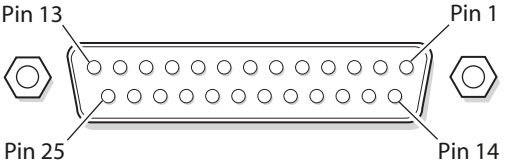
Height	10.7 cm (4.2 in)
Length	34 cm (13.2 in)
Width	23 cm (8.9 in)
Weight	2.6 kg (5.7 lb)
AC electrical rating	~ 100 to 240V, 1.0 to 0.5A, 50 to 60 Hz
Operating temperature	-20ºC to +55ºC (-4ºF to +131ºF)
Storage temperature	-30ºC to +70ºC (-22ºF to +158ºF)
Humidity (non-condensing)	10 to 90%
Ethernet 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

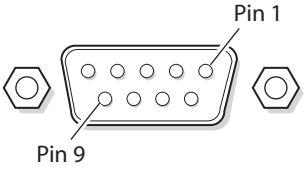
GPIO Port



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

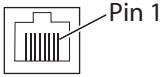
Serial Ports (COM1, COM2)



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).

B Configuring and Using the SAP Device Controller

This appendix explains how to use the SAP device controller edgeware on the IF61. It includes a section that explains how to use the SAP data processors with tag data.

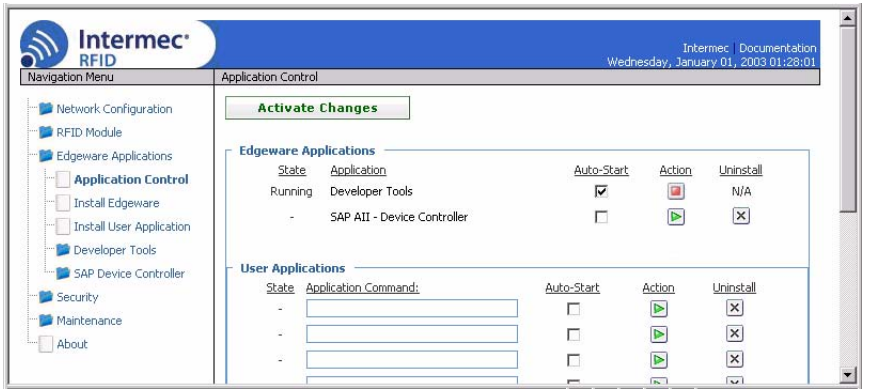
About the SAP Device Controller

This section explains how to run and use the SAP device controller on the IF61. In your SAP system, the controller communicates with an SAP Auto-ID Infrastructure (SAP-AII) server. On the IF61, the device controller software is installed in the /home/developer/edgeware/sap directory.

Note: To prevent processing errors, Intermec recommends that you not run the Developer Tools or the ALE edgeware simultaneously with the SAP device controller. For help, see "Managing Applications" on page 45.

To start or stop the SAP device controller

1. Start the web browser interface. For help, see "Using the Web Browser Interface" on page 10.
2. Assign a static IP address to the IF61. For help, see "Configuring the IF61" on page 8.
3. In the web browser interface menu, choose Edgeware Applications. The Application Control screen appears.



4. To run the SAP device controller whenever the IF61 boots, check the **Auto-Start** check box and then click **Activate Changes**. The device controller will auto-start the next time the IF61 boots.

   You can also manually stop or start the device controller as follows:

   - If the device controller is running, click  to stop it.

- If the device controller is not currently running, click  to start it.

5 (Optional) If actual time should be used in messages reported by the SAP device controller, set SNTP parameters. For help, see "Configuring Common Network Settings" on page 23.

6 (Optional) Change settings in the SAP-DC configuration files as needed. For help, see "Editing the Configuration Files" on page 126.

7 Click **Activate Changes** to save your additional changes. All changes become active the next time the device controller starts.

Stopping or Reconfiguring the Device Controller Over the Network

When the device controller is running, you can stop or reconfigure the controller by sending an XML command message over HTTP to the configured listening port (typically port 9000).

To stop the device controller, send this command message:

```
<?xml version="1.0" encoding="utf-8"?>
<Command id="123456789" response="rec1">
<Shutdown/>
</Command>
```

To reconfigure the device controller, send this command message:

```
<?xml version="1.0" encoding="utf-8"?>
<Command id="123456789" response="rec1">
<Reconfigure URL="http://hostname/config.xml">
</Command>
```

where:

hostname is the directory where the configuration file is located.

config.xml is the name of the configuration file.

About the SAP-DC Configuration Files

The SAP device controller uses several configuration files:

- SDCConfiguration.xml

  Main configuration file for the device controller. Not required if the SimpleDevice.property file points to other than this default location. For more information, see "About the SDCConfiguration XML File" on page 127.

- RfidReader.properties

  Defines hardware-specific settings, such as tag ID length or the number of Read tries. For more information, see "About the RfidReader.properties File" on page 133.

- SimpleDevice.property

  Defines logging properties and the URL of the main configuration file for the device controller. This file is loaded at startup of the device controller. To use another filename, add the filename as an additional parameter to the command line when starting the device controller.

  For more information on logging, see "Setting Parameters for Logging" on page 139.

- FieldMap.xml

  Defines field maps that the device controller may use. A field map maps logical field names to specific tag memory addresses.

All the configuration files are stored on the IF61 in the /home/developer/edgeware/sap directory.

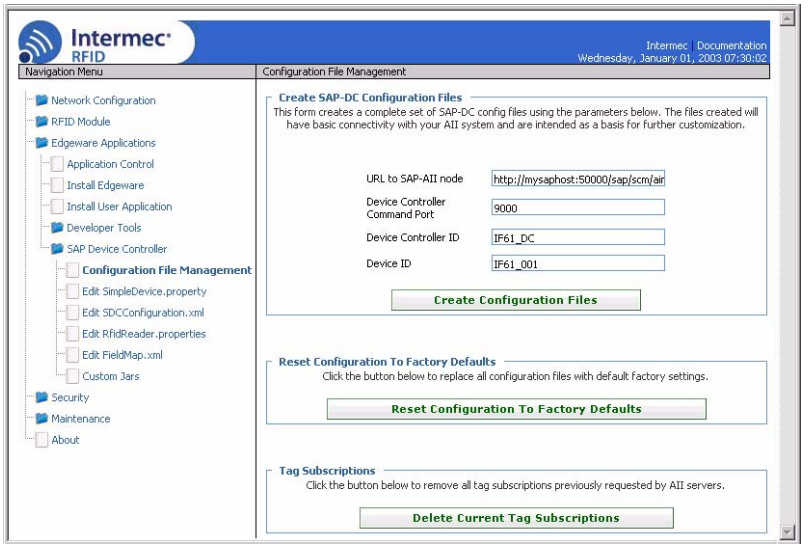
Creating Configuration Files

You can generate a complete set of SAP-DC configuration files via the web browser interface. The files can then be further customized for your system.

To create SAP-DC configuration files

1. Open a web browser interface to the IF61. For help, see "Using the Web Browser Interface" on page 10.

2 From the menu, choose **Edgeware Applications** > **SAP Device Controller**. The Configuration File Management screen appears.



3 In the **Create SAP-DC Configuration Files** box, enter settings as needed. For more information, see the next table.

4 Click **Create Configuration Files**. The files are created. Settings in the new files become active the next time the device controller starts.

SAP-DC Configuration File Settings Descriptions

Setting	Description
URL to SAP-AII node	URL of the SAP-AII node that this device controller connects to.
Device Controller Command Port	TCP port on which the device controller accepts SAP communications. Default is 9000.
Device Controller ID	Name of this device controller in SAP-AII.
Device ID	Name of this device in SAP-AII.

After the files are created, you can edit them via the web browser interface. For help, see the next section.

Editing the Configuration Files

To edit the configuration files, you can access the files via the web browser interface. If you make changes to the files, the changes take effect when you restart the device controller.

Follow the next procedure to edit the SAP-DC configuration files. To restore the configuration files to default values, see "Restoring the Default Configuration Files" on page 127.

To edit the configuration files

1. Open a web browser interface to the IF61. For help, see "Using the Web Browser Interface" on page 10.
2. From the menu, choose **Edgeware Applications** > **SAP Device Controller** and then choose one of the links to open a text editor for that file:
   - Click **Edit SimpleDevice.property** to change logging options or to redirect the device controller to read its configuration from a file other than SDCConfiguration.xml. For more information, see "Setting Parameters for Logging" on page 139.
   - Click **Edit SDCConfiguration.xml** to define additional readers or AII receiver nodes, or to create and customize data processor pipelines.

     For more information on the SDCConfiguration.xml file, see "About the SDCConfiguration XML File" on page 127.

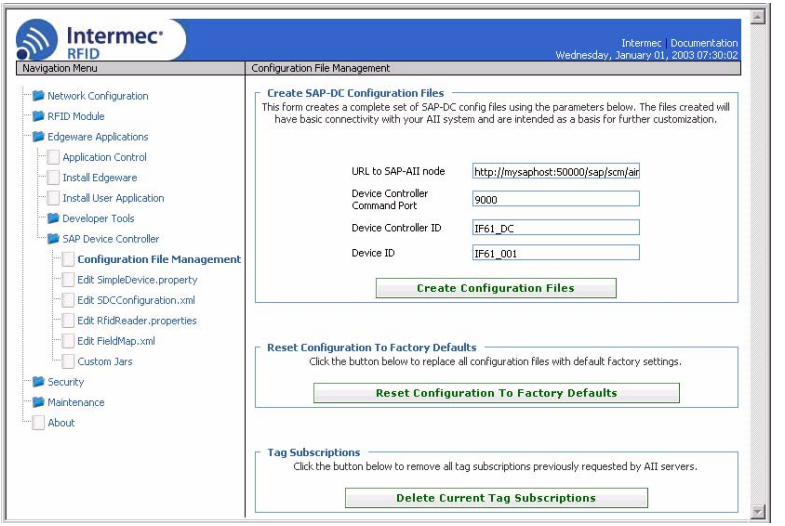
     For more information on data processor pipelines, see "Using the Data Processors" on page 143.
   - Click **Edit RfidReader.properties** to change configuration information for readers controlled by the device controller. For more information, see "About the RfidReader.properties File" on page 133.
   - Click **Edit FieldMap.xml** to change the mapping of logical field names to concrete RFID tag memory addresses.
3. Click **Activate Changes** to save your changes. Settings become active the next time the device controller starts.

Restoring the Default Configuration Files

Follow the next procedure to restore the default SAP-DC configuration files on the IF61.

To restore the default SAP-DC configuration files

1. Open a web browser interface to the IF61. For help, see "Using the Web Browser Interface" on page 10.
2. From the menu, choose **Edgeware Applications** > **SAP Device Controller**. The Configuration File Management screen appears.



3. Click **Reset Configuration to Factory Defaults**. The device controller configuration files are reset to defaults. The changes become active when you restart the device controller.

About the SDCConfiguration XML File

This file defines settings that determine how event data is transmitted to the SAP-AII server. These settings are described next.

Controller ID

The Controller element has an ID attribute that should contain the ID of this device controller in the SAP system. For example, UNLOAD_GATE_IF61 is the controller ID attribute in this XML fragment:

```
<Configuration xmlns:opt=”c:\”>
   <Controller id=”UNLOAD_GATE_IF61” description=”Receiving Gate -
    Intermec IF61 Fixed Reader”>
      <ReceiverList>
```

HTTPServer

This element specifies the port on which SAP-DC will accept commands from AII servers.

Element	Description
port	Port number to accept commands on.
timeout	Socket accept timeout value (in ms).

This example sets the port to 9000 and sets a timeout value of 2 seconds:

```
<Controller id="__CONTROLLER__" description="Intermec Fixed Reader">
<HttpServer port="9000" timeout="2000"/>
<ReceiverList>
```

ReceiverList

This element specifies a list of destinations that receive RFID tag events from the device controller. Each Receiver element defines one destination, which is generally an SAP-AII node, and contains an id attribute that identifies the receiver. Other parts of the SDCConfiguration file may refer to this attribute. A receiver element also includes option list elements and a MessageTransformer element, which are described in the next table.

ReceiverList Element Descriptions

Element	Description
opt:Name	Name of the receiver. This name will be displayed in logs.
opt:URL	URL that receives tag event data when transmitted by the controller. For SAP-AII nodes, this is usually `http://mySAPserver:50000/sap/scm/aim`
MessageTransformer	Stores the name of the software component that formats messages transmitted to this receiver. Leave this setting at the default.

In the sample XML below, the Receiver element defines the SAP-AII node and defines the receiver id as “rec1”.

```
<ReceiverList>
   <Receiver id=”rec1” protocol=”HTTP” description=”SAP AII NODE”
      <OptionList>
         <opt:Name>SDCReceiver</opt:Name>
         <opt:URL>http://136.179.176.37:8080/DummyServlet</opt:URL>
         <opt:Port>9000</opt:Port>
         <opt:Synchronization>asynchronous</opt:Synchronization>
      </OptionList>
      <MessageTransformer>
<APIImplementationClass>com.sap.device.controller.messaging.
XMLTransformer</APIImplementationClass>
      </MessageTransformer>
   </Receiver>
</ReceiverList>
```

OutboundQueuing

This element specifies settings for queuing of messages to be sent to AII. This prevents the loss of messages during a temporary network outage.

OutboundQueuing Element Descriptions

Element	Description
maxQueueSize	Maximum number of messages that may be queued for a receiver. If this limit is reached, the oldest messages are deleted without being sent. Since all messages in the queue consume memory, setting this limit arbitrarily high could cause an out of memory situation that SAP-DC may not recover from. Set this value to the expected number of messages that would be sent during a reasonable network outage for your usage scenario.
messageTimeToLive	Specifies the maximum amount of time (in ms) that a message remains in the queue. Messages that expire in the queue are deleted without being sent. Choose a value that is consistent with your usage scenario.

This example sets the maximum queue size to 1000 messages and the message "time to live" to 60 minutes.

```
</ReceiverList>
<OutboundQueuing maxQueueSize="1000" messageTimeToLive="3600000"/>
<ReaderList retryInterval="10">
```

ReaderList

This element defines the readers that the controller manages. The Reader id attribute defines the name of the IF61 in the SAP system. The LogicalName value is the name assigned to the reader in the RfidReader.properties file.

In the sample XML below, the IF61 name in the SAP system is "Fixed_Reader_18":

```
<ReaderList retryInterval=”10”>
   <Reader id=”Fixed_Reader_18” description=”Reader”>
      <LogicalName>IF61_reader1</LogicalName>
   </Reader>
</ReaderList>
```

To define more than one reader, add the additional readers to the reader list as shown in the next example.

```
<ReaderList retryInterval="10">
   <Reader id="Fixed_Reader_A" description="ReaderA">
      <LogicalName>IF61_reader1</LogicalName>
   </Reader>
   <Reader id="Fixed_Reader_B" description="ReaderB">
      <LogicalName>IF61_reader2</LogicalName>
   </Reader>
</ReaderList>
```

FieldMap

This element defines the location of the field map definitions, and generally points to the FieldMap.xml file in the home/developer/cd/config directory on the IF61. The defaultTable attribute specifies which Table element in the .xml file is used to map RFID tag fields. In the next example, the defaultTable is defined as "Intermec".

```
<FieldMap defaultTable="Intermec">file:config/FieldMap.xml</FieldMap>
```

ExtensionCommandHandler

This element defines the software component that processes VendorExtension commands from receivers. Do not change this element.

ProcessorChainList

This element defines the data processors of your system and how they are linked together. For more information, see "Using the Data Processors" on page 143.

The ProcessorChainList contains a DataProcessorList and a LinkList. The DataProcessorList element contains a list of data processors that the system contains. Each data processor is defined in a DataProcessor element as shown in this example:

```
        <DataProcessor id="agg" description="Aggregation">
          <APIImplementationClass>
com.sap.devicecontroller.core.dataprocessors.TimeFixedSizeAggregator
          </APIImplementationClass>
          <OptionList>
            <opt:TimerInterval>1000</opt:TimerInterval>
            <opt:MaxCount>1000</opt:MaxCount>
          </OptionList>
        </DataProcessor>
```

About the DataProcessor Element

A DataProcessor element has an id attribute used to refer to this data processor in other parts of the xml file. It also contains two subelements as described next:

DataProcessor Subelement Descriptions

Subelement	Description
APIImplementationClass	Specifies the Java class that implements the data processor. Data processor implementations are generally in the com.sap.devicecontroller.core.dataprocessors package. For a complete list of available data processors, see the SAP documentation.
OptionList	A list of configuration options that the data processor uses to determine its behavior. The available options and their effects are specific to each data processor implementation. By convention, the name of each option element in the option list is prefaced with “opt:”.

About the LinkList Element

The LinkList element defines how the data processors are connected together and includes two subelements:

LinkList Subelement Descriptions

Subelement	Description
ToDP	Specifies the data processor that events are coming from. Use the DataProcessor element ‘id’ attribute to specify a data processor.
FromDP	Specifies the data processor where events are going. Use the DataProcessor element ‘id’ attribute to specify a data processor.

The device controller default configuration specifies a sample pipeline. Make sure that ReaderIDs specified in ProcessorChainList match the Reader ids of the reader definitions in ReaderList as shown in the next example.

```
<ReaderList retryInterval="10">
   <Reader id="Fixed_Reader_18" description="Reader">
      <LogicalName>IF61_reader1</LogicalName>
   </Reader>
</ReaderList>
      .
      .
      .
<ProcessChainList>
   <DataProcessorList>
      <DataProcessor id="lp" description="LowPassFilter">
<APIImplementationClass>com.sap.devicecontroller.core.dataprocessors
.LowPassFilter</APIImplementationClass>
        <OptionList>
          <opt:ReaderID>Fixed_Reader_18</opt:ReaderID>
          <opt:TimerInterval>500</opt:TimerInterval>
        </OptionList>
      </DataProcessor>
```

About the RfidReader.properties File

This .xml file defines properties specific to the IF61 RFID module. RfidReader.properties.xml must reside in the /home/developer/dc directory on the IF61.

The next table lists properties you can set for BRI implementation. For more information on reader-specific properties, see the *Basic Reader Interface Programmer's Reference Manual* (P/N 937-000-xxx).

RfidReader.properties Element Descriptions

Element	Default	Description
Name	-	(Required) Defines the name of this reader. Used in the main XML configuration file as "LogicalName" to reference this reader. You can define the properties for more than one reader. For more information, see "Defining Properties for More than One Reader" on page 138.
Classname	-	(Required) Sets the LLI Java implementation class for this reader. Always use com.sap.readerImplementations.intermec.IntermecBRIReader.

RfidReader.properties Element Descriptions (continued)

Element	Default	Description
readerAddress	-	(Required) Specifies the IP address of the reader. If the SAP device controller is running on the reader directly, set to localhost or 127.0.0.1.
readerPort	-	(Required) Specifies the TCP/IP port to use for the BRI interface. Set to 2189.
pollingInterval	1000 ms	Sets the interval (in ms) at which the device controller requests tag data from the reader when tag identification is active. Longer intervals are more efficient but may cause delays in reporting tag arrivals. This value should be set as high as your usage scenario tolerates.
tagID.type	EPC	Defines the type of tag to be read: **EPC**: EPC tag ID stored on the tag in the standard location for that tag type. **ISO**: For UCODE 1.19 tags, this is the ISO tag ID, stored in the standard ISO tag ID location. For EPC Class 1 Gen 2 tags, the TID field is returned as the tag ID. **CUSTOM**: ID is stored in a customer-defined area in user memory on the tag. The tagID.address and tagID.length properties determine where the ID is stored on the the tag.
tagID.address	0	(Optional) Defines the memory address where the tag ID is stored. This can be used when some ID other than the manufacturer-set tag ID is desired. Set tagID.type to CUSTOM to define tagID.address. Use an integer to specify the memory address for ISO tag types. For EPC Class 1 Gen 2 tags, specify the address as <memory bank>:<memory address>. For example, use “3:15” to choose memory bank 3 at address 15.
tagID.length	8	(Optional) Sets the length of the tag ID. Set tagID.type to CUSTOM to define tagID.length.
logFile	-	(Optional) Specifies the file name that BRI logs should be written to. If not set, no BRI logging occurs.
output.use	0	(Optional) Set to 1 to use GPIO output ports to indicate the operation the reader is performing.

RfidReader.properties Element Descriptions (continued)

Element	Default	Description
output.mode.inactive	0	(Optional) When output.use=1, the outputs are set to this value when the reader is inactive.
output.mode.readingNoTags	0	(Optional) When output.use=1, the output ports are set to this value when the reader is reading and no tags are found in the field.
output.mode.reading	0	(Optional) When output.use=1, the output ports are set to this value when the reader is reading and tags are found.
output.mode.writing	0	(Optional) When output.use=1, the output ports are set to this value when the reader is writing to a tag.
idTries	2	(Optional) Sets the ID tries.
readTries	3	(Optional) Sets the Read tries.
writeTries	3	(Optional) Sets the Write tries.
selectTries	1	(Optional) Sets the Select tries.
unselectTries	1	(Optional) Sets the Unselect tries.
lockTries	254	(Optional) Sets the Lock tries.
initTries	1	(Optional) Sets the Initialization tries.
antennaTries	3	(Optional) Sets the Antenna tries.
antennas	1,2,3,4	(Optional) Sets the antennas to be used and the firing sequence for those antennas.
tagType	EPCC1G2	Defines the type of tags to be read: **G1**: ISO Class 1 Gen 1 tags **G2**: ISO Class 1 Gen 2 tags **UCODE119**: Phillips v1.19 tags **EPCC1G2**: EPC Class 1 Gen 2 tags **MIXED**: Mixed groups of tags
identifyStart.mode	Continuous	Determines when tag identification starts: • None - no identification occurs • Continuous - identification is always active • Periodic - identification starts at regular intervals • GPITrigger - identification starts in response to a GPI trigger
identifyStart.trigger	-	Name of the GPITrigger that starts tag identification. Valid only when identifyStart.mode is set to GPITrigger.

RfidReader.properties Element Descriptions (continued)

Element	Default	Description
identifyStart.time	-	Sets the delay time (in ms) between successive identification starts. Valid only when identifyStart.mode is set to Periodic.
identifyStop.mode	None	Determines when tag identification stops. Choose from: • None - identification never stops • Periodic - identification stops at a fixed time after identification starts • GPITrigger - identification stops in response to a GPI trigger.
identifyStop.trigger		Name of the GPITrigger that stops tag identification. Valid only when identifyStop.mode is set to GPITrigger.
identifyStop.time	-	When identifyStop.mode is set to Periodic, this value sets the fixed amount of time (in ms) that tag identification continues after identification begins. When identifyStop.mode is set to GPITrigger, this value sets the longest amount of time that tag identification is allowed to continue before stopping. When identifyStop.mode is set to None, this value is ignored.
additionalReadFieldMapper	Intermec	Name of the FieldMap table used to resolve additional read field names into concrete tag memory addresses.
additionalReadFields	-	Names of fields from the field map to be retrieved along with the tag ID during identification. Use this as a high performance alternative to using an event pipeline with a SelectedFieldEnricher data processor. In this case, the processor may continually interrupt continuous identification, affecting reader performance.
trigger*n*.name	-	Name of the trigger. For more information, see “About the triggern Properties” on page 137.
trigger*n*.mask	15	Bit mask applied to the GPI lines. Determines which input lines were examined by this trigger. Default is 15 (all lines are examined). For more information, see “About the triggern Properties” on page 137.

RfidReader.properties Element Descriptions (continued)

Element	Default	Description
trigger*n*.value	-	GPI data value (after applying the mask) that fires the trigger. For more information, see "About the triggern Properties" on page 137.
trigger*n*.filter	150	Delay time (in ms) after the trigger fires before the trigger can fire again. Use for signal debouncing. For more information, see "About the triggern Properties" on page 137.
trigger*n*.sendtodps	0	Determines if GPI Trigger events are sent into the reader's data pipeline. A non-zero value causes events to be forwarded into the pipeline. Default is 0 (events are not forwarded). For more information, see the next section, "About the trigger*n* Properties."
GPIOValue.green	-	(Optional) Sets the value of the GPIO output lines in response to a GREEN ExtensionCommand.
GPIOValue.yellow	-	(Optional) Sets the value of the GPIO output lines in response to a YELLOW ExtensionCommand.
GPIOValue.red	-	(Optional) Sets the value of the GPIO output lines in response to a REDExtensionCommand.

Note: To handle custom ExtensionCommand strings, more GPIOValue.xxx properties can be added. The command string name must be in lowercase characters in the .xml file.

For example, to make the controller respond to a BUZZER ExtensionCommand by setting GPIO output lines to 7, add this property: `GPIOValue.buzzer=7`

About the trigger*n* Properties

You can define up to 10 different triggers for a given reader. The trigger*n* properties function as groups where *n* is an integer between 0 and 9 that defines the properties for a single trigger. This example defines a trigger named DIRSWITCH that fires when a value of 1 appears on the GPI lines. When the trigger fires, a GPITrigger event is sent into the reader's data processor pipeline.

Example

```
reader.intermecBRI.trigger1.name=DIRSWITCH
reader.intermecBRI.trigger1.mask=15
reader.intermecBRI.trigger1.value=1
reader.intermecBRI.trigger1.filter=100
reader.intermecBRI.trigger1.sendtodps=1
```

Defining Properties for More than One Reader

If you have listed more than one reader in the SDCConfiguration.xml file, you define properties for each reader in the RfidReader.properties file as follows.

At the top of the file, the `readers` property specifies a comma delineated list of readers whose properties are defined in the file, as shown in this example:

```
readers=intermecBRI,intermecBRI2,intermecBRI3
```

This field is used to locate the prefixes that prepend each property in the RfidReader.properties file, and associates those properties with the appropriate reader.

For each reader defined, the .name property must match the LogicalName property assigned to that reader in the SDCConfiguration.xml file.

The next example shows how properties might be defined for three readers:

```
readers=intermecBRI,intermecBRI2,intermecBRI3

reader.intermecBRI.name=IF61_reader1
reader.intermecBRI.classname=com.sap.readerImplementations.intermec.
IntermecBRIReader
reader.intermecBRI.readerAddress=136.179.176.30
.
.
reader.intermecBRI2.name=IF61_reader2
reader.intermecBRI2.classname=com.sap.readerImplementations.intermec
.IntermecBRIReader
reader.intermecBRI2.readerAddress=136.179.176.36
.
.
.
reader.intermecBRI3.name=IF61_reader3
reader.intermecBRI3.classname=com.sap.readerImplementations.intermec
.IntermecBRIReader
reader.intermecBRI3.readerAddress=136.179.176.37
```

Setting Parameters for Logging

The SimpleDevice.property file sets parameters for logging. The SAP device controller uses the SAP logging API. There are two types of logs:

- Traces (LOCATION), for developers to use when debugging
- Logs (CATEGORY), for administrators monitoring regular operation

You can define a log level and format for each type. Logging can be done to the console, a file, or both. You can also log to a rotating set of files instead of a single file.

For the IF61 SAP device controller, Intermec recommends using the /tmp directory (or a subdirectory thereof) for best performance.

The next example shows a sample SimpleDevice.property file.

```
URL=file:config/SDCConfiguration.xml
LOCATION_LEVEL=ALL
LOC_TYPE=BOTH
LOC_FILENAME=/tmp/dc%g.trc
LOC_MAXFILESIZE=32000
LOC_NO_OF_FILES=10
LOC_FORMATTER=TRACE
CATEGORY_LEVEL=NONE
CAT_TYPE=FILE
CAT_FILENAME=/home/developer/sap/admin%g.log
CAT_MAXFILESIZE=32000
CAT_NO_OF_FILES=10
CAT_FORMATTER=TRACE
```

Logging parameters are described in the next table.

Logging Parameter Descriptions

Parameter	Description
LOCATION_LEVEL, CATEGORY _LEVEL	Sets the type of values to be logged: ALL, DEBUG, PATH, INFO, WARNING, ERROR, FATAL, NONE
LOC_TYPE, CAT_TYPE	Sets the location of the logging: FILE, CONSOLE, or BOTH
LOC_FILENAME, CAT_FILENAME	Sets the name of the log file. Required if LOC_TYPE is set to FILE or BOTH. Use the format <filename>.
LOC_MAXFILESIZE, CAT_MAXFILESIZE	Sets the maximum size of the logfile. Use the format <integer>. Default is FileLog.NO_LIMIT. Required only if LOC_TYPE is set to FILE or BOTH.

Logging Parameter Descriptions (continued)

Parameter	Description
LOC_NO_OF_FILES, CAT_NO_OF_FILES	Sets the number of logfiles if you want to log to more than one file. Use the format <integer>. Default is FileLog.NO_CNT. Required only if LOC_TYPE is set to FILE or BOTH.
LOC_FORMATTER, CAT_FORMATTER	Sets the format for the logfile entries: XML, LIST, or TRACE.

About Tag Subscriptions

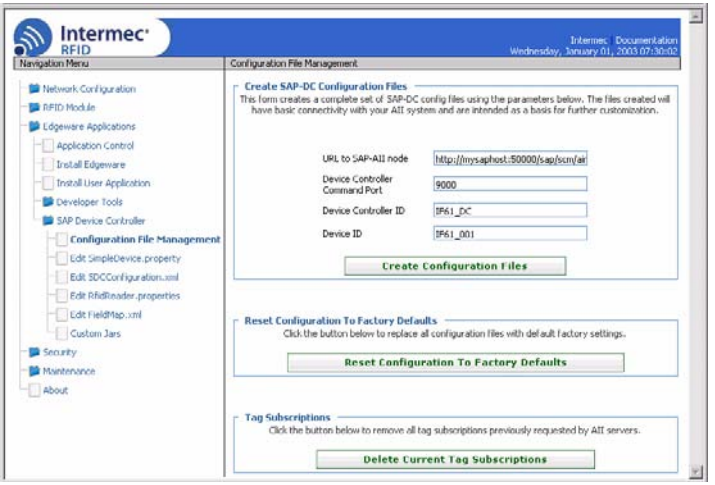
SAP-AII 4.0 provides a feature by which AII can command device controllers to begin sending tag data from a particular reader to a particular AII node using a specified tag data filtering scheme. This process is called creating a tag subscription. These subscriptions persist across reboots of the reader.

You can use the web browser interface to delete any tag subscriptions previously placed on the IF61 by the SAP-AII server.

Note: The current defined tag subscriptions are written to the LOCATION log at application startup if debug logging level is used. For more on tag subscription definitions, see the AII-DC Protocol specification document.

To delete tag subscriptions

1. Open a web browser interface to the IF61. For help, see "Using the Web Browser Interface" on page 10.
2. From the menu, choose **Edgeware Applications** > **SAP Device Controller**. The Configuration File Management screen appears.



3 Click **Delete Current Tag Subscriptions**. The subscription file is deleted and the change take effect when you restart the device controller.

Using Custom .jar Files

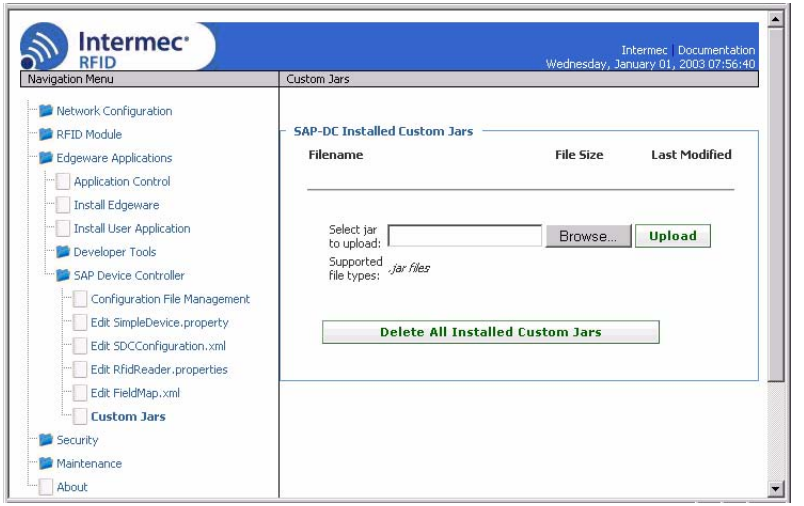
You can create custom Java .jar files to add custom data processor and transformer classes to the device controller.

Install or delete custom .jar files using the web browser interface.

To load or delete custom .jar files

1 Open a web browser interface to the IF61. For help, see "Using the Web Browser Interface" on page 10.

2 From the menu, choose **Edgeware Applications** > **SAP Device Controller** > **Custom Jars**. The Custom Jars screen appears.



3 To install .jar files, click **Browse**. Follow the prompts to browse to the location of the .jar files, and then click **Upload** to install the files on the IF61.

Or, click **Delete All Installed Custom Jars**. Any previously installed custom .jar files are deleted.

Changes become active after you restart the device controller.

Upgrading the SAP Device Controller

You use the web browser interface to install new SAP device controller firmware. When you install new firmware, your current configuration files are saved so you do not have to reconfigure the device controller.

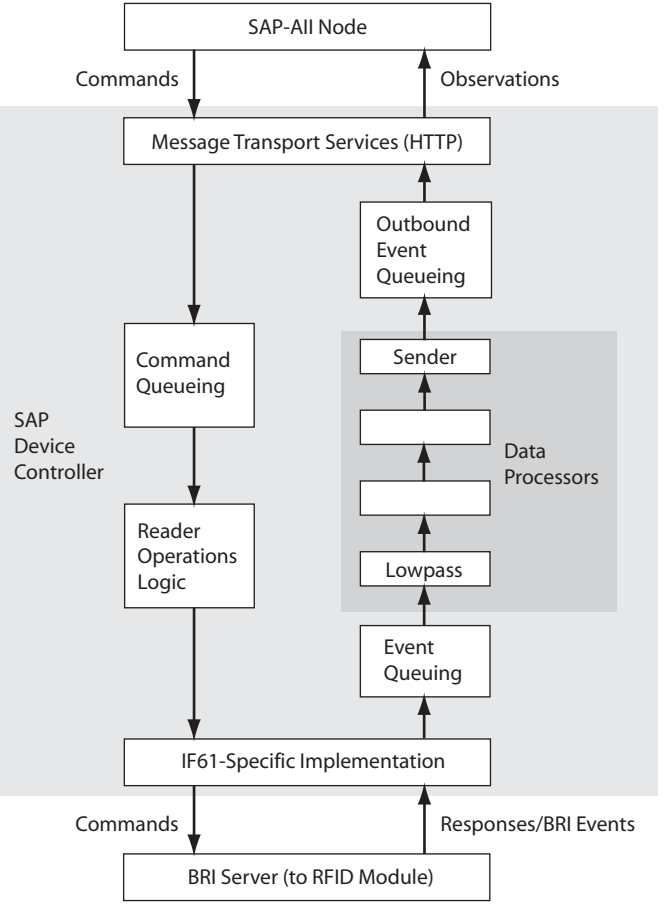
For more information on upgrading or installing the device controller, see "Upgrading or Installing Edgeware Applications" on page 47.

For information on uninstalling the device controller, see "Managing Applications" on page 45.

Using the Data Processors

SAP defines a data processor as a simple component implementing a special function. Data processors process events from RFID readers asynchronously and send the processed events to SAP-AII. Data processors can be arranged flexibly and added as necessary to add sophisticated event filtering to your system.

The next diagram shows the relationship of data processors to the system with regard to command and data flow:



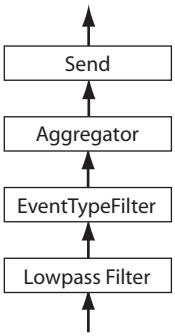
Data Processor Flow Chart: *This diagram shows how data processors are integrated into SAP command and data flow.*

Data Processor Types

There are five main types of data processors:

- **Enrichers** read additional data from the tags (or other sources) and add this data to the data structure of the event.
- **Writers** write data to or change data on the tags.
- **Filters** filter out certain events according to some criteria (for example, they could filter out all events coming from case tags, or clean out false "tagDisappeared" events ("low pass filter").
- **Buffers** buffer the events for later processing and keep an inventory of tags currently in the field.
- **Aggregators** aggregate several events into a single event so they can be transmitted in a single message, thereby improving system efficiency.
- **Senders** transform the internal data structure with the help of a Transformer and sends the information to registered recipients (generally SAP-AII).

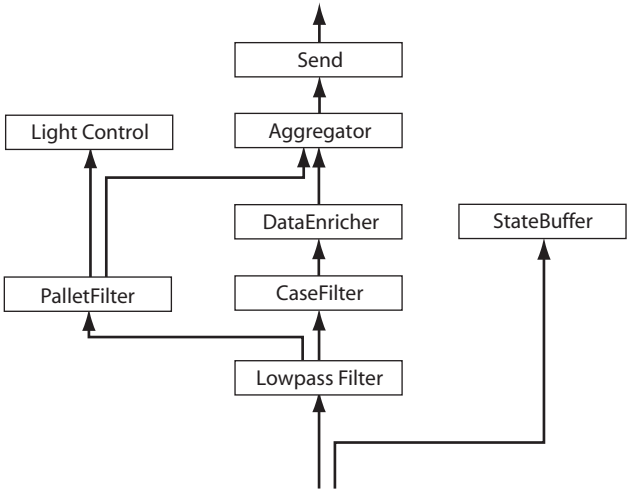
To achieve the desired functionality (filtering, aggregation, etc.), data processors are arranged into chains or meshes. A processor receives events, performs its function, and passes the events on to the next processor. The next illustration shows a simple data processor chain as specified in the default configuration:



Default Data Processor Chain

This chain passes events through a low pass filter (to remove false "disappeared" events), filters out unwanted events using the EventType filter, bundles events together using the aggregator, and finally transmits the bundled events to SAP-AII using a Send data processor.

Data processor chains need not be linear. The theoretical example below processes tag events from pallets and cases differently. Pallets can set lights on a light tower while events from cases are augmented with user data from the tags (using a data enricher). This example assumes you have a tag data scheme set up so you can differentiate pallets and cases using the tag data.



Nonlinear Data Processing

Standard Data Processors

All data processors are implemented as Java classes in the com.sap.devicecontroller.core.dataprocessors package.

CheckReader

This processor checks if a reader is still working.

- It periodically calls `identify()` to check all specified readers. If the call does not throw an exception, the reader is considered to be working properly. Otherwise the reader is disconnected and added to the ReaderErrorManager singleton.
- Received RfidEvents and DataProcessorEvents are forwarded to the next data processors in the chain. However, events where the tag ID equals the check tag ID are filtered out.

All tag IDs returned from `identify()` (except the check tag ID) are packaged in a DataProcessorEvent and forwarded.

DuplicateFilter

This class filters all events that appear or disappear twice (or more times) in a row. If the event is of type "APPEARED" or "DISAPPEARED", and received twice, the second event is ignored. For example, DuplicateFilter can be used when the Device Controller is monitoring a gate consisting of two or more physical readers that form one logical read point.

SimpleDuplicateFilter

Filters out all duplicate tags of the same type (appeared/disappeared), regardless of which reader the tags came from. This simple duplicate filter does not maintain a history of past events and only filters duplicates in the current event message it is processing. Use SimpleDuplicateFilter inside a chain after an aggregator data processor.

EPCEnricher

A special type of SelectedFieldEnricher that reads an EPC from the user memory of the tag and replaces the manufacturer tag id with the EPC value. Used with non-EPC tags.

EqualizeTimeStamp

Equalizes the time stamp. The time stamp of all RfidEvents is set to the value of the time stamp of the enclosing DataProcessorEvent. This is useful when grouping single events together to simplify processing on the AIN side and when detailed millisecond-level time stamps are not required.

EventTypeFilter

Filters out RFID events based on type. Either "APPEARED" or "DISAPPEARED" events are filtered out.

GpiTriggerSwitchableSend

Transforms RFID events into XML and sends this information to registered receivers. Additionally, the action string of the resulting XML can be changed based on GPI trigger events received from the pipeline. A map defined by configuration options associating GPI trigger names with corresponding action strings determines which action string is used.

GpiTriggerSwitchableSend processors do not forward GPI Trigger events to receivers.

HierarchyBuilderSend

Builds RFID events into simple hierarchies (for example, the building of a pallet with information about the cases contained on the pallet).

The following assumptions are made:

- The system consists of a simple hierarchy of one single container object (such as a pallet), containing an unlimited number of contained objects (for example, cases).
- Two different readers are used to read the RFID tags of containers and contained objects.
- No new container object appears before the previous one has disappeared (physically impossible for this to happen).
- No contained objects appear if there is no container object. Should this happen, the contained objects are assigned to the next visible container. The error condition is logged.

The hierarchy is built according to the following algorithm:

- (Start state) No events have been received.

- When a container "appeared" event is received, the building process starts.
- All following "appeared" events for contained objects are assigned to the current container.
- When a "disappeared" event for the same container is received, the building of the current container is finished. The data is transformed into a message by the assigned transformer object and sent out.

More complex hierarchies, or the association with delivery or order numbers, can only be done at a higher level such as an AutoID Node.

LowPassFilter

Shortly buffers events to filter out false "disappeared" events. This data processor is usually the first one in a chain.

Note: This filter is deprecated. Instead, increase the polling interval in the reader properties to avoid false disappeared events.

OneAppearanceFilter

Filters tag appearance and disappearance events so that each tag ID appears and disappears exactly once.

SelectedFieldEnricher

Reads data from selected data fields of the tag and adds this data to the event. It uses the FieldNameMapper to map from logical field names to physical addresses on the tag.

Send

Transforms the internal event data structure into XML (using the configured transformer) and sends the information to registered receivers.

Send processors filter out GPI Trigger events and do not forward them to receivers.

SimplePackSend

This data processor does a simple packing operation assuming a single read point. A read point could be composed of several physical readers, but the algorithm regards them as one.

Like HierarchyBuilderSend, it builds RFID events into simple hierarchies. An example is the building of a pallet with information about the cases contained on the pallet.

The following assumptions are made:

- The system consists of a simple hierarchy of one single container, containing an unlimited number of contained objects.
- The first tag seen is interpreted as the container.
- No new container object appears before the previous one has disappeared (physically impossible for this to happen).
- No contained objects appear if there is no container object. Should this happen, the contained object is interpreted as a container. This situation cannot be recognized as an error.

How the hierarchy is built depends upon the option setting.

SimplePackSend processors filter out GPI Trigger events and do not forward them to receivers.

TagBitsFilter

Filters tag events based on the contents of the tag fields. You can specify a bit mask and value used to filter tags. TagBitsFilters can filter on the contents of any tag field defined in the field map including the EPC ID.

TagLogger

Logs detailed information about events encountered in the pipeline to the Location log file. Used for debugging data processor chains.

TimeFixedSizeAggregator

Aggregates several events into a single one. The aggregation is done during a configurable time interval or up to a configurable maximum number of events, whichever comes first. If no events are received during this interval, no event is forwarded.

About Transformers

The sender type data processors (Send, HierarchyBuilderSend) use a transformer to transform the internal event data structure into a message string and send the message out. The following transformers are available:

EPCPMLTransformer
Specialization of PMLTransformer, where the tag id is given in the EPC URN-notation. The tag IDs should be valid EPCs. Otherwise the numbers are reported as either epc.raw or empty EPCs.

MultiEPCPMLTransformer
Specialization of PMLTransformer, where the tag ID is given both as a hexadecimal string as well as in the EPC URN-notation, separated by a comma. The tag IDs must be valid EPCs. This transformer is mainly used for debugging.

PMLTransformer
Generates a message conforming to the PML Core 1.0 specification. Tag IDs are given as hexadecimal strings.

PMLTransformer2
Specialization of PMLTransformer that does not return a schema ID in XML messages. This creates XML compatible with SAP-AII version 4.0.

PMLTransformerAII4
Specialization of PMLTransformer that populates XML messages with EPC_1.30 schema IDs. This creates XML compatible with SAP-AII version 4.0.

ValidEPCPMLTransformer
Similar to EPCMLTransformer, where the tag ID is given in the EPC URN-notation. Non-valid EPCs are removed from the message and not reported. If no valid tags are in the event structure, no message is sent.

About Data Processor Options

You can set a variety of options for each data processor. One option applies to all processor types, some apply only to sender types, and others are specific to one data processor class.

Options for All Processor Types

These options apply to any data processor type (class: DataProcessor):

ReaderID
The ID of a reader from which RfidEvents are to be received. Used only if the data processor receives events directly from a reader.

Options for Send Processors

These options apply only to send processors (Send, GpiTriggerSwitchableSend, HierarchyBuilderSend):

ReceiverID
The ID of a receiver (AIN) where notifications are sent.

Transformer
The class name of the transformer to be used to transform the internal DataProcessorEvents into a message (for example, into PML Core).

InCommand
The command used in the PML Core message for "appeared" events. Default is null.

OutCommand
The command used in the PML Core message for "disappeared" events. Default is OUT.

Options for CheckReader

CheckParams
The ID of the reader to be checked (optionally, an ID of a check tag). The two values are separated by a comma, as in "ReaderID, CheckTagID". The CheckTagID is a hex string.

TimerInterval
The time (in seconds) between two reader checks. Default is 10.

Options for EPCEnricher

EPCFieldName
The logical field name where the EPC is stored. The mapping table used is defined with the parameter "MappingTable" of the SelectedFieldEnricher. Default is EPC.

Note that all options of the SelectedFieldEnricher are also valid for this data processor.

FilterBadTags
Boolean value indicating if tags where the EPC could not be read should be filtered out (true) or not (false). If set to false, the original tag ID is used as ID for tags that could not be read. Default is false.

Options for EventTypeFilter

FilterAppeared
Boolean value (true/false) indicating if "appeared" events should be filtered out. Default is false.

FilterDisappeared
Boolean value (true/false) indicating if "disappeared" events should be filtered out. Default is true.

FilterGpiTriggers
Boolean value (true/false) indicating of GPI Trigger events should be filtered out. Default is false.

Options for GpiTriggerSwitchableSend

trigger.<*name*>
The action string text that should be used when a trigger event from the trigger named <*name*> is encountered. There should be one option for each trigger of interest.

Options for HierarchyBuilderSend

ContainedObjectReader
The ID of the reader used for identifying contained objects (such as cases).

ContainerReader
The ID of the reader used for identifying the container object (such as a pallet).

InCommand
The command used to be used in the PML Core message. This is a redefinition of the "InCommand" parameter of the parent SendDataProcessor class. Default is PACK.

Options for SimplePackSend

SendTrigger
Defines when to trigger the sending of the packing message. If set to "Container", the message is sent as soon as the container tag disappears. If set to "All", then the message is sent when no more tags are seen. Default is Container.

RemoveTags

If set to true, tags that disappear are removed from the list (except the pallet). The risk of using this setting is that tags may be reported as "disappeared" due to a misread, although they are still in the field. Default is false.

InCommand

The command used to be used in the PML Core message. This is a redefinition of the the "InCommand" parameter of the parent SendDataProcessor class. Default is PACK.

Options for LowPassFilter

TimerInterval

The time (in milliseconds) to wait before a "disappeared" event is sent on. If an "appeared" event appears within this time interval, no events are sent on. Default is 100.

Options for OneAppearanceFilter

TimerInterval

Time interval during which duplicate tag appearance and disappearance events are ignored for a given tag ID. Events occurring after the expiration of the timer interval reset the timer and allow the tag to appear again (that is, the timer is reset and the tag may appear again only once during the interval).

MaxTagListSize

The data processor maintains a list of observed tags to keep track of appearances. This option specifies the size of this list. If the list size is reached, the oldest tag IDs are deleted (and thus are "forgotten" by the data processor, allowing the tag ID to appear again) to honor the maximum list size.

Options for SelectedFieldEnricher

AddField

Adds the logical field name of a data field that should be read. This option can be repeated multiple times.

ClearFields

Clears the list of data fields that should be read. Not necessary in complete configuration files.

MappingTable
The name of the mapping table for converting logical field names into physical memory addresses on the tag. The mapping tables are defined in the global field map.

RemoveField
Removes a logical field name from the data fields that should be read. This option can be repeated multiple times. Not necessary in complete configuration files.

Retries
The number of read retries performed if there was an error reading a data field.

Options for TagBitsFilter

FilterField
Defines the tag data that will be filtered on. The default value is "EPC", which uses the EPC tag ID. Note that when filtering on fields other than tag ID, the data must already be in the event passed on to this data processor. Thus, you must place a SelectedFieldEnricher data processor in your pipeline in front of this data processor to filter on user data fields.

FilterBitMask
Defines the bit comparison you want to make on the tag field. 1s and 0s indicate mandatory bit values. Xs mean "don't care". If the mask is smaller than the actual data, the extra data is not checked. If the mask is longer than the tag data, the tag event fails the comparison.

The mask can be specified in base-2 or in hexadecimal (prepend an H). For example, the filter mask `00110000XXXX00101111` can also be expressed as `H30x2F`.

Invert
A Boolean value that defines the filter effect. If false (default), only tag events that pass the bit filter are passed on in the pipeline. If true, only tag events that fail the bit filter are passed on in the pipeline.

Here is example XML showing use of the filter options:

```
<DataProcessor id="tfilter" description="TagIDFilter">
   <APIImplementationClass>
      com.sap.devicecontroller.core.dataprocessors.TagBitsFilter
   </APIImplementationClass>
   <OptionList>
      <opt:FilterBitMask>00110000XXXX0010</opt:FilterBitMask>
      <opt:Invert>false</opt:Invert>
   </OptionList>
</DataProcessor>
```

Options for TimeFixedSizeAggregator

MaxCount

The maximum number of events for the aggregation. All events are counted until this number is reached or until the maximum time interval since the first event has passed. Aggregated events within the message keep their original timestamp. Default is 100.

TimerInterval

The length of the time window (in milliseconds) for the aggregation. All events within this window are aggregated into a single message, unless the maximum number of events is reached first. Aggregated events within the message keep their original timestamp. Default is 10000.

GPITriggerBoundary

If present, this option causes the data processor to break out forwarding of events based on the arrival of GPI Trigger events. Events that arrive before the trigger are sent grouped in their own data processor event. Events arriving after a trigger are sent together with the trigger event itself.

Note that receiving a GPI Trigger event does not cause aggregation to stop. The timer and event limit logic still applies; it merely dictates the grouping of the events as they leave the data processor. This is useful in conjunction with the GpiTriggerSwitchableSend data processor.

Configuring SAP-AII for SAP-DC

The configuration of SAP-AII is beyond the scope of this manual, but here is some basic information to get you started. In SAP-AII you must define:

- a device controller.
- a device group for that controller.
- a device for that group.

You need to make sure that the device controller and device names specified in your SAP installation match the ones you specify in the device controller configuration files.

For help with creating configuration files, see "Creating Configuration Files" on page 124.

For help with editing configuration files, see "Editing the Configuration Files" on page 126.

About the SAP Device Controller URL

The URL that SAP-AII should use to send commands to the device controller is:

`http://<if61machinename>:<port>/SimpleDeviceController`

where:

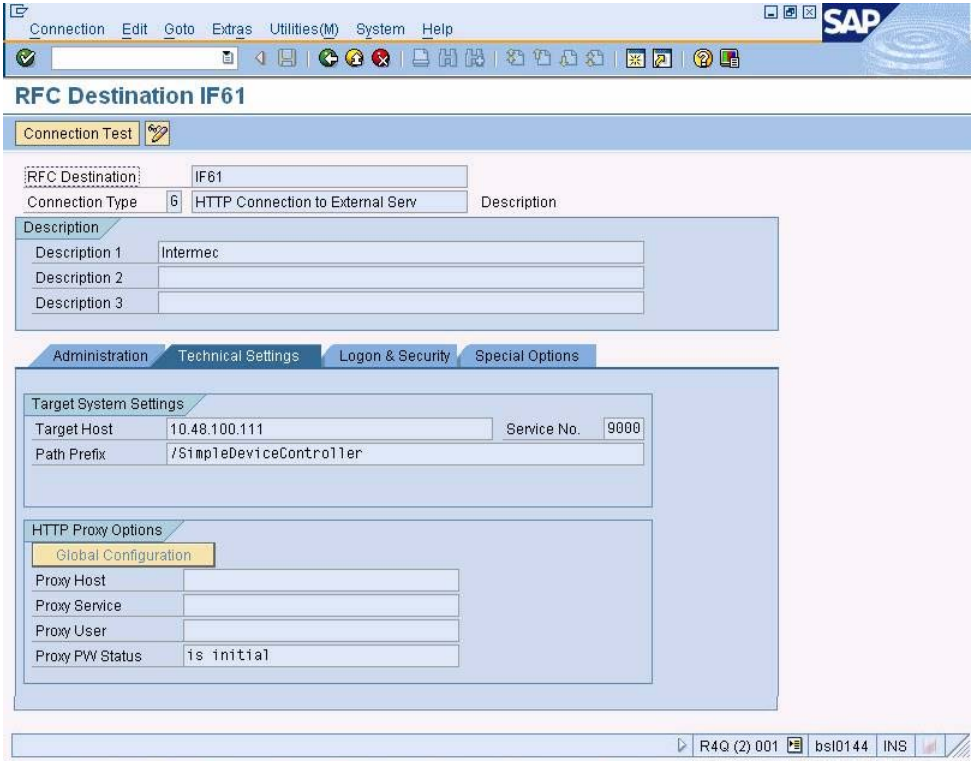
<*if61machinename*> is the IF61's IP address. Note that the device controller does not support DNS names, so you need to specify the raw IP address.

<*port*> is the port SAP-DC opens to accept commands (usually 9000).

For example, if the IF61 has IP address 192.168.1.12 and the controller listens on port 9000, SAP-AII should use the following URL to communicate with the device controller:

`http://192.168.1.12:9000/SimpleDeviceController`

The next illustration shows an example of configuring the URL in SAP-AII.



SAP-AII Sample Screen: *This example shows where to configure the URL for the IF61 in SAP-AII.*

Index

Symbols

A

B

C

S

T

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 935-011-001