Iris® Gateway

Masimo

Contents

About this Manual

This manual explains how to configure and use the Masimo® Iris® Gateway server and system. Important safety information relating to general use of the Iris Gateway appears in this manual. Read and follow any warnings, cautions, and notes presented throughout this manual. The following are explanations of warnings, cautions, and notes.

A warning is given when actions may result in a serious outcome (for example, injury, serious adverse effect, death) to the patient or user. The following is an example of a warning:

Warning: This is a sample of a warning statement.

A caution is given when any special care is to be exercised by the patient or user to avoid injury to the patient, damage to this device, or damage to other property. The following is an example of a caution:

Caution: This is a sample of a caution statement.

A note is given when additional general information is applicable. The following is an example of a note:

Note: This is a sample of a note.

Definitions

Vitals Out: The Iris Gateway is capable of sending POC device HL7 Vitals Out Message to a listener (IHE PCD-01)[1].

Vitals Out Listener: Is a system/device that is capable of receiving and processing HL7 Vitals Out Messages (IHE PCD-01)[1].

Alarm Reporting: The Iris Gateway is capable of sending POC Device Alarm to an Alarm Listener (IHE-PCD-04)[1].

Alarm Report Listener: Is a system/device that is capable of receiving and processing HL7 Alarm Messages (IHE PCD-04)[1].

ADT: A system used in hospitals to track the Admission, Discharge, and Transfer of patients throughout the facility.

Keep Alive: Is a periodic message sent between two entities to continuously check connectivity between the two entities.

[1] Refer to the *Integrating the Healthcare Enterprise IHE Patient Care Device (PCD) Technical Framework, Volume 1, IHE PCD TF-1, Profiles* document located at http://www.ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_TF_Vol1.pdf.

Product Description, Features and Indications for Use

Product Description

The Iris® Gateway can be used to connect and convert data from multiple patient monitoring devices and make it available to other systems and is part of the Hospital Automation™ portfolio.

Key Features

The Iris Gateway may consist of the following features:

- Support for up to 500 devices for Iris Gateway server and virtual machine.

- Support for up to 40 devices for Iris Gateway mini.

- Ability to communicate over a IEEE 802.11 wireless (2.4 & 5 GHz) or hard wired network

- HL7 Protocol Support

Indications for Use

The Masimo® Iris Gateway is intended to be used to connect and convert the data from multiple patient monitoring devices and make it available to other systems. Iris Gateway can be used in hospital or hospital like environments.

Safety Information, Warnings and Cautions

Safety Warnings and Cautions

Warning: Do not to place the Iris Gateway server where it may be accessible by patients.

Warning: Do not use Iris Gateway server if it appears or is suspected to be damaged.

Warning: Do not use unauthorized devices with the Iris Gateway server. Possible loss of performance and/or patient injury may result.

Warning: Do not place Iris Gateway server in any position that might cause it to fall on the patient.

Warning: Explosion hazard: Do not use Iris Gateway server in the presence of flammable anesthetics or other flammable substance in combination with air, oxygen-enriched environments, or nitrous oxide.

Warning: To protect against injury, follow the directions below:

- Avoid placing the device or accessories on surfaces with visible liquid spills.

- Do not soak or immerse the device in liquids.

- Use cleaning solutions only as instructed in this operator's manual

Warning: Do not use the Iris Gateway server during or near magnetic resonance imaging (MRI).

Performance Warnings and Cautions

Warning: The Iris Gateway system does not generate or manage alarms. It is intended as a connectivity solution. The standalone device's audible and visual alarms, used in conjunction with clinical signs and symptoms, are the primary sources for determining that an alarm condition exists.

Warning: Iris Gateway is only responsible for the communicating alarms to the hospital alarm management system. Once an alarm has been sent to the hospital alarm management system, per Masimo's network specifications, any failure to receive and transmit that alarm will be a result of an error caused by the hospital alarm management system.

Warning: Do not place containers with liquids on or near the Iris Gateway server. Liquids spilled on the Iris Gateway server may cause it to perform inaccurately or fail.

Caution: It is strongly recommended that the Iris Gateway "Keep Alive" messages be verified to be active and working properly on the hospital alarm management system before monitoring patients.

Caution: The Iris Gateway server is intended to operate across the facility's network. Unanticipated failure or alteration of network components (including but not limited to: disconnection or malfunctioning of a networking device/switch/router/ethernet cable) may result in loss of connectivity of the Iris Gateway server/system to other hospital systems. Altering or making changes to the Hospital Network should be done with proper knowledge.

Caution: Additional tests should be performed when any changes or modifications have been made to the hospital alarm management system.

Caution: The Quality of Service (QoS) of connectivity to the Point-of-Care (POC) Devices may be affected by:

- Network Failure

- Increased number of connected devices on the Network

- Modifications to the Network

- Presence of devices provided with radio transmitters

- Improper network configuration on POC

- Signal Priorities of the Network

- Latency

Caution: Network performance may be affected by changes in the network including the addition of additional network devices.

Caution: Use redundant network connections to ensure reliable network connectivity to the Iris Gateway server.

Caution: Utilize a back-up AC power source to minimize the interruption of service due to the loss of power to the Iris Gateway server.

Caution: To prevent tampering with the Iris Gateway server should be located in a secure location.

Caution: Carefully route power supply cords to minimize the accidental disconnection.

Caution: Do not place Iris Gateway server on electrical equipment that may affect the devices, preventing it from working properly.

Caution: To ensure proper system operation, always verify successful connection between Point of Care devices and Iris Gateway.

Note: Successful connection between Iris Gateway and a standalone device via Masimo Root's Iris port requires:

- The standalone device is correctly configured to output data.

- The standalone device is connected to Masimo Root via an authorized and approved Iris Adapter

- The standalone device is the correct make, model, and software version for the attached Iris Adapter.

- Masimo Root is connected to Iris Gateway and displays successful Iris connection to the standalone device.

Note: Iris Gateway sends all POC device alarms to the External Alarm Management System without applying any filters or delays.

Cleaning and Service Warnings and Cautions

Warning: Do not adjust, repair, open, disassemble, or physically modify the Iris Gateway server. Injury to personnel or equipment damage could occur. Return Iris Gateway server for servicing.

Warning: If the Iris Gateway server fails any part of the setup procedures or electrical safety tests, remove the device from operation until qualified service personnel have corrected the situation.

Warning: Do not autoclave, pressure sterilize, or gas sterilize Iris Gateway server.

Warning: Use cleaning solutions only as instructed in the operator's manual for the Iris Gateway server.

Note: Modifications to the Iris Gateway server's settings, and those of any components connected thereto, should be made by qualified personnel only.

Note: Iris Gateway server installation must be completed by Masimo or an authorized service department.

Compliance Warnings and Cautions

Warning: Do not attempt to repair or modify any part of the Iris Gateway server doing so may void the warranty or the authorization to use the Iris Gateway System components.

Warning: Disposal of product - Comply with local laws in the disposal of Iris Gateway server and/or its accessories.

Warning: When using devices with wireless features outside the United States, consideration should be taken to local government frequency allocations and technical parameters to minimize the possibility of interference to/from other wireless devices.

Warning: In accordance with international telecommunication requirements, the frequency band of 2.4 GHz and 5.15 to 5.25 GHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems.

Note: The Iris Gateway server has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

Chapter 1: Technology Overview

Introduction

The Iris Gateway can be used to connect and convert data from multiple patient monitoring devices and make it available to other systems.

Iris Gateway Modes (ADT, Vital Out & Alarm Reporter)

The Iris Gateway system has the following HL7 inbound and outbound interface support:

1. **Inbound:** The Iris Gateway can receive hospital HL7 ADT information for positive patient association to a connected Masimo device.

2. **Outbound:**

   - **Vitals Out Reporting:** The Iris Gateway is capable of periodically sending patient device data to other systems, like the hospital EMR.

   - **Alarm Reporting:** The Iris Gateway is capable of sending patient device alarm data to other systems, like the hospital alarm management system.

Patient Association

Patient association ensure the correct patient is associated with the correct device. There are three methods in which the Iris Gateway can associate the outbound HL7 data to the correct patient:

- **ADT Interface:** When a clinician admits a patient (associates a patient to a device) using ADT data, Iris Gateway can use the patient identifying information and location to ensure the device data is correlated with the correct patient.

- **Device Location:** A system administrator can specify a device's location to support workflows that use a static method of patient association. The Iris Gateway can output the device's location information as part of the outbound HL7 data.

- **Device Serial Number:** The Iris Gateway can output the device's serial number information as part of the outbound HL7 data.

Compatible Masimo Bedside Point of Care Devices

- Radical® Pulse Oximeter

- Radical-7® Pulse CO-Oximeter

- Rad-87® Pulse CO-Oximeter

- Rad-8® Pulse Oximeter
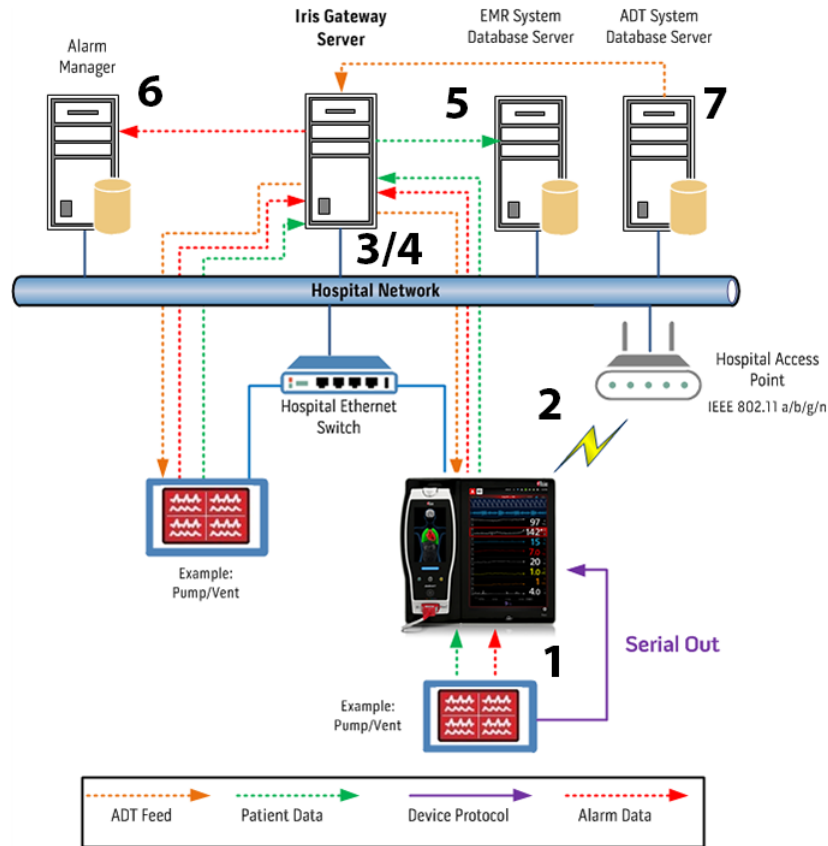
- Masimo Root®

- Radius-7® Pulse CO-Oximeter

Admit and Discharge via Masimo Root

Refer to Masimo Root Operator's Manual for complete information.

Chapter 2: System Components

The diagram below represents the Iris Gateway server and components. The Iris Gateway is able to receive data from Point of Care devices (POC) using their proprietary device communication protocol(s). The Iris Gateway can send POC device data and alarm data to other hospital systems via outbound HL7 interfaces. Iris Gateway is capable of receiving the parsing patient ADT information via an inbound HL7 interface.

Note: Iris Gateway is compatible with IEEE 802.11 a/b/g Hospital Access Point

1. The device (Pump/Vent shown in diagram above) is connected to the Masimo POC device (Masimo Root shown in diagram above) via an Iris Adapter cable. In some cases, devices may have built-in communication technologies which allow the device to communicate directly with the Iris Gateway.

2. Depending on the network configuration, the POC device communicates through a wireless link via Hospital Access Point(s), or hard wired to a switch.

3. The Wireless Access Point(s) transmit data through a Network Switch to the Iris Gateway server. The Access Point(s) connect to the Network Switch via standard network cable.

4. The Iris Gateway server is capable of communicating with the Wireless Access Points across the network.

5. The Iris Gateway is capable of communicating with the Hospital "Vital Out Listener" or "charting system" using the existing hospital wired or wireless network (example Electronic Medical Record System).

6. The Iris Gateway is capable of communicating with the Hospital Alarm Management System using the existing hospital wired or wireless network (example Enterprise Alarm Management System).

7. The Iris Gateway is capable of communicating with the Hospital ADT system using the existing hospital wired or wireless network.

Chapter 3: Iris Gateway Configuration

System Administration

Iris Gateway provides a configuration tool that system administrators can use to configure the Iris Gateway system. This section will describe all the configuration capabilities.

The tool is privileged based and allows access to the various configuration options based on the user's defined privileges.

Note: User privileges are defined by Masimo personnel during system implementation, not all privileges may be available to the user. Contact a Masimo representative for additional user privileges.

How to Access the Configuration Tool

There are two ways to access the configuration tool:

- **Direct Access:** Users who have physical access to the Iris Gateway system: After the server is powered on and fully booted, the system will prompt for a user name and password.

- **Remote Access:** Iris Gateway runs an SSH service (Secure Shell Protocol). Users can remotely login to the system using an SSH tool.

After authentication takes place, the Iris Gateway configuration tool will run and display the available configuration options the user has privilege to access.

Note: The Iris Gateway Configuration tool is a command line interface, the main method for interaction with the tool is via keyboard. When the following instructions state 'select' the user is to type the corresponding line # listed for each action they are trying to perform.

Configuration Menus

The Iris Gateway Configuration tool has two levels of menus:

- Main Menu

- Sub Menus

Main Menu

The main menu will be the first screen displayed when the system is accessed.

The main menu has five submenus:

1. **Application Configuration (Device & Location):** The options in this submenu will allow the user to add/modify/remove devices and associated locations of those devices.

2. **Application Configuration:** The options in this submenu will allow the user to: check the status of the HL7 inbound and outbound services, and restart the HL7 inbound and outbound services.

3. **Server & OS Configuration:** The options in this submenu will allow the user to perform configure server and OS level configuration options, like shutdown or/restart the Iris Gateway server, change the system IP address and more.

4. **HL7 Interface Outbound Configuration:** The options in this submenu allow the user to: configure the Iris Gateway outbound interface for HL7 vital signs device data reporting and HL7 alarm reporting, configure the listening/recipient appliance IP address and /port, change the frequency of message updates, change keep alive message frequency, and many more.

5. **HL7 Interface Inbound Configuration:** The options in this submenu will allow the user to configure the Iris Gateway inbound interface for patient ADT (Admit, Discharge and Transfer) information.

Application Configuration (Device & Location)

The Application Configuration (Device & Location) configuration options allow the user to add, modify, and remove devices and associated device locations.

To navigate to the Application Configuration (Device & Location) Menu, perform the following:

1. From the Main Menu, select option **#1 – Application Configuration (Device & Location)** and press 'Enter'.

Location Operations

These options allow the user to add, modify, remove, and display locations associated with devices in the system. Added location can be assigned to a device (see **Device Operations** on page 20). Location information will be included as part of the Iris Gateway HL7 outbound messages. The HL7 message listener/recipient services (like the EMR) can use the device location information to map data.

When configuring a location the following information is required:

1. Floor

2. Point of Care

3. Room

4. Bed

Modify Location

This option allows you to modify an existing location.

1. From the Main Menu, select Option **#1 – Application Configuration (Device & Location)** and press 'Enter'.

2. Select Option **#2 – Modify Location** and press 'Enter'.

3. Type the applicable location id and press 'Enter'.

4. Select the applicable item to edit in the location: Floor, Point of Care, Room or Bed and press 'Enter'.

5. Type the updated information for the prior selection and press 'Enter'.

```
Enter 'exit' to return to the previous menu

LOC#  | Floor | Point of Care | Room | Bed
-----------------------------------------
1       8West   NICU             E789   A


Type the id (1,2) of the location from the above list: 1

1. Floor
2. Point of Care
3. Room
4. Bed

Select the data of the Location to edit: 3

Enter the Room for the Location (Room cannot be empty): E889

Location was successfully modified!
LOC#  | Floor | Point of Care | Room | Bed
-----------------------------------------
1       8West   NICU             E889   A

Press enter to return to the main selection menu
```

6. Upon confirmation the location will be modified.

7. Press 'Enter' to return to the prior menu.

Add Location

This option allows you to add a location to an existing floor.

1. From the Main Menu, select Option **#1 – Application Configuration (Device & Location)** and press 'Enter'.

2. Select Option **#5 – Add Location** and press 'Enter'.

```
1. Modify Device Location
2. Modify Location
3. Modify Device Label
4. Add Device
5. Add Location
6. Remove Device
7. Remove Location
8. Display Devices
9. Display Locations
```

3. Type 'Y' to use an existing floor and press 'Enter'.

4. Select the applicable Floor ID and press 'Enter'.

5. To use an existing configured Point of Care, type 'Y', else type 'N' and press 'Enter'.

6. Select the applicable Point of Care ID and press 'Enter'.

7. Type the Room for the location (required).

8. Type the Bed for the location.

9. To confirm your entries, type 'Y' or type 'N' to reject.

```
Enter 'exit' to return to the previous menu

Do you wish to use an existing Floor? (Y/N): y

FLR# | Floor
-------------
1       8West

Please choose one of the above Floor id (FLR#): 1

Do you wish to use an existing Point of Care? (Y/N): y

POC# | Point of Care
-------------
1       NICU

Please choose one of the above Point of Care areas (POC#): 1

Enter the Room for the Location (Room cannot be empty): E342

Enter the Bed for the Location: A

Location as described by the user:

Floor: 8West
Point of Care: NICU
Room: E342
Bed: A

Is this the desired location to be added? (Y/N): y

Location successfully created!
LOC# | Floor | Point of Care | Room | Bed
----------------------------------------
1       8West   NICU            E342   A

Press enter to return to the main selection menu
```

10. Upon confirmation the location will be created.

11. Press 'Enter' to return to the prior menu.

Remove Location

This option allows you to remove a location.

1. From the Main Menu, select Option **#1 – Application Configuration** (**Device & Location**) and press 'Enter'.

2. Select Option **#7 – Remove Location** and press 'Enter'.

```
1. Modify Device Location
2. Modify Location
3. Modify Device Label
4. Add Device
5. Add Location
6. Remove Device
7. Remove Location
8. Display Devices
9. Display Locations
```

3. Type the applicable location id and press 'Enter'.

4. Type 'Y' to confirm removal of the location or type 'N' to cancel.

```
Enter 'exit' to return to the previous menu

LOC#  | Floor | Point of Care | Room | Bed
------------------------------------------
1       8West    NICU             E889   A


Type the id (1,2) of the location from the above list: 1

Location to be removed:
Floor: 8West
Point of Care: NICU
Room: E889
Bed: A
Are you sure you want to remove the following location? (Y/N):
```

5. Upon confirmation the location will be removed.

6. Press 'Enter' to return to the prior menu.

Display Locations

This option allows you to display configured locations.

1. From the Main Menu, select Option **#1 – Application Configuration** (**Device & Location**) and press 'Enter'.

2. Select Option **#9 – Display Locations** and press 'Enter'.

```
1. Modify Device Location
2. Modify Location
3. Modify Device Label
4. Add Device
5. Add Location
6. Remove Device
7. Remove Location
8. Display Devices
9. Display Locations
```

3. Select the applicable location id to display associated devices and press 'Enter'.

```
Enter 'exit' to return to the previous menu

LOC#  | Floor | Point of Care | Room | Bed
------------------------------------------
1       8West    NICU             E173   A
2       8West    NICU             E173   B
3       8West    NICU             E175   A
4       8West    NICU             E175   B
5       8West    NICU             E342   A
6       8West    NICU             E889   A
7       8West    NICU             E932   A

Press enter to return to the main selection menu
Type the id (1,2) of a location to view associated devices:
```

4. Press 'Enter' to return to the prior menu.

Device Operations

These options allow the user to add, modify, remove and display devices in the system. During the device creation/modification, a location can be assigned to the devices (see previous section Location Operations).

Modify Device Location

This option allows you to modify a device location.

1. From the Main Menu, select Option **#1 – Application Configuration (Device & Location)** and press 'Enter'.

2. Select Option **#1 – Modify Device Location** and press 'Enter'.

3. Select the applicable device id and press 'Enter'.

4. Type 'c' to change the device location or type 'r' to remove the device location.

5. Upon confirmation the device will be linked to the modified location.

6. Type 'Y' to modify another device location or type 'N' to return to the prior menu.

Modify Device label

This option allows you to modify a device label.

1. From the Main Menu, select Option **#1 – Application Configuration (Device & Location)** and press 'Enter'.

2. Select Option **#3 – Modify Device Label** and press 'Enter'.

```
1. Modify Device Location
2. Modify Location
3. Modify Device Label
4. Add Device
5. Add Location
6. Remove Device
7. Remove Location
8. Display Devices
9. Display Locations
```

3. Select the applicable device id and press 'Enter'.

4. Type a label for the device and press 'Enter'.

    NOTE: Spaces and special characters are not allowed.

```
Enter 'exit' to return to the previous menu

DEV#  | Label         | Serial    | Location  {Floor | Point of Care | Room | Bed}| CONNECTED
------------------------------------------------------------------------------------------
1        Instrument1    2000008011           8West    NICU              E175   A    YES
2        Instrument1234 2000001234           8West    NICU              E889   A    NO
3        Instrument814  200000814            8West    NICU              E889   A    NO
4        Instrument816  200000816            8West    NICU              E173   A    NO

Type the id (1,2) to select that device from the above list: 1

Enter the new label for the POC Device.
Spaces and special characters are not allowed: Instrument8011

POC Device was modified successfully!
DEV#  | Label         | Serial    | Location  {Floor | Point of Care | Room | Bed}| CONNECTED
------------------------------------------------------------------------------------------
1        Instrument8011 2000008011           8West    NICU              E175   A    YES

Press enter to return to the main selection menu
```

5. Upon confirmation the device label will be modified.

6. Press 'Enter' to return to the prior menu.

Add Device

This option allows you to add a device to an existing location.

1. From the Main Menu, select Option **#1 – Application Configuration (Device & Location)** and press 'Enter'.

2. Select Option **#4 – Add Device** and press 'Enter'.

3. Type the serial number for the device and press 'Enter'.

4. Type a label for the device and press 'Enter'.

    NOTE: Spaces and special characters are not allowed.

5. Type 'Y' to add a location to the device and press 'Enter'. Type 'N' do not wish to add a location to the device.

6. Select the applicable location id and press 'Enter'.

7. Upon confirmation the device will be created and linked to the selected location.

8. Press 'Enter' to return to the prior menu.

Note: There may be situations where devices that are added to the system are not used in a fixed location. This situation is common when devices are used as needed and not mounted or placed in a specific location.

Remove Device

This option allows you to remove a device.

1. From the Main Menu, select Option **#1 – Application Configuration (Device & Location)** and press 'Enter'.

2.   Select Option **#6 – Remove Device** and press 'Enter'.

```
1. Modify Device Location
2. Modify Location
3. Modify Device Label
4. Add Device
6. Remove Device
8. Display Devices
9. Display Locations
```

3.   Select the applicable device id and press 'Enter'.

4.   Type 'Y' to confirm removal of the device or type 'N' to cancel.

```
Enter 'exit' to return to the previous menu

DEV# | Label         | Serial    | Location  {Floor | Point of Care | Room | Bed}| CONNECTED
-------------------------------------------------------------------------------------------
1      Instrument1234 2000001234            8West    NICU            E889   A     NO
2      Instrument8011 2000008011            8West    NICU            E175   A     YES
3      Instrument814  200000814             8West    NICU            E889   A     NO
4      Instrument816  200000816             8West    NICU            E173   A     NO

Type the id (1,2) to select that device from the above list: 1

Device to be removed:   POC Device ID: Instrument1234
Are you sure you want to remove the following device? (Y/N): y

POC Device successfully removed!
Press enter to return to the main selection menu
```

5.   Upon confirmation the device will be removed.

6.   Press 'Enter' to return to the prior menu.

Display Devices

This option allows you to display configured devices.

1.   From the Main Menu, select Option **#1 – Application Configuration (Device & Location)** and press 'Enter'.

2.   Select Option **#8 – Display Devices** and press 'Enter'.

```
1. Modify Device Location
2. Modify Location
3. Modify Device Label
4. Add Device
5. Add Location
6. Remove Device
8. Display Devices
```

3.   Press 'Enter' to return to the prior menu.

```
Enter 'exit' to return to the previous menu

DEV# | Label         | Serial    | Location  {Floor | Point of Care | Room | Bed}| CONNECTED
-------------------------------------------------------------------------------------------
1      Instrument8011 2000008011            8West    NICU            E175   A     YES
2      Instrument814  200000814             8West    NICU            E889   A     NO
3      Instrument816  200000816             8West    NICU            E173   A     NO

Press enter to return to the main selection menu
```

Application Configuration

The Application Configuration menu allows the user to check the HL7 service status and restart the enabled services on the Iris Gateway when needed.

```
Iris Gateway Appliance Configuration Tool
Please select from one of the following options
(Appliance Configuration, General Menu)

HL7 ADT: Enabled
HL7 Alarm Reporter: Enabled
HL7 Vitals Out: Disabled

1. Check Running Services
2. Restart HL7 Interface ADT & Vitals Out Service
3. Restart HL7 Interface Alarm Reporter Service
4. Restart Iris Gateway Service

Enter 'exit' to return to the previous menu
Select the number of one of the above options

Or type 'help #':
```

To navigate to the Application Configuration menu, perform the following:

1. From the Main Menu, select Option **#2 – Application Configuration** and press 'Enter'

```
1. Application Configuration (Device & Location)
2. Application Configuration
3. Server & OS Configuration
4. HL7 Interface Outbound Configuration
5. HL7 Interface Inbound Configuration
```

Check Running Services

This option allows you to check the running services.

1. From the Main Menu, select Option **#2 – Application Configuration** and press 'Enter'.

2. Select Option **#1 – Check Running Services** and press 'Enter'.

```
1. Check Running Services
2. Restart HL7 Interface ADT & Vitals Out Service
3. Restart HL7 Interface Alarm Reporter Service
4. Restart Iris Gateway Service
```

3. Press 'Enter' to return to the prior menu.

```
HL7 ADT & Vitals Out service is UP, and was started on 2015-09-25 at 12:00:48

HL7 Alarm Reporter service is UP, and was started on 2015-09-25 at 12:00:48

Press enter to continue to the main menu
```

Restart HL7 Interface ADT & Vitals Out Service

This option allows you to restart the HL7 interface ADT & Vitals Out service.

1. From the Main Menu, select Option **#2 – Application Configuration** and press 'Enter'.

2. Select Option **#2 – Restart HL7 Interface ADT & Vitals Out** service and press 'Enter'.

```
1. Check Running Services
2. Restart HL7 Interface ADT & Vitals Out Service
3. Restart HL7 Interface Alarm Reporter Service
4. Restart Iris Gateway Service
```

3. Type 'Y' to confirm restarting of the HL7 ADT & Vitals Out Service or N to cancel.

```
*******************WARNING*******************
Restarting the HL7 ADT & Vitals Out service will interrupt the service
Instrument Parameter data will not be sent out while the service is being restarted
Make sure that hospital administrators are informed of any HL7 interruption.

Are you sure you want to restart the HL7 ADT & Vitals Out service? (Y/N): y
Restarting HL7 ADT & Vitals Out ...
HL7 Vitals Out & ADT successfully restarted

Press enter to continue to the main menu
```

Restart HL7 Interface Alarm Reporter Service

This option allows you to restart the HL7 interface Alarm Reporter service.

1. From the Main Menu, select Option **#2 – Application Configuration** and press 'Enter'.

2. Select Option **#3 – Restart HL7 Interface Alarm Reporter** service and press 'Enter'.

```
1. Check Running Services
2. Restart HL7 Interface ADT & Vitals Out Service
3. Restart HL7 Interface Alarm Reporter Service
4. Restart Iris Gateway Service
```

3. Type 'Y' to confirm restarting of the HL7 Alarm Reporter or N to cancel.

```
*******************WARNING*******************
Restarting the HL7 Alarm Reporter service will interrupt the service
Patient and Instrument Alarms not be sent out while the service is being restarted
Make sure that hospital administrators are informed of any HL7 Alarm interruption.

Are you sure you want to restart the HL7 Alarm Reporter? (Y/N): y
Restarting HL7 Alarm Reporter ...
HL7 Alarm Reporter successfully restarted

Press enter to continue to the main menu
```

Restart Iris Gateway

This option allows you to restart the Iris Gateway service.

1. From the Main Menu, select Option **#2 – Application Configuration** and press 'Enter'.

2. Select Option **#4 – Restart Iris Gateway Service** and press 'Enter'.

```
1. Check Running Services
2. Restart HL7 Interface ADT & Vitals Out Service
3. Restart HL7 Interface Alarm Reporter Service
4. Restart Iris Gateway Service
```

3. Type 'Y' to confirm restarting of the Iris Gateway or N to cancel.

```
*******************WARNING*******************
Restarting the Iris Gateway service will interrupt all services
All Instruments will disconnect while the server is not on.
Instrument Parameter data will not be sent out while the service is being restarted
Patient and Instrument Alarms not be sent out while the service is being restarted
Make sure that hospital administrators are informed of any Iris Gateway interruption.

Are you sure you want to restart the Iris Gateway? (Y/N): y
Restarting Iris Gateway ...
```

Server and OS Configuration

The Server & OS Configuration sub menu options allows the user to shutdown, restart, change the network interface settings and change the date settings on the Iris Gateway. Additionally the password can be changed for the logged-in user.

```
Iris Gateway Appliance Configuration Tool
Please select from one of the following options
(Server & OS Configuration Menu)

Current User: root
Current Date & Time: 09 09 2015, 08:32
Current IP Address: 10.1.104.220

1. Shutdown Appliance
2. Restart Appliance
3. Change Network Interface Settings
4. Change Date
5. Change Password

Enter 'exit' to return to the previous menu
Select the number of one of the above options

Or type 'help #':
```

To navigate to the Server & OS Configuration Menu, perform the following:

1. From the Main Menu, select Option **#3 – Server & OS Configuration** and press 'Enter'.

```
1. Application Configuration (Device & Location)
2. Application Configuration
3. Server & OS Configuration
4. HL7 Interface Outbound Configuration
5. HL7 Interface Inbound Configuration
```

Shutdown Appliance (Server)

This option allows you to shutdown the Iris Gateway server.

1. From the Main Menu, select Option **#3 – Server & OS Configuration** and press 'Enter'.

2. Select Option **#1 – Shutdown Appliance** and press 'Enter'.

```
1. Shutdown Appliance
2. Restart Appliance
3. Change Network Interface Settings
4. Change Date
5. Change Password
```

3.   Type 'Y' to confirm shut down of the Iris Gateway Appliance server or N to cancel.

Note: For traceability, users can add comments pertaining to the reason(s) for shutting down the server.

Restart Appliance (Server)

This option allows you to restart the Iris Gateway server.

1.   From the Main Menu, select Option **#3 – Server & OS Configuration** and press 'Enter'.

2.   Select Option **#2 – Restart Appliance** and press 'Enter'.

3.   Type 'Y' to confirm restarting of the Iris Gateway Appliance server or N to cancel.

Note: For traceability, users can add comments pertaining to the reason(s) for shutting down the server.

Change Network Interface Settings

This option allows you to change the network interface settings.

1.   From the Main Menu, select Option **#3 – Server & OS Configuration** and press 'Enter'.

2.   Select Option **#3 – Change Network Interface Settings** and press 'Enter'.
      NOTE: Changing the network interface settings will cause the network service to restart, which will disconnect all devices. All devices configured to connect to the Iris Gateway must have their destination IP addresses changed to the newly configured Iris Gateway IP address.

3.   Enter the new IP address in dotted decimal format or press 'Enter' to leave the current setting.

4.   Enter the new subnet mask in dotted decimal format or press 'Enter' to leave the current setting.

5. Enter the new broadcast address in dotted decimal format or press 'Enter' to leave the current setting.

6. Enter the new gateway address in dotted decimal format or press 'Enter' to leave the current setting.

7. Type 'Y' to confirm the new settings or type 'N' to cancel.

Change Date

This option allows you to change the date.

1. From the Main Menu, select Option **#3 – Server & OS Configuration** and press 'Enter'.

2. Select Option **#4 – Change Date** and press 'Enter'.

Note: Date must be entered in the following format: MMDDhhmmYY, where 'MM' is month, 'DD' is day, 'hh' is hour in 24-hour format, 'mm' is minute and 'YY' is year.

Note: Changing the date will require the Iris Gateway services to restart, which will temporarily disconnect all connected devices.

Note: For traceability, users can add comments pertaining to the reason(s) for shutting down the server.

3.   Enter the new date and press 'Enter'.

```
Enter 'exit' at any time to return to the previous menu

*****************WARNING*******************
Changing the Date will require the Iris Application to restart
All Instruments and SafetyNet Views will
temporarily disconnect during this restart

Reason for changing date? (press enter to leave blank):

Hours (hh), Minutes (mm) are based on 24-hr time.
For example, 3:00 PM would be entered as 1500
Enter date in MMDDhhmm[YY] format (YY is optional)
NOTE: Time is based on 24-hr time.
For example, 3:00 PM on July 4 would be entered as 07041500


Enter new date:
```

4.   Press 'Enter' to return to the prior menu.

Change Password

This option allows you to change the password for the currently logged in user.

1.   From the Main Menu, select Option **#3 – Server & OS Configuration** and press 'Enter'

2.   Select Option **#5 – Change Password** and press 'Enter'.
     NOTE: Users are responsible for maintaining their password. Technical Support must be contacted for lost or forgotten passwords.

```
1. Shutdown Appliance
2. Restart Appliance
3. Change Network Interface Settings
4. Change Date
5. Change Password
```

3.   Type the new password and press 'Enter'.

```
Enter 'exit' at any time to return to the previous menu

*****************WARNING*******************
Users are responsible for maintaining their password.
Technical Support must be contacted for lost or forgotten passwords.

Early exiting from this menu is disabled (Use Ctrl+C to leave the Gateway).

Enter the new password:
```

4.   Re-type the password and press 'Enter'.

5.   Press 'Enter' to return to the prior menu.

HL7 Interface Outbound Configuration

The HL7 Interface Outbound Configuration enables the user to configure Iris Gateway outbound listeners/recipients.

```
1. Application Configuration (Device & Location)
2. Application Configuration
3. Server & OS Configuration
4. HL7 Interface Outbound Configuration
5. HL7 Interface Inbound Configuration
```

There are two outbound listener types supported by the Iris Gateway.

- HL7 Vitals Out Listener
- HL7 Alarm Reporter Listener

```
Iris Gateway Appliance Configuration Tool
Please select from one of the following options
(HL7 Interface Outbound Configuration)

Available HL7 Vitals Out Listeners | HL7 Vitals Out Timers (in secs)
Name            IP address   Port  | Publish Time
HL7MLLPClient   127.0.0.1  : 5555  | 60

Available HL7 Alarm Listeners        | HL7 Alarm Timers (in secs)
Name              IP address   Port | Keep Alive / Publish Time / Expiration Time
HL7MLLPClient-ACM  127.0.0.1 : 5555 | 60          60              600

1. Add HL7 Vitals Out Listener
2. Add HL7 Alarm Listener
3. Change HL7 Vitals Out Listener IP Address
4. Change HL7 Alarm Listener IP Address
5. Change HL7 Vitals Out port
6. Change HL7 Alarm Listener Port
7. Change Vitals Out Message Frequency
8. Change Alarm Publish Message Frequency
9. Change Unacknowledged Alarm Expiration Time
10. Change HL7 Alarm Reporter Keep Alive Frequency
11. Remove HL7 Vitals Out Listener
12. Remove HL7 Alarm Listener
13. Disable HL7 Vitals Out Service
14. Enable Unassigned HL7 Results Output
15. Disable HL7 Alarm Report Service

Enter 'exit' to return to the previous menu
NOTICE: Pending changes require an HL7 ADT & Vitals Out restart before taking affect
Please restart the appropriate HL7 service(s) before exiting the Iris Gateway Tool

Select the number of one of the above options

Or type 'help #':
```

HL7 Vitals Out Listener

HL7 Vitals Out Listener allows the user to configure a maximum of 2 listeners for vitals out. The user will be able to configure the following:

1. The listener IP address

2. The listener port

3. The frequency of vitals out (interval)

Add HL7 Vitals Out listener

This option allows you to add a Vitals Out listener.

Note: Before adding a vitals out listener, the ADT and Vitals Out service needs to be enabled. Otherwise, Iris Gateway will show an error message.

```
Enter 'exit' at any time to return to the previous menu


IPTables successfully restarted

HL7 Vitals Out successfully enabled
Please issue a restart of the HL7 ADT & Vitals Out service to start the Vitals Out service.

Press enter to continue to the main menu
```

Note: To enable the ADT and Vitals Out service see Enable/Disable HL7 Vitals Out Service section.

1. From the Main Menu select Option **#4 - HL7 Interface Outbound Configuration** and press 'Enter'.

   Note: The Iris Gateway configuration tool will display the current configured outbound listeners.

2. Select **Option #1 - Add HL7 Vitals Out Listener** and press 'Enter'.

```
1. Add HL7 Vitals Out Listener
2. Add HL7 Alarm Listener
3. Change HL7 Vitals Out Listener IP Address
4. Change HL7 Alarm Listener IP Address
5. Change HL7 Vitals Out port
6. Change HL7 Alarm Listener Port
7. Change Vitals Out Message Frequency
8. Change Alarm Publish Message Frequency
9. Change Unacknowledged Alarm Expiration Time
10. Change HL7 Alarm Reporter Keep Alive Frequency
11. Remove HL7 Vitals Out Listener
12. Remove HL7 Alarm Listener
13. Disable HL7 Vitals Out Service
14. Enable Unassigned HL7 Results Output
15. Disable HL7 Alarm Report Service
```

3. Type the listener IP address and press 'Enter'.

4. Type the listener port and press 'Enter'.

```
Enter 'exit' at any time to return to the previous menu


Please enter the name of the new HL7 Vitals Out listener: EMR1

Please enter the ip address of the new HL7 Vitals Out listener (###.###.###.###): 10.1.104.200

Please enter the port of the new HL7 Vitals Out listener (Valid Range 1 - 65535): 4545

IPTables successfully restarted

New HL7 Vitals Out listener EMR1 successfully saved

Press enter to continue to the main menu
```

5. Upon confirmation the vitals out listener will be updated

6. Press Enter to exit from the sub menu.

7. The HL7 Outbound Submenu will display the newly entered listener configuration on the top of the sub menu:

```
Iris Gateway Appliance Configuration Tool
Please select from one of the following options
(HL7 Interface Outbound Configuration)

Available HL7 Vitals Out Listeners| HL7 Vitals Out Timers (in secs)
Name    IP address     Port  | Publish Time
EMR1    10.1.104.200 : 4545  | 60

Available HL7 Alarm Listeners         | HL7 Alarm Timers (in secs)
Name             IP address    Port  | Keep Alive / Publish Time / Expiration Time
HL7MLLPClient-ACM  127.0.0.1  : 5555  | 60              60               600

1. Add HL7 Vitals Out Listener
2. Add HL7 Alarm Listener
3. Change HL7 Vitals Out Listener IP Address
4. Change HL7 Alarm Listener IP Address
5. Change HL7 Vitals Out port
6. Change HL7 Alarm Listener Port
7. Change Vitals Out Message Frequency
8. Change Alarm Publish Message Frequency
9. Change Unacknowledged Alarm Expiration Time
10. Change HL7 Alarm Reporter Keep Alive Frequency
11. Remove HL7 Vitals Out Listener
12. Remove HL7 Alarm Listener
13. Disable HL7 Vitals Out Service
14. Enable Unassigned HL7 Results Output
15. Disable HL7 Alarm Report Service

Enter 'exit' to return to the previous menu
NOTICE: Pending changes require an HL7 Vitals Out restart before taking affect
Please restart the appropriate HL7 service(s) before exiting the Iris Gateway Tool

Select the number of one of the above options

Or type 'help #':
```

8. Changes to the HL7 inbound and outbound configuration requires the HL7 service(s) to be restarted. Refer to **Restart HL7 Interface ADT & Vitals Out Service** on page 24 and **Restart HL7 Interface Alarm Reporter Service** on page 25.

Configure Vitals Out Message Frequency

This option allows you to configure the vitals out message frequency.

Note: Vitals Out frequency is defaulted to 60 seconds.

1.   From the Main Menu select Option **#4 - HL7 Interface Outbound Configuration** and press 'Enter'.

2.   Select Option **# 7 – Change Vitals Out Message Frequency** and press 'Enter'.

```
1. Add HL7 Vitals Out Listener
2. Add HL7 Alarm Listener
3. Change HL7 Vitals Out Listener IP Address
4. Change HL7 Alarm Listener IP Address
5. Change HL7 Vitals Out port
6. Change HL7 Alarm Listener Port
7. Change Vitals Out Message Frequency
8. Change Alarm Publish Message Frequency
9. Change Unacknowledged Alarm Expiration Time
10. Change HL7 Alarm Reporter Keep Alive Frequency
11. Remove HL7 Vitals Out Listener
12. Remove HL7 Alarm Listener
13. Disable HL7 Vitals Out Service
14. Enable Unassigned HL7 Results Output
15. Disable HL7 Alarm Report Service
```

3.   Select the vitals out listener.

4.   Type the desired vitals out publishing frequency in seconds and press 'Enter'.

```
Enter 'exit' at any time to return to the previous menu

HL7 Vitals Out publish timer values should be entered in seconds
HL7 Vitals Out publish timer minimum value: 60
HL7 Vitals Out publish timer maximum value: 28800 (8 hrs)

Please enter the new publishing interval: 120

New HL7 Vitals Out interval of 120 successfully saved

Press enter to continue to the main menu
```

5.   Upon confirmation the vitals out publishing frequency will be updated.

6.   Press Enter to exit from the submenu.

The Iris Gateway Configuration tool will display the configured listeners and in this example you can see that the HL7 vitals out frequency has been changed to 120 seconds.

HL7 Alarm Listener

HL7 Alarm Listener allows the user to configure a maximum of 2 Alarm listener. The user will be able to configure the following:

1.   The listener IP address

2.   The listener port

3.   Maximum Retry time (before the alarm is considered expired)

Add HL7 Alarm listener

This option allows you to add an alarm listener.

1. From the Main Menu select Option **#4 - HL7 Interface Outbound Configuration** and press 'Enter'.

2. Select Option **#2 – Add HL7 Alarm Listener** and press 'Enter'.

```
1. Add HL7 Vitals Out Listener
2. Add HL7 Alarm Listener
3. Change HL7 Vitals Out Listener IP Address
4. Change HL7 Alarm Listener IP Address
5. Change HL7 Vitals Out port
6. Change HL7 Alarm Listener Port
7. Change Vitals Out Message Frequency
8. Change Alarm Publish Message Frequency
9. Change Unacknowledged Alarm Expiration Time
10. Change HL7 Alarm Reporter Keep Alive Frequency
11. Remove HL7 Vitals Out Listener
12. Remove HL7 Alarm Listener
13. Disable HL7 Vitals Out Service
14. Enable Unassigned HL7 Results Output
15. Disable HL7 Alarm Report Service
```

3. Type the name of the new HL7 Alarm Reporter and press 'Enter'.

4. Type the IP address of the new HL7 Alarm Reporter and press 'Enter'.

5. Type the port of the new HL7 Alarm Reporter and press 'Enter'.

```
Enter 'exit' at any time to return to the previous menu

Please enter the name of the new HL7 Alarm Reporter: AlarmManager1

Please enter the ip address of the new HL7 Alarm Reporter (###.###.###.###): 10.1.104.199

Please enter the port of the new HL7 Alarm Reporter (Valid Range 1 - 65535): 3215

IPTables successfully restarted

New HL7 Alarm Reporter Listener AlarmManager1 successfully saved

Press enter to continue to the main menu
```

6. Upon confirmation the IP address or port information will be updated.

7. Press Enter to exit from the sub menu.

Change HL7 Listeners IP/Ports

To change the HL7 Vitals Out or Alarm Listeners IP address or port information, perform the following:

1. From the Main Menu select Option **#4 - HL7 Interface Outbound Configuration** and press 'Enter'.

2. Select the corresponding option you wish to perform from the HL7 Interface Outbound Configuration submenu (Options #3 though #6) and press 'Enter'.

```
1. Add HL7 Vitals Out Listener
2. Add HL7 Alarm Listener
3. Change HL7 Vitals Out Listener IP Address
4. Change HL7 Alarm Listener IP Address
5. Change HL7 Vitals Out port
6. Change HL7 Alarm Listener Port
7. Change Vitals Out Message Frequency
8. Change Alarm Publish Message Frequency
9. Change Unacknowledged Alarm Expiration Time
10. Change HL7 Alarm Reporter Keep Alive Frequency
11. Remove HL7 Vitals Out Listener
12. Remove HL7 Alarm Listener
13. Disable HL7 Vitals Out Service
14. Enable Unassigned HL7 Results Output
15. Disable HL7 Alarm Report Service
```

3. Type the ID of the listener you wish to edit and press 'Enter'.

4. Type the desired IP address or port information and press 'Enter'.

```
Enter 'exit' at any time to return to the previous menu

Available HL7 Alarm Listeners
ID   Name                  IP address     Port
1    AlarmManager1         10.1.104.199 : 3215
2    HL7MLLPClient-ACM     127.0.0.1    : 5555

Please select the ID (1, 2) of the listener you wish to edit: 1

Please enter the new ip address (###.###.###.###): 10.1.104.198

New IP address 10.1.104.198 for HL7 Alarm Listener AlarmManager1 successfully saved

Press enter to continue to the main menu
```

```
Enter 'exit' at any time to return to the previous menu

Available HL7 Alarm Listeners
ID   Name                  IP address     Port
1    AlarmManager1         10.1.104.198 : 3215
2    HL7MLLPClient-ACM     127.0.0.1    : 5555

Please select the ID (1, 2) of the listener you wish to edit: 2

Please enter the new port (Valid Range 1 - 65535): 8754

IPTables successfully restarted

New Port 8754 for HL7 Alarm Reporter Listener HL7MLLPClient-ACM successfully saved

Press enter to continue to the main menu
```

5. Upon confirmation the IP address or port information will be updated.

6. Press Enter to exit from the sub menu.

Change Alarm Publish Message Frequency

The Iris Gateway Alarm Reporter has the capability to send alarm updates to the Alarm Listener. The Alarm Publish Message Frequency is a configuration the Alarm Reporter uses to determine when to send an update of an alarm status.

This updated HL7 message serves two purposes:

- Confirm that the Alarm is still active

- Updates to any clinical reading values that changed

Note: If an SpO2 Low Alarm occurs (SpO2 value = "84", SpO2 Low alarm limit = "88"), the Iris Gateway Alarm reporter sends a "start" HL7 alarm message to the Alarm Listener. If the alarm sustains longer than the set Alarm Publish Message Frequency (20 seconds in this example), the Iris Gateway Alarm Reporter sends another "updated" HL7 Alarm Message, along with the updated SpO2 value (assuming SpO2 value has changed during the 20 seconds).

1. From the Main Menu select Option **#4 - HL7 Interface Outbound Configuration** and press 'Enter'.

2.   Select Option **#8 – Change Alarm Publish Message Frequency** and press 'Enter'.

Note: The configuration tool will first display the current listener(s) configuration information to the user (see below).

3.   Type the new Alarm Reporter publish timer frequency in seconds and press 'Enter'.

4.   Enter the Minimum Alarm Retry time and press 'Enter'. (expiration time see definition section).

5.   Upon confirmation the alarm publishing frequency will be updated.

6.   Press Enter to exit from the sub menu.

Change Unacknowledged Alarm Expiration Time

When Iris Gateway send's an alarm to an Alarm Listener, Iris Gateway expects a message back from the Alarm Listener. This response from the Alarm Listener is called the Acknowledgment Message (ACK).

Iris Gateway uses this setting to determine when to stop sending an alarm to the Alarm Listener, when there is no response. The Unacknowledged Alarm Expiration Time can be set in one second increments, with a maximum setting of 1200 seconds.

Note: If the Alarm Listener is not available or is unable to send the ACK back to the Iris Gateway, the Iris Gateway Alarm Reporter will continue to send the message repeatedly (using the configured Alarm Publish Frequency outlined in the previous section) until the ACK is received from the Alarm listener, or it reaches the configured Unacknowledged Alarm Expiration Time.

1.   From the Main Menu select Option **#4 - HL7 Interface Outbound Configuration** and press 'Enter'.

2.   Select Option **#9 – Change Unacknowledged Alarm Expiration Time** and press 'Enter'.

3. Type the new unacknowledged alarm expiration time in seconds and press 'Enter'.

4. Upon confirmation the unacknowledged alarm expiration time will be updated.

5. Press Enter to exit from the sub menu.

Change Alarm Reporter HL7 Keep Alive Frequency

This option allows you to change the Keep Alive Message Frequency.

Note: The Keep Alive Message is used by listening systems to acknowledge communication from the Iris Gateway system. Some listening systems can be configured to alert users when the Keep Alive message is not received.

1. From the Main Menu select **Option #4 - HL7 Interface Outbound Configuration** and press 'Enter'.

2. Select Option **#10 – Change HL7 Alarm Reporter Keep Alive Frequency** and press 'Enter'.

3. Type the desired keep alive time in seconds and press 'Enter'

4. Upon confirmation the keep alive time will be updated.

5. Press Enter to exit from the sub menu.

Remove HL7 Vitals Out Listener

This option allows you to remove an HL7 Vitals Out Listener.

1. From the Main Menu select Option **#4 - HL7 Interface Outbound Configuration** and press 'Enter'.

2. Select Option **#11 – Remove HL7 Vitals Out Listener** and press 'Enter'.

```
1. Add HL7 Vitals Out Listener
2. Add HL7 Alarm Listener
3. Change HL7 Vitals Out Listener IP Address
4. Change HL7 Alarm Listener IP Address
5. Change HL7 Vitals Out port
6. Change HL7 Alarm Listener Port
7. Change Vitals Out Message Frequency
8. Change Alarm Publish Message Frequency
9. Change Unacknowledged Alarm Expiration Time
10. Change HL7 Alarm Reporter Keep Alive Frequency
11. Remove HL7 Vitals Out Listener
12. Remove HL7 Alarm Listener
13. Disable HL7 Vitals Out Service
14. Enable Unassigned HL7 Results Output
15. Disable HL7 Alarm Report Service
```

3. Select the HL7 Vitals Out Listener you wish to remove and press 'Enter'.

```
Enter 'exit' at any time to return to the previous menu

Available HL7 Vitals Out Listeners
ID    Name    IP address       Port
1     EMR1    10.1.104.202 : 5454

Please select the ID (1, 2) of the consumer you wish to edit: 1

Are you sure you want to remove the HL7 Vitals Out Listener? (Y/N): y
HL7 Vitals Out successfully removed from the Iris Configuration

Press enter to continue to the main menu
```

4. Upon confirmation the HL7 Vitals Out Listener will be removed.

5. Press Enter to exit from the sub menu.

Remove HL7 Alarm Listener

This option allows you to remove an HL7 Alarm Listener.

1. From the Main Menu select Option #4 - HL7 Interface Outbound Configuration and press 'Enter'.

2. Select Option **#12 – Remove HL7 Alarm Listener** and press 'Enter'.

```
1. Add HL7 Vitals Out Listener
2. Add HL7 Alarm Listener
3. Change HL7 Vitals Out Listener IP Address
4. Change HL7 Alarm Listener IP Address
5. Change HL7 Vitals Out port
6. Change HL7 Alarm Listener Port
7. Change Vitals Out Message Frequency
8. Change Alarm Publish Message Frequency
9. Change Unacknowledged Alarm Expiration Time
10. Change HL7 Alarm Reporter Keep Alive Frequency
11. Remove HL7 Vitals Out Listener
12. Remove HL7 Alarm Listener
13. Disable HL7 Vitals Out Service
14. Enable Unassigned HL7 Results Output
15. Disable HL7 Alarm Report Service
```

3.   Select the HL7 Alarm Listener you wish to remove and press 'Enter'.

```
Enter 'exit' at any time to return to the previous menu

Available HL7 Alarm Listeners
ID   Name                 IP address    Port
1    AlarmManager1        10.1.104.198 : 3215
2    HL7MLLPClient-ACM     127.0.0.1    : 8754

Please select the ID (1, 2) of the listener you wish to edit: 2

Are you sure you want to remove the HL7 Alarm Reporter Listener? (Y/N): y
HL7 Alarm Reporter Listener successfully removed from the Iris application

Press enter to continue to the main menu
```

4.   Upon confirmation the HL7 Alarm Listener will be removed.

5.   Press Enter to exit from the sub menu.

Disable HL7 Vitals Out Service

This option allows you to enable/disable HL7 Vitals Out Service.

1.   From the Main Menu select Option **#4 - HL7 Interface Outbound Configuration** and press 'Enter'.

2.   Select Option **#13 – Enable/Disable HL7 Vitals Out Service** and press 'Enter'.

   Note: If the HL7 Vitals Out Service is currently disabled selecting this option will enable and vice versa.

```
1. Add HL7 Vitals Out Listener
2. Add HL7 Alarm Listener
3. Change HL7 Vitals Out Listener IP Address
4. Change HL7 Alarm Listener IP Address
5. Change HL7 Vitals Out port
6. Change HL7 Alarm Listener Port
7. Change Vitals Out Message Frequency
8. Change Alarm Publish Message Frequency
9. Change Unacknowledged Alarm Expiration Time
10. Change HL7 Alarm Reporter Keep Alive Frequency
11. Remove HL7 Vitals Out Listener
12. Remove HL7 Alarm Listener
13. Disable HL7 Vitals Out Service
14. Enable Unassigned HL7 Results Output
15. Disable HL7 Alarm Report Service
```

3.   Upon confirmation the HL7 Vitals Out Service will either be enabled or disabled.

```
Enter 'exit' at any time to return to the previous menu

HL7 Vitals Out successfully enabled

Press enter to continue to the main menu
```

4.   Press Enter to exit from the sub menu.

Enable/Disable Unassigned HL7 Results Output

This option allows you to enable/disable Unassigned HL7 Results Output.

Note: Enable/disable Unassigned HL7 Results Output will only show if the HL7 Vitals Out Service is enabled. When enabling Unassigned HL7 Results Output. Iris Gateway vitals out service will send vitals out without the need for patient admission from POC device that has this capabilities.

1.   From the Main Menu select Option **#4 - HL7 Interface Outbound Configuration** and press 'Enter'.

2.   Select Option **#14 – Enable/Disable Unassigned HL7 Results Output** and press 'Enter'.

Note: If the Unassigned HL7 Results Output is currently disabled selecting this option will enable and vice versa.

3. Upon confirmation the Unassigned HL7 Results Output will either be enabled or disabled.

4. Press Enter to exit from the submenu.

Disable HL7 Alarm Report Service

This option allows you to enable/disable HL7 Alarm Report Service.

1. From the Main Menu select Option **#4 - HL7 Interface Outbound Configuration** and press 'Enter'.

2. Select Option **#15 – Enable/Disable HL7 Alarm Report Service** and press 'Enter'.

    Note: If the HL7 Alarm Report Service is currently disabled selecting this option will enable and vice versa.

3. Upon confirmation the HL7 Alarm Report Service will either be enabled or disabled.

4. Press Enter to exit from the submenu.

HL7 Interface Inbound Configuration

The Iris Configuration Tool allows the user to change the HL7 Inbound configuration. The configuration tool will display the HL7 Inbound configuration to the user before displaying the submenu option for configuration.

The user will be able to perform two actions:

1. Edit the listening port for ADT.

2. Disable HL7 ADT service.

Edit the Listening Port for ADT

This option allows you to edit the listening port for ADT.

1. From the Main Menu select Option **#5 - HL7 Inbound Configuration** and press 'Enter'.

2. Select Option **#1 – Edit the Listening Port for ADT** and press 'Enter'.

3. Type the listening port for the inbound ADT and press 'Enter'.

4. Upon confirmation the listening port for the HL7 Inbound ADT will updated.

5. Press Enter to exit from the submenu.

Disable HL7 ADT service

This option allows you to enable/disable HL7 ADT service.

1. From the Main Menu select Option **#5 - HL7 Inbound Configuration** and press 'Enter'.

2. Select Option **#2 – Enable/Disable HL7 ADT Service** and press 'Enter'.
    Note: If the HL7 ADT service is currently disabled selecting this option will enable and vice versa.

3.   Upon confirmation the HL7 ADT service will either be enabled or disabled.

```
Enter 'exit' at any time to return to the previous menu

Restarting ..
The HL7 ADT was successfully disabled, and the Iris application is not running.

Press enter to continue to the main menu
```

4.   Press Enter to exit from the submenu.

Chapter 4: Reports

The following chapter describes the various types of reports that are available in Iris Gateway. This chapter also provides use cases for each report.

The following are the top-level reports and descriptions of individual sections contained within those reports.

- System Report
- Patient Report
- Patient Trend Analysis Report
- Data Export Report
- Patient Summary Report

The Iris Gateway system provides the ability to generate reports from any computer that has access to the same network as the Iris Gateway system, with a user account that has privileges to generate the reports using a web browser. Iris Gateway provides System Reports and Patient Reports.

Note: The URL used to access Iris Gateway Reports is system specific and configured upon installation. Please contact your local system administrator for more information.

Note: Masimo Iris Gateway utilizes the Masimo Patient SafetyNet system report feature. Since Iris Gateway does not support notification delivery, any references to notifications in the report will not be applicable for Iris Gateway.

System Report

The *System Report* encapsulates system data for up to 30 days for a specified time range within the previous year.

Use Cases

- Provides the user the ability to understand alarm distribution across the care area.
- Provides the user the ability to compare different alarm protocols.
- Provides the user the ability to compare various clinical units to each other.

Generate Report

1. From the Report Type drop-down list, select system report.
2. From the Domain drop-down list, select the desired domain.
3. Select Start Date and End Date.
4. Click the boxes for desired report types.
5. Click the boxes for desired report categories.
6. Select Generate Report.

Header Information

The following is an example of the Header Information section.

Hospital Title

Hospital Address

Top Level Domain	Report Date
Parent Domain	Report Start Date
Domain	Report End Date
Number of Instruments (Avg)	Report First Event Time
Utilization	Report Last Event Time
# of Active Instruments	Total Monitoring Time

Active Instrument Utilization	

The following table defines the terms used in the Header Information section.

Terms	Description
Top Level Domain	Name of facility where the Iris Gateway server is located (configured during installation)
Parent Domain	The highest level domain of the Iris Gateway server (configured during installation)
Domain	A subset of the parent domain (configured during installation)
Number of Instruments (Avg)	The average number of instruments connected to the Iris Gateway server for the selected time frame
Report First Event Time	The date and time of the first event for the selected time frame
Report Last Event Time	The date and time of the last event for the selected time frame
Total Monitoring Time	The total time monitored during the selected time frame
Report Date	The date and time that the report was generated
Report Start Date	The start of the time frame selected before the report was generated
Report End Date	The end of the time frame selected before the report was generated
Monitoring Time	The summation of all of the active instrument monitoring time since system installation
Utilization	Monitoring Time divided by the number of connected instruments divided by the selected time frame
# of Active Instruments	The number of instruments connected to the Iris Gateway server
Active Instrument Utilization	Monitoring Time divided by the number of connected instruments actively monitoring divided by the selected time frame

Event Reports

The following is an example of the Clinical Events Report.

1.1 Event Report: Clinical Event

Type [of Clinical Event]	Count	% [Count]	Total Duration (sec)	% [Duration]	Max Duration (sec)

The following is an example of the Non-Clinical Events Report.

1.2 Event Report: Non-Clinical Event

Type [of Non-Clinical Event]	Count	% [Count]	Total Duration (sec)	% [Duration]	Max Duration (sec)

The following is an example of the Modifiers Event Report.

1.3 Event Report: Modifiers Event

Type [of Modifiers Event]	Count	% [Count]	Total Duration (sec)	% [Duration]	Max Duration (sec)

The following table defines the terms used in the Clinical Events, the Non-Clinical Events, and the Modifiers Event reports.

Terms	Description
Type [of Clinical Event]	An event is recorded when a physiological parameter exceeds the configured alarm threshold. See Clinical Events.
Type [of Non-Clinical Event]	An event that triggers an audible alarm but is not related to physiological parameters. See **Non-Clinical Events** on page 58.

Terms	Description
Type [of Modifiers Event]	Environmental states that affect monitored parameters, but do no generate alarms by themselves. See **Modifiers** on page 59.
Count	The number of times that one of the above events or modifiers occurred for the selected time frame
% [Count]	The percentage of occurrence of a type of event or modifier for the selected time frame
Total Duration (sec)	The total number of seconds for all events or modifiers of a particular type for a selected time frame
% [Time Duration]	The percentage of one type of an event or modifier compared to the combined total duration of all other events or modifiers within the same report category of the System Report
Max Duration (sec)	The duration of the longest event or modifier of a particular type

Event Duration Report

The following is an example of the Clinical Event Duration Report.

2.1 Event Duration Report: Clinical Event

Type [of Clinical Event]	2 - 15 (sec)	16 - 30 (sec)	31 -60 (sec)	61 - 180 (sec)	3 - 4 (min)	4 - 5 (min)	>5 min

The following is an example of the Non-Clinical Event Duration Report.

2.2 Event Duration Report: Non-Clinical Event

Type [of Non-Clinical Event]	2 - 15 (sec)	16 - 30 (sec)	31 -60 (sec)	61 - 180 (sec)	3 - 4 (min)	4 - 5 (min)	>5 min

The following is an example of the Modifiers Event Duration Report.

2.3 Event Duration Report: Modifiers Event

Type [of Modifiers Event]	2 - 15 (sec)	16 - 30 (sec)	31 -60 (sec)	61 - 180 (sec)	3 - 4 (min)	4 - 5 (min)	>5 min

The following table defines the terms used in the Clinical Events, the Non-Clinical Events, and the Modifiers Event reports.

Terms	Description
Type [of Clinical Event]	An event is recorded when a physiological parameter exceeds the configured alarm threshold. See **Clinical Events** on page 54.
Type [of Non-Clinical Event]	An event that triggers an audible alarm but is not related to physiological parameters. See **Non-Clinical Events** on page 58.
Type [of Modifiers Event]	Environmental states that affect monitored parameters, but do no generate alarms by themselves. See **Modifiers** on page 59.

Patient Report

The Patient Report encapsulates patient data for up to 30 days for a specified time range within the previous year.

Use Cases

- Provides the user detailed patient events and notification information.*

- Provides the user with the ability to determine how patient events turned into notifications.*

- Provides the user the ability to see which notification devices were alerted.*

  * Masimo Iris Gateway utilizes the Masimo Patient SafetyNet system report feature. Since Iris Gateway does not support notification delivery, any indication for notification in the report will not be applicable for Iris Gateway reports.

Generate Report

1. From the Report Type drop-down list, select patient report.

2. From the Domain drop-down list, select the desired domain.

3. Select Start Date and End Date.

4. Select desired patient in the Patient List.

5. Click the boxes for desired report types.

6. Click the boxes for desired report categories.

7. Select organize report by event type or time.

8. Select Generate Report.

Header Information

The following is an example of the Header Information section.

Hospital Title

Hospital Address

Top Level Domain	Report Date
Parent Domain	Report Start Date
Domain	Report End Date
Patient Name	Report First Event Time
Instrument Label - Serial Number - Type	Report Last Event Time
Room Number	Total Monitoring Time
Admit Time	

The following table defines the terms used in the Header Information section.

Terms	Description
Top Level Domain	Name of facility where the Iris Gateway server is located (configured during installation)
Domain	A subset of the parent domain (configured during installation)
Patient Name	Name given to the patient during the admission process
Instrument Label - Serial Number - Type	The instrument's label, serial number, and type of instrument
Room Number	Room number assigned to patient
Admit Time	The time that patient was admitted
Report First Event Time	The date and time of the first event for the selected time frame
Report Last Event Time	The date and time of the last event for the selected time frame
Total Monitoring Time	The total time monitored during the selected time frame
Report Date	The date and time that the report was generated

Terms	Description
Report Start Date	The start of the time frame selected before the report was generated
Report End Date	The end of the time frame selected before the report was generated

Patient Information Report

The following is an example of the Patient Information Report.

Patient Information Report:

Patient Name
Instrument Label - Serial Number - Type
Room Number
Admit Time
Discharge Time
Admit Duration
Total Number of Events

The following table defines the terms used in the Patient Information Report.

Terms	Description
Patient Name	Name given to the patient during the admission process
Instrument Label	Name given to the instrument (configured during installation)
Instrument Serial Number	The serial number of the instrument that is connected to the patient
Type	The instrument type associated with the patient
Room Number	Room number given to the patient during the admission process
Admit Time	The date and time that the patient was admitted to the system
Admit Duration	The elapsed time between Admit Date and Discharge Date
Total Number of Events	The total number of events.

Events Report

The following is an example of the Clinical Events Report.

1.1 Events Report: Clinical Event

Event	Start Value	Stop Value	Duration (sec)	Start Time	Stop Time	Instrument Label

The following is an example of the Non-Clinical Events Report.

1.2 Events Report: Non-Clinical Event

Event	Duration (sec)	Start Time	Stop Time	Instrument Label

The following is an example of the Modifier Events Report.

1.3 Events Report: Modifiers Event

| Event | Duration (sec) | Start Time | Stop Time | Instrument Label |

The following table defines the terms used in the Clinical Events, the Non-Clinical Events, and the Modifiers Event reports.

Terms	Description
Event	See **Reports Glossary** on page 54.
Start Value	The value of the parameter at the start of an event
Stop Value	The value of the parameter at the end of the event
Event Duration (sec)	The time in seconds between the Start Value and the Stop Value
Start Time	The time and date that the conditions for a type of event were met
Stop Time	The time and date that the conditions for a type of event were no longer met
Instrument Label	The Instrument ID that was entered when the instrument was first added to the Iris Gateway system.

User Interaction Report

The following is an example of the Alarm Silence User Interaction Report.

User Interaction Report: Alarm Silence

| Event | Duration (sec) | Start Time | Stop Time | Instrument Label |

The following is an example of the Respond Instrument User Interaction Report.

User Interaction Report: Respondent Instrument Assignment

| Start Time | Stop Time | Notification ID* | Respondent name | Role |

The following table defines the terms used in the Alarm Silence User Interaction and Respondent Instrument User Interaction reports.

Terms	Description
Event	The instances when the alarm was silenced at the bedside instrument or using the Iris Gateway user interface
Duration (sec)	The duration in seconds that the alarm was silenced
Start Time [Alarm Silence]	The time and date that the alarm silence began
Stop Time [Alarm Silence]	The time and date that the alarm silence ended
Start Time [Respondent Instrument Assignment]*	The time and date that the Respondent Instrument was assigned to the patient
Stop Time [Respondent Instrument Assignment]*	The time and date that the Respondent Instrument was unassigned to the patient
Instrument Label	The Instrument ID that was entered when the instrument was first added to the Iris Gateway system
Notification ID*	The Cap Code of the pager, badge, or phone to which the notification was sent
Respondent Name	The name given to pager, badge, or phone when it was added to the system (configured during installation)

Terms	Description
Role	Whether the recipient of the notification was the primary, secondary, or supervisory

* Masimo Iris Gateway utilizes the Masimo Patient SafetyNet system report feature. Since Iris Gateway does not support notification delivery, any indication for notification in the report will not be applicable for Iris Gateway reports.

Patient Trend Analysis Report

The Patient Trend Analysis Report encapsulates patient data for up to five days for a specified time range within the previous 30 days.

Use Cases

- Provides the user the ability to view patient clinical trends over a selected time frame.

- Provides the user the ability to view overnight clinical information for patients who may be at risk of excessive oxygen desaturations.

Generate Report

1. From the Report Type drop-down list, select patient trend analysis report.

2. From the Domain drop-down list, select the desired domain.

3. Select desired patient in the Patient List.

4. Select Start Date and End Date.

5. Click the boxes for desired parameters and desired trend characteristics

6. Select Generate Report.

Header Information

The following is an example of the Header Information section.

Hospital Title

Hospital Address

Top Level Domain	Report Date
Parent Domain	Report Start Date
Domain	Report End Date
Patient Name	Admit Date
Instrument Name	Discharge Date
Report ID	Admit Duration

The following table defines the terms used in the Header Information section.

Terms	Description
Top Level Domain	The name of facility where the Iris Gateway server is located (configured during installation)
Domain	The domain where the patient is located in the system
Patient Name	The name given to the patient during the admission process
Instrument Name	The name given to the instrument (configured during installation)
Report ID	The sequential number of times for which the report was generated

Terms	Description
Admit Date	The date and time that the patient was admitted to the system
Discharge Date	The date and time that the patient was discharged from the system
Admit Duration	The elapsed time between the Admit Date and the Discharge Date
Report Date	The date and time that the report was generated
Report Start Date	The start of the time frame selected before the report was generated
Report End Date	The end of the time frame selected before the report was generated

Histograms

High and Low thresholds for SpO2, Respiratory Rate, and Pulse Rate can be adjusted in the Patient Trend Analysis Report.

Total time, longest duration, and number of events below or above a threshold can be set as an output for the report.

Histogram Images provide the duration the patient was monitored at a certain value as a percentage of total time monitored.
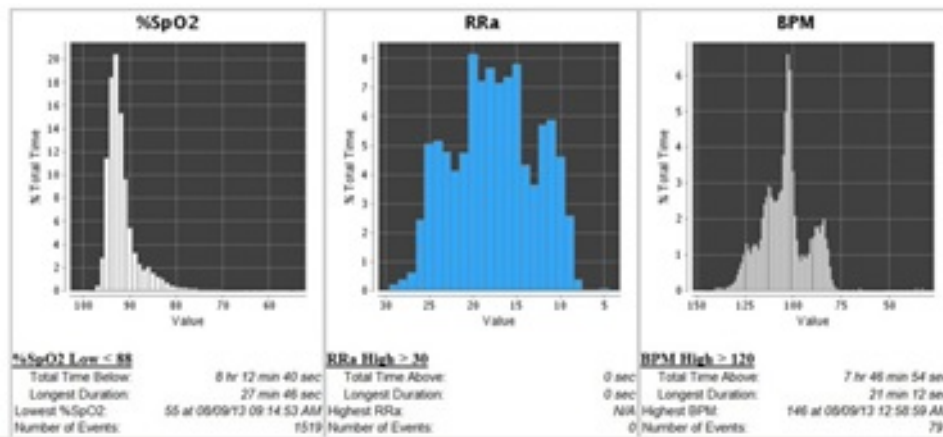
The Histogram section can display a five-day window of SpO2, RRa, and BPM data for up to the previous 30 days.

Trends

The Trends section can display a five-day window of SpO2, RRa, and BPM data for up to the previous 30 days.

The following is an example of the Trends section.
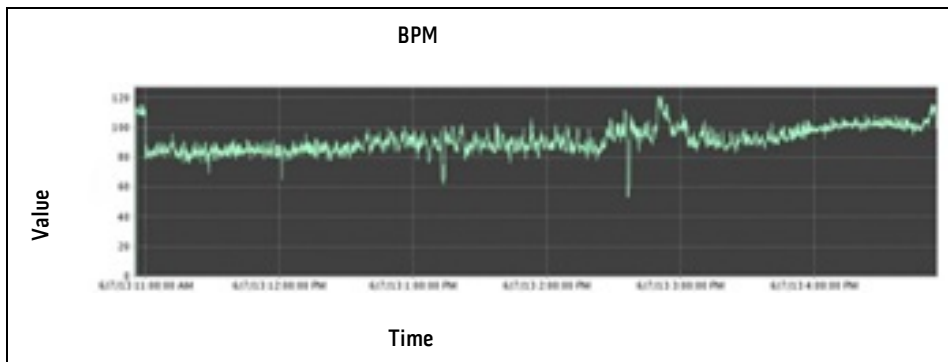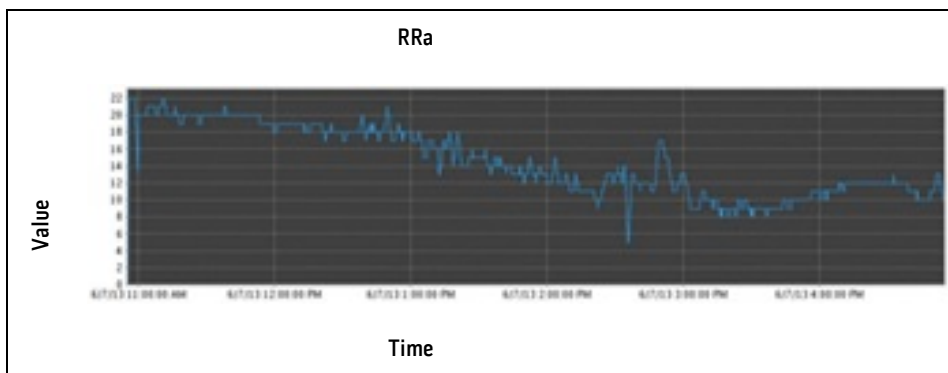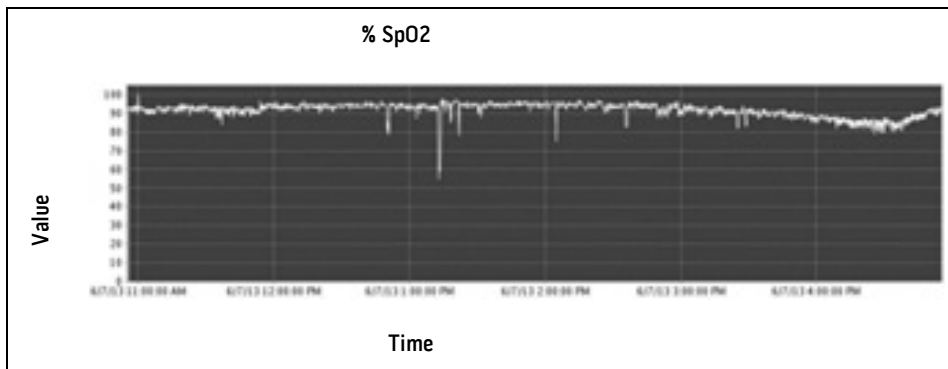
Data Export Report

The Data Export Report encapsulates system data for up to the previous 30 days.

Use Cases

- Provides the user the ability to extract the raw second by second data for each parameter and instrument for a patient.
- Provides the user the ability to create unique trends from raw data.

Generate Report

1. From the Report Type drop-down list, select data export report.

2.   From the Domain drop-down list, select the desired domain.

3.   Select Start Date and End Date.

4.   Select Apply

5.   Select desired patient in the Patient List.

6.   Select desired instrument in the Instrument List.

7.   Select Generate Report.

8.   Save .csv file in the desired location.

Patient Summary Report

The System Report encapsulates system data for up to 30 days for a specified time range within the previous year.

Use Cases

- Provides the user detailed event and notification information.*

- Provides the user the ability to determine how patient events turned into notifications.*

- Provides the user the ability to see which notification devices were alerted.*

- Provides the user with specific patient monitoring statistics.

- Provides the user the ability to determine what percentage of time the patient was being monitored.

- Provides the user the ability to determine how many events led to notifications.

   * Masimo Iris Gateway utilizes the Masimo Patient SafetyNet system report feature. Since Iris Gateway does not support notification delivery, any indication for notification in the report will not be applicable for Iris Gateway reports.

Generate Report

1.   From the Report Type drop-down list, select patient summary report.

2.   From the Domain drop-down list, select the desired domain.

3.   Select Start Date and End Date.

4.   Select desired parameters from the Parameter List.

5.   Select Generate Report.

6.   Select the desired patient from the Patient List.

7.   Select Generate Report.

Header Information: Patient Summary Report

The following is an example of the Header Information section.

Hospital Title

Hospital Address

Top Level Domain	Report Start Date
Parent Domain	Report End Date
Domain	Report Date

The following table defines the terms used in the Header Information section.

Terms	Description
Top Level Domain	The name of facility where the Iris Gateway server is located (configured during installation)
Domain	The domain where the patient is located in the system
Parent Domain	The parent domain where the patient is located in the system
Admit Date	The date and time that the patient was admitted to the system
Report Start Date	Start date and time selected for the report
Report End Date	End date and time selected for the report
Report Date	The date and time that the report was generated

Patient Information Report

The following is an example of the Patient Information Report.

Patient Information Report:

Patient Name
Instrument Name
Admit Date
Discharge Date
Admit Duration

The following table defines the terms used in the Patient Information Report.

Terms	Description
Patient Name	Name given to the patient during the admission process
Instrument Name	The name of the instrument that is connected to the patient
Admit Date	The date and time that the patient was admitted to the system
Discharge Date	The date and time that the patient was discharged to the system
Admit Duration	The elapsed time between Admit Date and Discharge Date

Patient Event List

The following is an example of the Clinical Events Report.

Patient Notification List*

Label	Cap Code	Start Time	Stop Time	Role	Number of Clinical Notifications	Number of Non Clinical Notifications

The following table defines the terms used in the Patient Notification List.*

Terms	Description
Label	Label given to notification device

Terms	Description
Cap Code	Cap Code for the notification device
Start Time	The time and date that the conditions for a type of event were met
Stop Time	The time and date that the conditions for a type of event were no longer met
Role	Whether the recipient of the notification was the primary, secondary, or supervisory
Number of Clinical Notifications	Number of Clinical Notifications in selected time frame
Number of Non Clinical Notifications	Number of Non Clinical Notifications in selected time frame

* Masimo Iris Gateway utilizes the Masimo Patient SafetyNet system report feature. Since Iris Gateway does not support notification delivery, any indication for notification in the report will not be applicable for Iris Gateway reports.

Reports Glossary

Clinical Events

Alarm Parameter	Notification	Definition
No Breath Detected	NO BREATH DETECTED	No breath detected. See capnography module Operator's Manual
SpO2 High	SPO2 HIGH	SpO2 parameter exceeds high threshold
SpO2 Low	SPO2 LOW	SpO2 parameter exceeds low threshold
SpfO2 High	SPFO2 HIGH	SpfO2 parameter exceeds high threshold
SpfO2 Low	SPFO2 LOW	SpfO2 parameter exceeds low threshold
PR High	PR HIGH	Pulse rate parameter exceeds high threshold
PR Low	PR LOW	Pulse rate parameter exceeds low threshold
RRa High	RRA HIGH	Acoustic respiration rate parameter exceeds high threshold
RRa Low	RRA LOW	Acoustic respiration rate parameter exceeds low threshold
RRp High	RRP HIGH	RRp parameter exceeds high threshold
RRp Low	RRP LOW	RRp parameter exceeds low threshold
EtCO2 RR High	ETCO2 RR HIGH	EtCO2 RR parameter exceeds high threshold
EtCO2 RR Low	ETCO2 RR LOW	EtCO2 RR parameter exceeds low threshold
EtCO2 High	ETCO2 HIGH	EtCO2 parameter exceeds high threshold
EtCO2 Low	ETCO2 LOW	EtCO2 parameter exceeds low threshold
SpHb High	SPHB HIGH	SpHb parameter exceeds high threshold
SpHb Low	SPHB LOW	SpHb parameter exceeds low threshold
SpCO High	SPCO HIGH	SpCO parameter exceeds high threshold

Alarm Parameter	Notification	Definition
SpCO Low	SPCO LOW	SpCO parameter exceeds low threshold
SpMet High	SPMET HIGH	SpMet parameter exceeds high threshold
SpMet Low	SPMET LOW	SpMet parameter exceeds low threshold
FiCO2 High	FICO2 HIGH	FiCO2 parameter exceeds high threshold
FiCO2 Low	FICO2 LOW	FiCO2 parameter exceeds low threshold
PVI High	PVI HIGH	PVI parameter exceeds high threshold
PVI Low	PVI LOW	SpCO parameter exceeds low threshold
PI High	PI HIGH	PI parameter exceeds high threshold
PI Low	PI LOW	PI parameter exceeds low threshold
SpOC High	SPOC HIGH	SpOC parameter exceeds high threshold
SpOC Low	SPOC LOW	SpOC parameter exceeds low threshold
PSI High	PSI HIGH	PSI parameter exceeds high threshold
PSI Low	PSI LOW	PSI parameter exceeds low threshold
Desaturation Index	DESAT INDEX	When Desaturation Index alarm is triggered based on user defined values, see Radical-7 Operator's Manual for more information.
PI Delta	PI DELTA	When PI Delta alarm is triggered based on user defined values, see Radical-7 Operator's Manual for more information.
All Mute	ALL MUTE	Device is in all mute state. See device Operator's Manual
No Sensor	NO SENSOR	A Sensor has not been detected
Defective Sensor	DEFECTIVE SENSOR / REPLACE SENSOR	Check/Replace Defective Sensor
Interference	INTERFERENCE	Light interference detected by pulse oximetry sensor. See sensor Directions For Use
Sensor Off	SENSOR OFF	Sensor is no longer on patient
Unrecognized Sensor	UNRECOGNIZED SENSOR	Unrecognized sensor has been detected
Incompatible Sensor	INCOMPATIBLE SENSOR	An Incompatible sensor has been detected
Check Sensor	CHECK SENSOR	Check connected sensor
No Cable Connected	NO CABLE CONNECTED	A cable has not been detected
Incompatible Cable	INCOMPATIBLE CABLE	Incompatible cable has been detected
Unrecognized Cable	UNRECOGNIZED CABLE	Unrecognized cable has been detected
Defective Cable	DEFECTIVE CABLE / REPLACE CABLE	Check/Replace Defective Cable

Alarm Parameter	Notification	Definition
Emitter Temp Out of Range	EMITTER TEMP OUT OF RANGE	The sensor emitter temperature is out of range of operation.
Sensor Current Limit Exceeded	SENSOR CURRENT LIMIT EXCEEDED	Sensor monitoring limit has been reached.
No Adhesive	NO ADHESIVE	Adhesive on sensor has not been detected
Incompatible Adhesive	INCOMPATIBLE ADHESIVE	An incompatible adhesive on sensor has been detected
Defective Adhesive	DEFECTIVE ADHESIVE	A defective adhesive on sensor has been detected
No Acoustic Sensor Connected	NO AC SENSOR	Acoustic sensor has not been detected
Defective Acoustic Sensor	DEFECTIVE AC SENSOR	A defective acoustic sensor has been detected
Respiratory Pause	RESP PAUSE	Acoustic sensor has detected a respiratory pause. See sensor Directions For Use
Acoustic Sensor Off Patient	AC SENSOR OFF	Acoustic sensor is no longer on patient
Bad Acoustic Sensor Placement	BAD AC SENSOR PLACEMENT	Check acoustic sensor placement. See sensor Directions For Use
Unrecognized Acoustic Sensor	UNRECOGNIZED AC SENSOR	Unrecognized acoustic sensor has been detected
Incompatible Acoustic Sensor	INCOMPATIBLE AC SENSOR	Incompatible acoustic sensor has been detected
No Acoustic Cable Connected	NO AC CABLE CONNECTED	Acoustic cable has not been detected
Incompatible Acoustic Cable	INCOMPATIBLE AC CABLE	Incompatible acoustic cable has been detected
Unrecognized Acoustic Cable	UNRECOGNIZED AC CABLE	Unrecognized acoustic cable has been detected
Defective Acoustic Cable	DEFECTIVE AC CABLE	A defective acoustic sensor cable has been detected
No AC Adhesive	NO AC ADHESIVE	Acoustic sensor adhesive has not been detected
Incompatible AC Adhesive	INCOMPATIBLE AC ADHESIVE	Incompatible acoustic sensor adhesive has been detected
Defective AC Adhesive	DEFECTIVE AC ADHESIVE	A defective acoustic sensor adhesive has been detected
(CO2) Sensor Error	SENSOR ERROR	Capnography module sensor error. See capnography module Operator's Manual
(CO2) Sampling Line Clogged	(CO2) SAMPLING LINE CLOGGED	Sampling line is clogged. See Nomoline Directions For Use
(CO2) Replace O2 Sensor	(CO2) REPLACE O2 SENSOR	Replace capnography module O2 sensor. See capnography module Operator's Manual
(CO2) Calibration Required	(CO2) CALIBRATION REQ	Capnography module requires calibration. See capnography module Operator's Manual

Alarm Parameter	Notification	Definition
(CO2) Temp Out Of Range	(CO2) TEMP OUT OF RANGE	Capnography module temperature is out of range. See capnography module Operator's Manual
(CO2) Pressure Out Of Range	(CO2) PRESSURE OUT OF RANGE	Capnography module pressure is out of range. See Capnography module Operator's Manual
(CO2) Zeroing Required	(CO2) ZEROING REQUIRED	Capnography module requires zeroing. See capnography module Operator's Manual
(CO2) No Sampling Line	(CO2) NO SAMPLING LINE	No sampling line detected. See Nomoline Directions For Use
(CO2) O2 Port Failure	(CO2) O2 PORT FAILURE	Capnography module port has failed. See capnography module and Masimo Root Operator's manual
Capnography Disconnected	O2 MODULE DISCONN	Capnography module is disconnected. See capnography module Operator's Manual
EMG No Cable	(EMG) NO CABLE	No Sedline cable detected. See Sedline Operator's Manual
EMG Incompatible Cable	(EMG) INCOMPATIBLE CABLE	Cable attached to Sedline module is incompatible. See Sedline Operator's Manual
EMG Cable Life Expired	(EMG) CABLE LIFE EXPIRED	Sedline cable has expired. See Sedline Operator's Manual
EMG Defective Cable	(EMG) DEFECTIVE CABLE	Sedline cable is defective. See Sedline Operator's Manual
EMG No Sensor	(EMG) NO SENSOR	No Sedline sensor detected. See Sedline Operator's Manual
EMG Incompatible Sensor	(EMG) INCOMPATIBLE SENSOR	Sensor attached to Sedline cable is incompatible. See Sedline Operator's Manual
EMG Sensor Life Expired	(EMG) SENSOR LIFE EXPIRED	Sedline sensor has expired. See Sedline Operator's Manual
EMG Defective Sensor	(EMG) DEFECTIVE SENSOR	Sedline sensor is defective. See Sedline Operator's Manual
EMG Sensor Off	(EMG) SENSOR OFF	Sedline sensor is off patient. See Sedline Operator's Manual
EMG No Tape	(EMG) NO TAPE	No Sedline sensor adhesive detected. See Sedline Operator's Manual
EMG Incompatible Tape	(EMG) INCOMPATIBLE TAPE	Sedline sensor adhesive is incompatible. See Sedline Operator's Manual
EMG Defective Tape	(EMG) DEFECTIVE TAPE	Sedline sensor adhesive is defective. See Sedline Operator's Manual
EMG Tape Life Expired	(EMG) TAPE LIFE EXPIRED	Sedline sensor adhesive has expired. See Sedline Operator's Manual
EMG High Impedance	(EMG) HIGH IMPEDANCE	High impedance detected. See Sedline Operator's Manual
EMG Gel Bridging	(EMG) GEL BRIDGING	Problem with Gel Bridging. See Sedline Operator's Manual
Improper Sensor Connection	(EMG) IMPROPER SENSOR CONN	Improper Sedline sensor connected. See Sedline Operator's Manual
Sedline Disconnected	SEDLINE DISCONNECTED	Sedline module disconnected. See Sedline and Masimo Root Operator's Manual
Low Battery	INST BATT LOW	Battery is low

NOTE: Displayed alarm parameters may depend on the monitoring bedside device.

Non-Clinical Events

Alert Parameter	Notification	Definition
All Mute	ALL MUTE	Instrument is in an All Mute state.
No Sensor	NO SENSOR	No sensor detected as being attached to the patient cable.
Defective Sensor	DEFECTIVE SENSOR / REPLACE SENSOR	Sensor appears to be defective.
Interference	INTERFERENCE	Ambient light interference is detected by sensor.
Sensor Off	SENSOR OFF	The sensor is off the patient.
Unrecognized Sensor	UNRECOGNIZED SENSOR	Instrument does not recognize sensor.
Check Sensor	CHECK SENSOR	Check the sensor placement to ensure that emitter and detector are in alignment.
No Cable Connected	NO CABLE CONNECTED	Cable is disconnected from the instrument.
Incompatible Cable	INCOMPATIBLE CABLE	Instrument is incompatible with cable.
Unrecognized Cable	UNRECOGNIZED CABLE	Instrument does not recognize cable.
Defective Cable	DEFECTIVE CABLE / REPLACE CABLE	Cable is defective.
Emitter Temp Out of Range	EMITTER TEMP OUT OF RANGE	The temperature of the sensor emitter is out of range.
Sensor Current Limit Exceeded	SENSOR CURRENT LIMIT EXCEEDED	The sensor has exceeded the current limit.
No Adhesive	NO ADHESIVE	Instrument does not detect adhesive.
Invalid Adhesive	INVALID ADHESIVE	Instrument detects invalid adhesive.
Defective Adhesive	DEFECTIVE ADHESIVE	The adhesive is defective.
No Acoustic Sensor Connected	NO AC SENSOR	Instrument does not detect acoustic sensor connected.
Defective Acoustic Sensor	DEFECTIVE AC SENSOR	The acoustic sensor is defective.
Respiratory Pause	RESP PAUSE	Sensor detects a respiratory pause longer than the user defined time period.
Acoustic Sensor Off Patient	AC SENSOR OFF	The acoustic sensor is disconnected from the patient.
Bad Acoustic Sensor Placement	BAD AC SENSOR PLACEMENT	The acoustic sensor is incorrectly placed.
Unrecognized Acoustic Sensor	UNRECOGNIZED AC SENSOR	Instrument does not recognize the acoustic sensor.
Incompatible Acoustic Sensor	INCOMPATIBLE AC SENSOR	The acoustic sensor is incompatible with the instrument.
No Acoustic Cable Connected	NO AC CABLE CONNECTED	There is not acoustic cable connected.
Incompatible Acoustic Cable	INCOMPATIBLE AC CABLE	The acoustic cable is incompatible with the instrument.
Unrecognized Acoustic Cable	UNRECOGNIZED AC CABLE	Instrument does not recognize acoustic cable.
Defective Acoustic Cable	DEFECTIVE AC CABLE	The acoustic cable is defective.

Alert Parameter	Notification	Definition
Low Battery	INST BATT LOW	The instrument battery is low.

Modifiers

Modifier Parameter	Notification	Definition
Patient Interference	PAT INTERFERENCE	Acoustic sensor detects interference from the patient.
Background Interference	BACKGROUND INTERFERENCE	Acoustic sensor detects interference from the room.
Low SIQ	SIQ LOW	Instrument detects low SIQ at sensor site.
Low Perfusion	LOW PERF	Instrument detects low perfusion at sensor site.
Low PR SIQ	LOW PR SIQ	Instrument detects low pulse rate SIQ at sensor site.
Low EtCO2 SIQ	LOW ETCO2 SIQ	Instrument detects low EtCO2 SIQ at sensor site.
Low RR Confidence	LOW RR SIQ	Instrument detects low confidence of respiration rate at sensor site.
Low RR Signal Strength	LOW RR SIG STR	Instrument detects weak signal of respiration rate at sensor site.
SpHb Low Confidence	LOW SPHB SIQ	Instrument detects low confidence of SpHb at sensor site.
SpCO Low Confidence	LOW CO SIQ	Instrument detects low confidence of SpCO at sensor site.
SpMet Low Confidence	LOW MET SIQ	Instrument detects low confidence of SpMet at sensor site.
Low FiCO2 SIQ	LOW FICO2 SIQ	Instrument detects low FiCO2 SIQ at sensor site.
Low PVI SIQ	LOW PVI SIQ	Instrument detects low Pleth Variability Index SIQ at sensor site.
Low PI SIQ	LOW PI SIQ	Instrument detects low Perfusion Index SIQ at sensor site.
Low SpOC SIQ	LOW SPOC SIQ	Instrument detects low SpOC SIQ at sensor site.
Low PSI SIQ	LOW PSI SIQ	Instrument detects low PSI SIQ at sensor site.

Chapter 5: Iris Gateway Connectivity Support

Iris ports in Masimo Root device allows a variety of standalone devices to connect to the Iris Gateway server. When standalone devices are connected to Iris Gateway server via the Iris port of Masimo Root, patient data can be passed through Masimo Root to Iris Gateway which can send the data to the patient's electronic health records.

How to Connect a Standalone Device Via Masimo Root

In order to connect a standalone device to Iris Gateway via Masimo Root Iris ports, please ensure you have the correct Iris Adapter for the make and model of the standalone device you wish to connect.

1. Ensure the standalone device is configured to output data. For more information on how to configure the standalone device to output data consult that standalone device's manual(s).

2. Connect the proprietary end of the Iris Adapter to the standalone device.

3. Connect the RJ-45 end of the Iris Adapter to any of the 4 compatible Iris Connectivity Ports on Masimo Root using an Ethernet cable.

Below is an example of one scenario in which a standalone device is connected to Iris Gateway via Masimo Root.

For more information on ensuring proper connection of standalone device to Masimo Root consult the Masimo Root Operator's Manual and the Iris Adapter Directions For Use.

Chapter 6: Troubleshooting

The following chapter contains information about troubleshooting Iris Gateway.

Issue	Resolution
Alarm and Vital listeners stop receiving data from Iris Gateway	• Check Keep Alive HL7 messages frequency • Check Connectivity with devices • Check if Unassigned HL7 Results Output option is not enabled, if not enabled, check if a patient is admitted • Check device network connection • Check device power on • Check if the Vitals out and Alarm Reporter services are enabled • Check Vitals out and Alarm listeners IP address and port
Alarm and Vital listeners are not receiving data from some devices	• Check if Unassigned HL7 Results Output is enabled • Check device network connection • Check if the devices are added to the system
Not receiving HL7 Alarm update message	• Check Alarm Publish Message Frequency
Alarm and Vital listeners are receiving outdated HL7 message	• Check server date/time
Alarm and Vital listeners are receiving incorrect location HL7 message	• Check the device location assignment

Chapter 7: Specifications

Iris Gateway Server

NOTE: Use only components and accessories approved by Masimo. The use of non-approved parts may produce unreliable system operation.

Server	
CPU	minimum Quad-Core 1.8 GHz, 10 MB L3 Processor Cache
Memory	minimum 4 GB RAM
Storage	minimum 1 TB HDD storage array
Management	Remote access capable
Operating System	Linux
Input/Output Connection	• USB • Redundant Gigabit 10/100/1000 BaseT Ethernet NICs
AC Power:	Redundant power supplies (110 - 240 VAC, 50/60 Hz)
Temperature, Operating	50° - 95° F (10° - 35° C)
Physical Dimensions (H x W x D):	3.44 x 17.64 x 27.50 in (8.75 x 44.80 x 69.88 cm)
Weight (approximate):	51.5 lbs. (23.36 kg)

Wireless Specifications

Communication	
Radio Standards	IEEE 802.11a/b/g TX Max Radiated EIRP FCC Part 15
Frequency Characteristics of Modulation	DSSS, OFDM
Encryption	WEP, TKIP, and AES
Authentication	Pre-Shared Key (PSK), EAP (TTLS, PEAP, and TLS); Mutual Authentication and Anonymous Outer Identity supported
Support Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54, and MCS Rates 0-7
AC Power	110 - 240 VAC, 50/60 Hz
Temperature, Operating	32 - 104 degrees F (0 - 40 degrees C)
Dimensions (L x W x H)	6.5 x 3.3 x 1.2 in (16.5 x 8.5 x 3.0 cm)

Radio Compliance	
FCC Part 15	Applicable components of this system have been labeled to comply with FCC Part 15.

Iris Gateway Mini

Mini-PC	
CPU	minimum Single-Core 2.3 GHz
Memory	minimum 4 GB RAM
Storage	minimum 512 GB HDD storage array
Operating System	Linux
Input/Output Connection	USB

Iris Gateway Virtual Machine

Host Device	
CPU	Minimum Quad-Core, 1.8 GHz
Memory	Minimum 8 GB RAM
Storage	Minimum 512 GB HDD storage array
Input/Output Connection	Access to one (1) USB port (for virtual port)

Supported Hypervisors	Version
VMware	V5.x
VMware	V6.x
KVM	REHEL7

Username	Password
configip	configme

Chapter 8: Service and Maintenance

Routine Maintenance

For all Iris Gateway components, refer to the product manufacturer's instructions for cleaning.

Service and Repair

Repair Policy

Masimo or an authorized Service Department must perform warranty repair and service. Do not use malfunctioning equipment. Have the device repaired.

Clean contaminated and/or dirty equipment before returning, follow the procedure described in the product manufacturer's instructions for cleaning. Make sure the equipment is fully dry before packing.

To return the device for service, refer to **Return Procedure** on page 67.

Return Procedure

Clean contaminated/dirty equipment before returning, follow the product manufacturer's instructions for cleaning. Make sure the equipment is fully dry before packing. Call Masimo at 800-326-4890 and ask for Technical Support. Ask for an RMA number. Package the equipment securely, in the original shipping container if possible, and enclose or include the following information and items:

- A letter describing in detail any difficulties experienced with the Iris Gateway. Include the RMA number in the letter.

- Warranty information, a copy of the invoice or other applicable documentation must be included.

- Purchase order number to cover repair if the Iris Gateway is not under warranty, or for tracking purposes if it is.

- Ship-to and bill-to information.

- Person (name, telephone/Telex/fax number, and country) to contact for any questions about the repairs.

- A certificate stating the Iris Gateway has been decontaminated for bloodborne pathogens.

- Return the Iris Gateway to the shipping address listed in the Contacting Masimo section below.

Contacting Masimo

Masimo Corporation
52 Discovery
Irvine, California 92618

Tel:+1 949 297 7000
Fax:+1 949 297 7001

Limited Warranty

Masimo warrants to the original end-user purchaser the Masimo-branded hardware product (Masimo® Iris Gateway) and any software media contained in the original packaging against defects in material and workmanship when used in accordance with Masimo's user manuals, technical specifications, and other Masimo published guidelines for a period of 12 months and any batteries for six (6) months from the original date the Product was obtained by the end-user purchaser.

Masimo's sole obligation under this warranty is the repair or replacement, at its option, of any defective Product or software media that is covered under the warranty.

To request a replacement under warranty, Purchaser must contact Masimo and obtain a returned goods authorization number so that Masimo can track the Product. If Masimo determines that a Product must be replaced under warranty, it will be replaced and the cost of shipment covered. All other shipping costs must be paid by purchaser.

Exclusions

The warranty does not apply to any non-Masimo branded product or any software, even if packaged with the Product, or any Product that was: (a) not new or in its original packaging when supplied to purchaser; (b) modified without Masimo's written permission; (c) supplies, devices, or systems external to the Product; (d) disassembled, reassembled, or repaired by anyone other than a person authorized by Masimo; (e) used with other products, like new sensors, reprocessed sensors, or other accessories, not intended by Masimo to be used with the Product; (f) not used or maintained as provided in the operator's manual or as otherwise provided in its labeling; (g) reprocessed, reconditioned, or recycled; and (h) damaged by accident, abuse, misuse, liquid contact, fire, earthquake or other external cause.

No warranty applies to any Product provided to Purchaser for which Masimo, or its authorized distributor, is not paid; and these Products are provided AS-IS without warranty.

Limitation of Warranty

Except as otherwise required by law or altered by the purchase agreement, the above warranty is the exclusive warranty that applies to the Product and software media, and Masimo does not make any other promises, conditions, or warranties regarding the Product. No other warranty applies, express or implied, including without limitation, any implied warranty of merchantability, fitness for a particular purpose, satisfactory quality, or as to the use of reasonable skill and care. See the licensing terms for the terms and conditions that apply to and Software accompanying the Product. Additionally, Masimo will not be liable for any incidental, indirect, special, or consequential loss, damage, or expense arising from the use or loss of use of any Products or Software. In no event shall Masimo's liability arising from any Product or Software (under contract, warranty, tort, strict liability, or otherwise) exceed the amount paid by purchaser for the Product or Software. The above limitations do not preclude any liability that cannot legally be disclaimed by contract.

Sales & End-User License Agreement

This document is a legal agreement between you ("purchaser") and Masimo Corporation ("Masimo") for the purchase of this Product ("Product") and a license in the included or embedded Software ("Software") except as otherwise expressly agreed in a separate contract for the acquisition of this Product, the following terms are the entire agreement between the parties regarding your purchase of this Product. If you do not agree to the terms of this agreement, promptly return the entire Product, including all accessories, in their original packages, with your sales receipt to Masimo for a full refund.

Restrictions

1. Copyright Restrictions: The Software and the accompanying written materials are copyrighted. Unauthorized copying of the Software, including Software that has been modified, merged, or included with other software, or the written materials is expressly forbidden. Purchaser may be held legally responsible for any copyright infringement that is caused or incurred by Purchaser's failure to abide by the terms of this Agreement. Nothing in this License provides any rights beyond those provided by 17 U.S.C. §117.

2. Use Restrictions: Purchaser may physically transfer the Product from one location to another provided that the Software is not copied. Purchaser may not electronically transfer the Software from the Product to any other device. Purchaser may not disclose, publish, translate, release, distribute copies of, modify, adapt, translate, reverse engineer, decompile, disassemble, or create derivative works based on the Software or the written materials.

3. Transfer Restrictions: In no event may Purchaser transfer, assign, rent, lease, sell, or otherwise dispose of the Product or the Software on a temporary basis. Purchaser shall not assign or transfer this License, in whole or in part, by operation of law or otherwise without Masimo's prior written consent; except that the Software and all of Purchaser's rights hereunder shall transfer automatically to any party that legally acquires title to the Product with which this Software is included. Any attempt to assign any rights, duties or obligations arising hereunder other than as set forth in this paragraph shall be void.

4. U.S. Government Rights: If Purchaser is acquiring Software (including the related documentation) on behalf of any part of the United State Government, the following provisions apply: the Software and documentation are deemed to be "commercial software" and "commercial computer software documentation," respectively pursuant to DFAR Section 227.7202 FAR 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software (including the related documentation) by the U.S. Government or any of its agencies shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

Appendix

Iris Gateway Virtual Machine Download and Installation

This procedure is to assist the user in installing and setting up a Virtual Machine for Iris Gateway on a host device.

Virtual Machine Installation Procedure

Download the Virtual Machine from the USB

1. Remove the USB drive from the packaging and plug the USB onto a computer.

2. Locate the Iris Virtual Machine file (.ova file).

3. Save the file to the computer in a location that can be easily found later in this procedure.

Import VM into VSphere

1. Follow the instructions in the vSphere documentation for importing OVA file.

    - **vSphere 5.5 -**
      https://docs.vmware.com/en/VMware-vSphere/5.5/com.vmware.vsphere.hostclient.doc/GUID-6C847F77-8CB2-4187-BD7F-E7D3D5BD897B.html

    - **vSphere 6.5 -**
      https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vm_admin.doc/GUID-17BEDA21-43F6-41F4-8FB2-E01D275FE9B4.html

Modify any Additional Settings

1. Depending on the environment, modify any other settings on the VM.

    NOTE: The CPU and Memory requirements of the VM are necessary. If these are modified, performance of the system is not guaranteed

Power on the VM

1. From the VM settings screen, select the *Power On* button.

Configure Static IP Address (Optional)

1. From the VM *Console* tab, click on the console screen.

2. Hit any key to continue. The following screen displays:


```
Red Hat Enterprise Linux Server release 6.5 (Santiago)
Kernel 2.6.32-431.el6.x86_64 on an x86_64

SafetyNet login: _
```

3. Login using the following default credentials.

    1. User: configip

    2. Password: configme

4. Follow the on-screen instructions to set the IP address:

    Note: Type *exit* at any time to leave the IP configuration.

1. Upon login, the user should see the following screen. Type 'y' and hit *Enter* on the keyboard to proceed.

```
Current network settings
eth0      Link encap:Ethernet  HWaddr 00:0C:29:18:B3:C7
          inet addr:10.1.40.120  Bcast:10.1.40.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe18:b3c7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:116 errors:0 dropped:0 overruns:0 frame:0
          TX packets:11 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7754 (7.5 KiB)  TX bytes:678 (678.0 b)


Would you like to change the ip address? (enter exit to leave): _
```

2. For the IP address, type in the static ip address as instructed, and hit *Enter* on the keyboard.

```
Enter IP address in dotted-decimal format (ex 192.168.1.120).
Press enter to leave unchanged:
```

3. For the subnet mask, type in the subnet mask as instructed, and hit *Enter* on the keyboard.

```
Enter subnet mask in dotted decimal format (ex 255.255.255.0).
Press enter to leave unchanged:
```

4. For the gateway, type in the gateway as instructed, and hit *Enter* on the keyboard.

```
Enter gateway IP address in dotted decimal format (ex 255.255.255.0).
Press enter to leave unchanged:
```

5. Confirm the changes to the network settings. The updated settings will be applied.

6. The screen returns to the initial screen and displays the new network settings.

Send IP Address to Masimo Service team

1. Email the configured IP address to the Masimo Services team Project Manager.

Connecting KEYLOK with VM for license management

1. Plug the KEYLOK into the host device where the VM is installed.

2. Follow the instructions in the vSphere documentation for adding a USB device to the VM.

Index