RESOURCE AND PATIENT MANAGEMENT SYSTEM

Master Patient Index Interface

(AGMP)

HealthShare Ensemble 2017
Management Portal Manual

Version 1.0
July 2021

Office of Information Technology
Division of Information Resource Management

Document Revision History

Date of Change	Location of Revision	Revision
June 2021	All sections	Complete update

Table of Contents

1.0 Introduction 1
1.1 Productions 1
1.2 Namespaces 2
1.3 Management Portal 2
2.0 Start Ensemble 3
3.0 Navigation 5
3.1 Choosing a Namespace 5
3.2 Management Portal Home Page 6
3.3 Switch Productions 7
4.0 Individual Productions 10
4.1 Production Status 10
4.1.1 Relevant Menus 11
5.0 Messaging 15
5.1 Status 15
5.2 View Messages 15
6.0 View Events 21
6.1 Event Log 21
7.0 Credentials Page 24
8.0 Starting and Stopping a Production 26
8.1 Start Production 26
8.2 Stop Production 27
8.3 Auto-Start Production 28
9.0 Purge Management 31
10.0 System Monitor 32
11.0 Ensemble E-Mail Alerts 33
11.1 Erroneous messages 33
11.2 Segment undefined or unknown 34
11.3 Other Message Types 34
Glossary 47
Acronym List 49
Contact Information 50

List of Tables

Table 4-1: Production Status 10
Table 5-1: Message status meanings.....15

List of Figures

Figure 2-1: Ensemble button 3
Figure 2-2: Start management of a production 3
Figure 2-3: Production Page 4
Figure 3-1: Navigation Banner 5
Figure 3-2: Namespace list 5
Figure 3-3: Namespace Chooser 6
Figure 3-4: AGMPI Production selected 6
Figure 3-5: Close current page 6
Figure 3-6: Navigation Banner 7
Figure 3-7: Productions Settings pane 7
Figure 3-8: Actions Tab 8
Figure 3-9: Finder Dialog 9
Figure 4-1: Menus – Services, Processes, Operations 12
Figure 4-2: MPIInbound production configuration 12
Figure 4-3: RPMSInBound production configuration 13
Figure 4-4: RPMSOutBound production configuration 13
Figure 4-5: MPIOutBound 14
Figure 5-1: Ensemble – view all production messages 16
Figure 5-2: Message Viewer 16
Figure 5-3: Message details 17
Figure 5-4: HL7 message 18
Figure 5-5: Message flow through Ensemble 19
Figure 5-6: Visual Trace window 20
Figure 5-7: Visual Trace window - contents tab selected 20
Figure 6-1: Open Event Log 21
Figure 6-2: Events Log 22
Figure 6-3: Quick Search parameters 22
Figure 6-4: Event Types 23
Figure 7-1: Navigate to Credentials 24
Figure 7-2: Credentials Viewer 25
Figure 8-1: Production Configuration page – production running 26
Figure 8-2: Dialog box – start production 26
Figure 8-3: Start Production window 27
Figure 8-4: Production Configuration page - production suspended 27
Figure 8-5: Dialog box - stop production 28
Figure 8-6: Stop Production window 28
Figure 8-7: Management Portal 29
Figure 8-8: Auto-Start Production page 29
Figure 8-9: Auto-Start Production page - Apply 30
Figure 10-1: System Monitor 32
Figure 10-2: Systems Monitor page 32
Figure 11-1: Ensemble e-mail alert for MPIInbound 33

Figure 11-2: Ensemble e-mail alert for AGMPI.MPIMessageRouting 34
Figure 11-3: Ensemble e-mail error alert 34
Figure 11-4: Configuration Error Message 35
Figure 11-5: HLB global Error Message....35
Figure 11-6: HLA global Error Message 35
Figure 11-7: HL7 Error Message....35
Figure 11-8: HLOGlobalInbound Adapter Error Message 35
Figure 11-9: HLB global in the HLOGlobalOutbound Error Message 35
Figure 11-10: HLA global in the HLOGlobalOutbound Error Message 35
Figure 11-11: ACK without a Message Control ID Error Message 35
Figure 11-12: L ACK without a B reference node Error Message....35
Figure 11-13: Missing AA or CA ACK Code Error Message 36
Figure 11-14: Failure to find an open IEN Error Message....36
Figure 11-15: Failure with MessageID in HL7 Error Message....36
Figure 11-16: HLOGlobalOutbound adapter Error Message....36
Figure 11-17: HLOGlobal Patient Record Number Error Message 36
Figure 11-18: Patient Record Number Error Message for A01....36
Figure 11-19: Patient Record Number Error Message for A03....36
Figure 11-20: HLOGlobalOutbound adapter error....36
Figure 11-21: TCP Read timeout error 36
Figure 11-22: TCP Connect timeout error 37
Figure 11-23: No connection error 37
Figure 11-24: Failure to process message error....37

Preface

The purpose of this manual is to provide information about using the *Management Portal*. This manual has been written to allow users to monitor the Ensemble Integration Engine. However, the Beta testing process has identified that users should not use these features but instead should use the ***full*** Ensemble System Management Portal and the Management Portal for the Integration Engine.

1.0 Introduction

For over two decades, hospitals and health centers of the Indian Health Service (IHS) and numerous tribal health programs have used an information system called the Resource and Patient Management System (RPMS). RPMS is a highly integrated system consisting of some 50 health care and administrative applications. Virtually all these applications directly interact with one or more, and sometimes many, of the other RPMS applications.

RPMS applications are required to interact with the Master Patient Index (MPI) to meet the needs of the IHS MPI initiative. The RPMS/HL7-Optimized (HLO) interface is a way to send patient information Admission, Discharge, Transfer (ADT) to the MPI and to receive treating facility information from the MPI and store it into the RPMS database.

This manual describes the tools that are provided to manage and monitor the Ensemble Integration Engine (EIE). The first section describes how to use the portal in the management of the interface. The second section describes the portal in more technical detail for Office of Information Technology (OIT) personnel to assist the user in configuring the EIE and in troubleshooting problems.

> **Note:** Detailed instructions for installing and configuring the AGMP production in Ensemble are found in the *Patient Registration MPI Interface/Ensemble (AG) Installation Guide and Release Notes*.

1.1 Productions

A *production*, the unit of delivery for Ensemble-based development projects, is a package of host classes and configuration items that solves a specific integration problem for an enterprise.

The AGMP interface sends messages between RPMS and the MPI system to maintain the integrity and accuracy of patient records. The AGMPI.PatientRegistration production uses the Management Portal to provide a suite of tools for managing, monitoring, and troubleshooting the message transport between the two systems.

Productions can be started, stopped, configured, and monitored from the Management Portal using Ensemble. In addition, errors such as messaging errors and connection errors trigger e-mail alerts from EIE.

1.2 Namespaces

A *namespace* is a collection of one or more productions. The AGMPxxx namespace is created during the AGMP installation process (where "xxx" is the site's production namespace).

Warning: All system-provided namespaces except ENSEMBLE and USER are overwritten upon reinstallation or upgrade. For this reason, InterSystems recommends creating new namespaces, rather than placing custom code in any of the system-provided namespaces, where it could be overwritten and lost.

1.3 Management Portal

The Management Portal provides access to the tools and components required to manage the AGMP namespace and the AGMPI.PatientRegistration production instance.

Warning: It is critical to get permission from OIT before running a production instance. The patient bulk load file must be activated by OIT before running any Ensemble production instance.

It is highly recommended that sites use the full Management Portal to properly monitor productions.

2.0 Start Ensemble

There are multiple ways to enter Ensemble. To see individual production configurations, follow the steps below.

1. Click on the **Ensemble** button in the menu list on the left of the Management Portal page (Figure 2-1, yellow highlight).

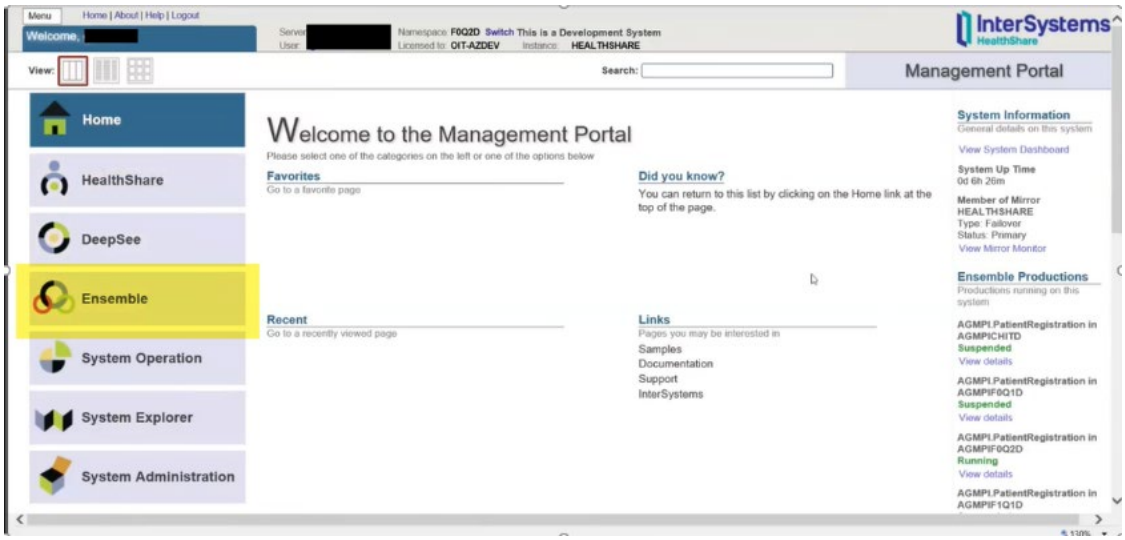

Figure 2-1: Ensemble button

2. To start management of a production, click on **Configure** then click on **Production**. The **Production** page opens (Figure 2-3).

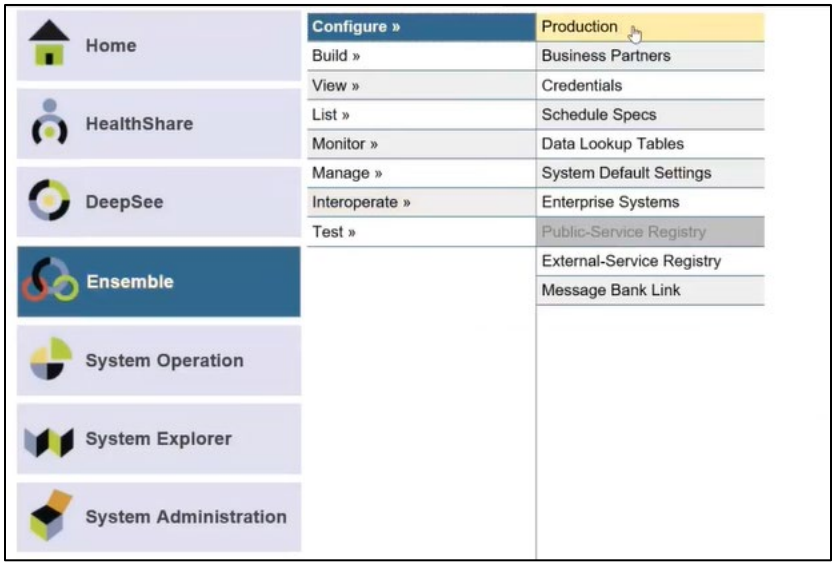

Figure 2-2: Start management of a production

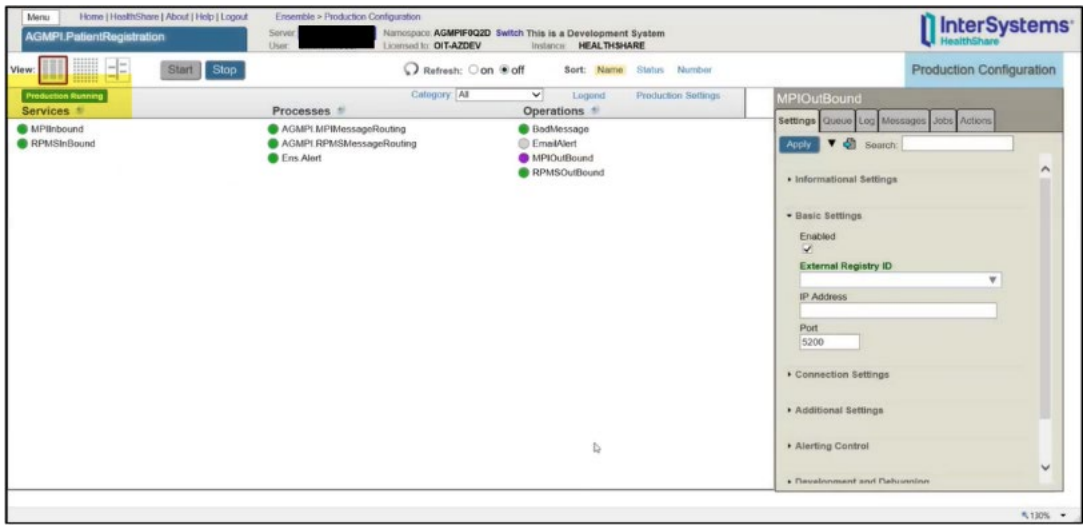

Figure 2-3: Production Page

3.0 Navigation

The Management Portal has multiple ways to navigate to productions. The banner at the top is key to navigation (Figure 3-1).

Figure 3-1: Navigation Banner

3.1 Choosing a Namespace

The Management Portal has a Namespace item at the top of the display area, as shown in Figure 3-2 (yellow highlight). To choose a Namespace, do the following:

1. Click on **Switch** (Figure 3-2, yellow highlight).

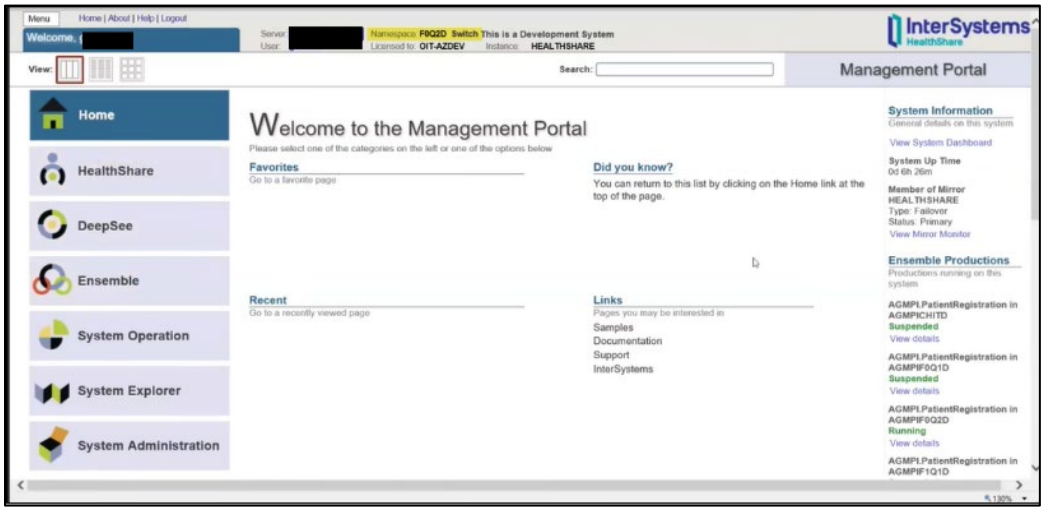

Figure 3-2: Namespace list

2. Select an AGMPI Namespace in the **Namespace Chooser** (Figure 3-3). Click **OK**.

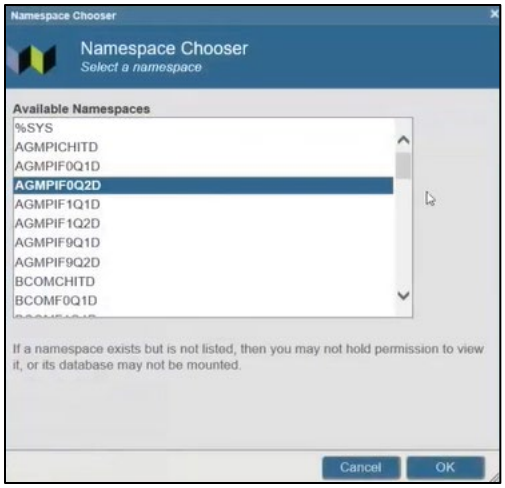

Figure 3-3: Namespace Chooser

3. The **Namespace** at the top of the Management Portal should now contain the AGMPI production (Figure 3-4).

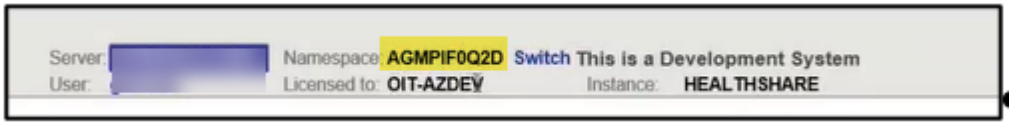

Figure 3-4: AGMPI Production selected

3.2 Management Portal Home Page

To reach another part of Ensemble while you are within Ensemble, return to the **HEALTHSHARE - Home** page (Figure 3-2).

1. At the very top of the page, the current page is highlighted in light blue. If you do not see the **Navigation Banner** (Figure 3-6), close the current page by clicking the **x** next to its name (Figure 3-5, green arrow). If necessary, close all pages until the **Navigation Banner** is visible.

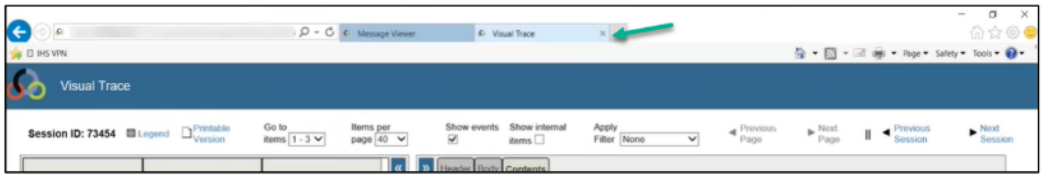

Figure 3-5: Close current page

2. Click **Ensemble** from the list at the top of the **Navigation Banner** (Figure 3-6). This will open the **HEALTHSHARE - Home** page (Figure 3-2).

Figure 3-6: Navigation Banner

3.3 Switch Productions

While managing a production it may be necessary to switch to another production from the **Productions Configuration** page.

1. From the **Production Configuration** page (see Section 2.0), go to the **Production Settings** pane and click on **Actions** (Figure 3-7).

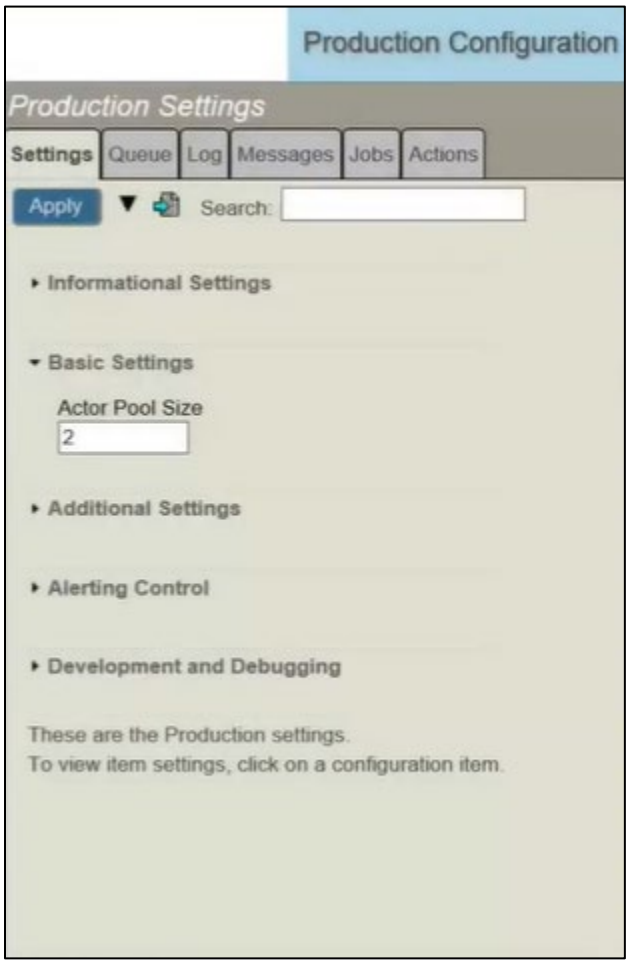

Figure 3-7: Productions Settings pane

2. On the **Actions** tab, click **Open** (Figure 3-8).

Figure 3-8: Actions Tab

3. In the **Finder Dialog** box, click on **AGMPI** then **PatientRegistration** (Figure 3-9). The new production opens in the **Production Configuration** window.

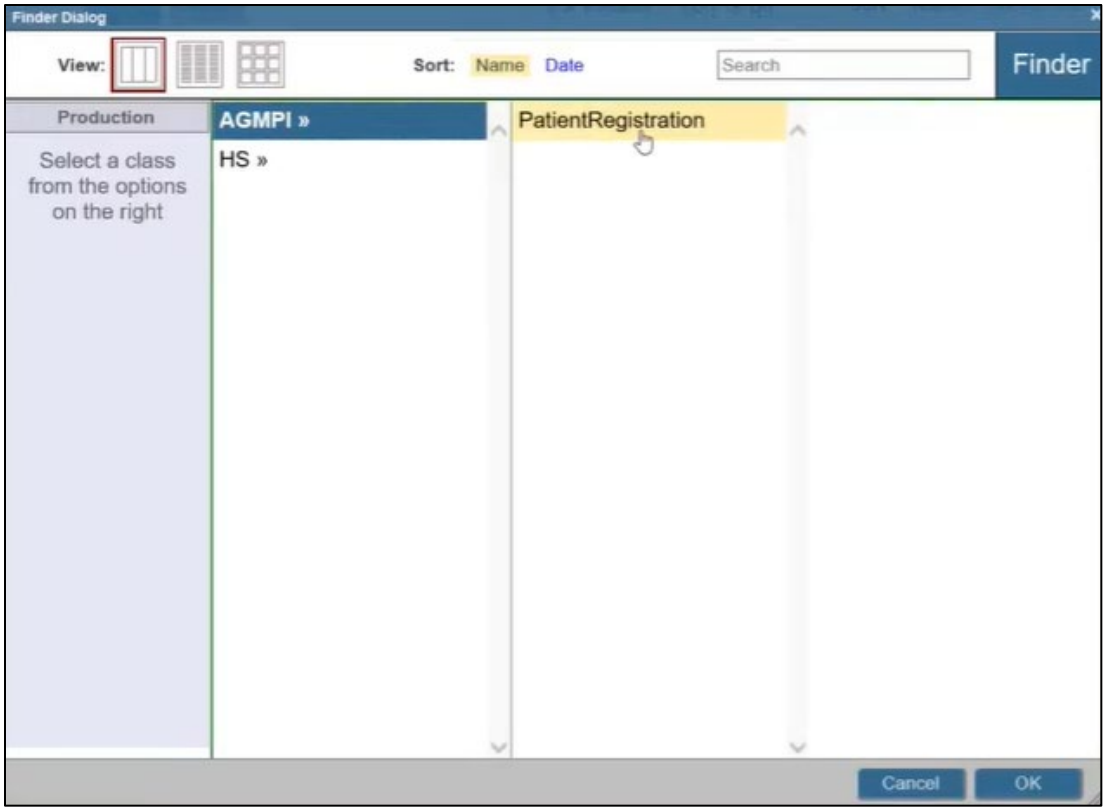

Figure 3-9: Finder Dialog

4.0 Individual Productions

This section addresses how to see details for individual productions. The other sections of this manual discuss how to view all production information at once and sort and filter that information.

There are three menu options available after going through the steps in Sections 2.0 and 3.0. The options are **Services**, **Processes**, and **Operations** (Figure 4-1).

> **Note:** Detailed instructions for using a production's configuration pages are found in the *Patient Registration MPI Interface/Ensemble (AG) Installation Guide and Release Notes*.

4.1 Production Status

Any changes made to a production while it is running are applied immediately, without requiring the stop and restart of the production. When a production is running, monitoring and diagnostic tasks can be performed from the Management Portal.

Always monitor Outlook e-mail for alerts from Ensemble. See Section 11.0 for information about Ensemble e-mail alerts.

The possible statuses for a production are listed in Table 4-1.

Table 4-1: Production Status

State	Meaning
Not running, enabled	When the production is stopped, no messages are processed by the production. It may be necessary to stop the production at times. However, the production should normally be in a Running state.
Running	When a production has been started and is operating normally, it has a status of Running. This is an acceptable state.

State	Meaning
Disabled	A production acquires the Suspended status if, at the end of the shutdown sequence, some queues still contain synchronous messages, waiting for a response. Depending on how the production has been designed, this may or may not indicate a problem. A Suspended production can be started. Starting the production again may permit the waiting messages to be processed. However, if the Suspended production is started, and more messages arrive while those in front of them in the queue cannot be resolved, queues may simply continue to fill. In that case investigate to discover why the incoming messages never complete. A Suspended production may be stopped. InterSystems advises stopping a production only during initial development and not on a deployed, live installation. For instructions, see the Stopping a Suspended Production section in the "Creating a New Production" chapter.
Error	Ensemble is stopped but the production did not shut down properly. This could happen if you restarted Ensemble or rebooted the machine without first stopping the production. In this case you need to issue a command to recover the production.
Retrying	When the production is unable to communicate with the central server, the business host may show a Retrying status. This is an acceptable state.
Inactive	At the end of the shutdown sequence, all of its queues are free of synchronous messages. This is an acceptable state.

4.1.1 Relevant Menus

The main items, **Services**, **Processes**, and **Operations** are shown in Figure 4-1. The relevant submenus are discussed below.

> **Note**: Each of the tabs in the dialog box shows data *only* for the chosen production.

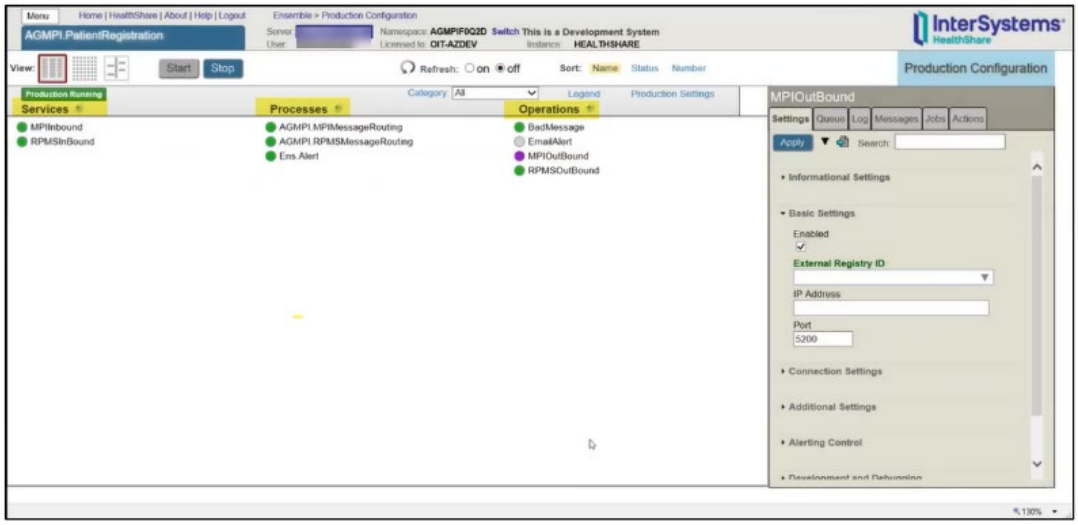

Figure 4-1: Menus – Services, Processes, Operations

1. **Services**

   a. Click on **MPIInbound**. The dialogue box at the right opens (Figure 4-2).

   MPIInbound is a business service that receives MPI messages from the central MPI and routes them to the RPMSOutbound business operation

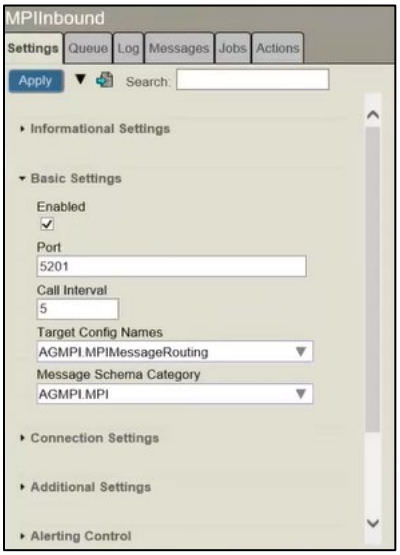

Figure 4-2: MPIInbound production configuration

   b. Click on **RPMSInBound**. The dialogue box at the right opens (Figure 4-3).

   RPMSInBound is a business service that retrieves MPI messages from the outbound HLO queue and routes them to the MPIOutbound business operation

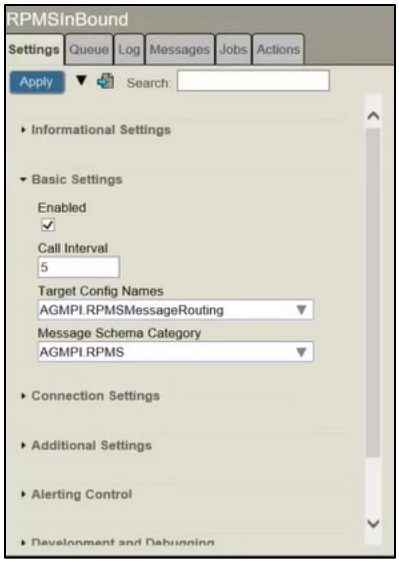

Figure 4-3: RPMSInBound production configuration

2. **Operations**

   a. Click on **RPMSOutBound**. The dialogue box at the right opens (Figure 4-4).

   RPMSOutBound is a business operation that receives MPI messages from MPIInbound and files them into the inbound HLO queue for processing

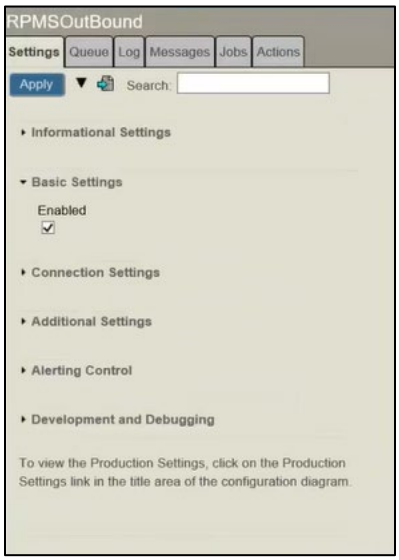

Figure 4-4: RPMSOutBound production configuration

   b. Click on **MPIOutBound**. The dialogue box at the right opens (Figure 4-5).

   MPIOutBound is a business operation that receives MPI messages from RPMSInbound and uploads them to the central MPI

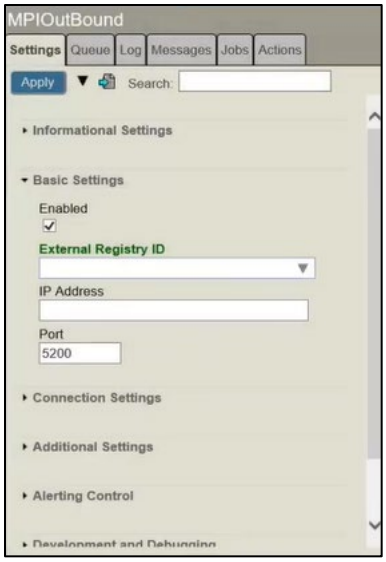

Figure 4-5: MPIOutBound

5.0 Messaging

All communication that passes between configuration items in Ensemble is accomplished using messages.

5.1 Status

The status of a message within its normal life cycle can have several values: Created, Queued, Delivered, Deferred, Completed, Discarded, or Suspended.

Table 5-1: Message status meanings

Message Status	Meaning
Completed	The intended recipient has received the message and has finished processing the message.
Created	The message is in transit between sender and target.
Deferred	The message response has been deferred by the business operation for later delivery.
Delivered	The intended recipient has received the message.
Discarded	The message is a response that reached its destination after the timeout period for the corresponding request expired.
Queued	The message is on a queue.
Suspended	The message was suspended by the business operation after failing to reach its external destination, or by an administrator from the Instances display on the **Host Monitor** page. In either case, the message can be resent from clicking **Maintenance** and then Suspended Messages or by clicking **Resend Messages** on the **Messages** page.

5.2 View Messages

Follow the steps below to manage all productions at once.

1. After clicking on **Ensemble**, click on **View**, then **Messages** (Figure 5-1).

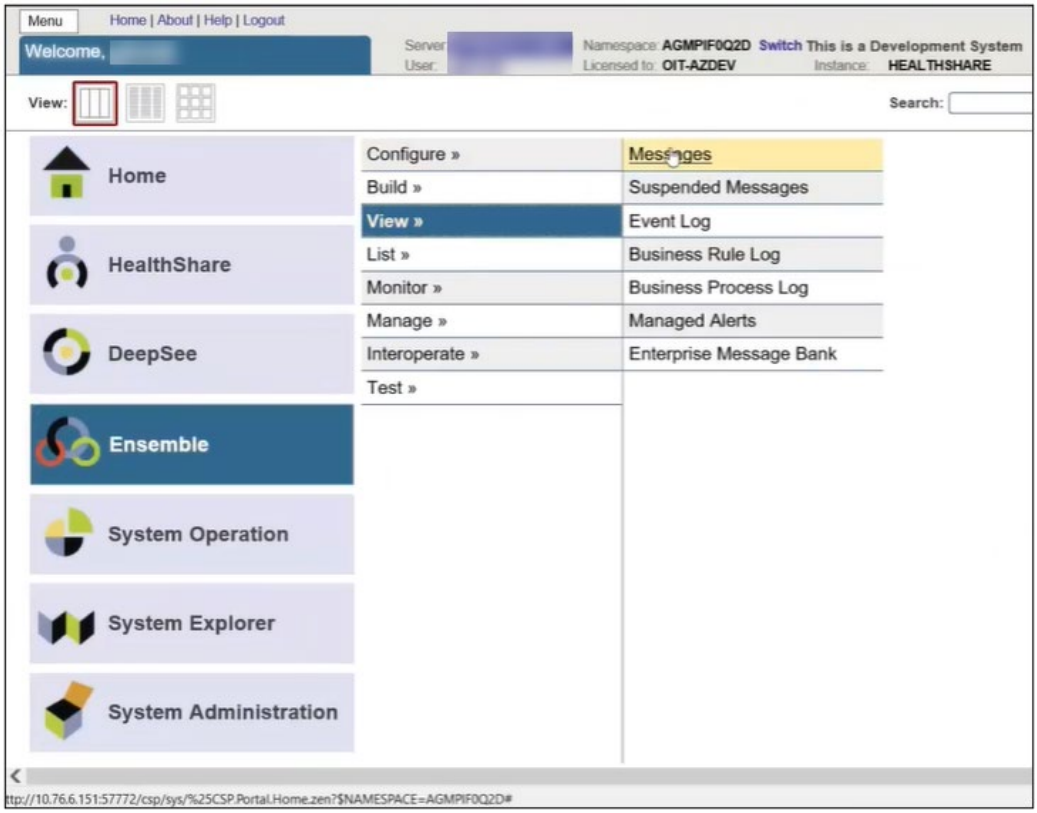

Figure 5-1: Ensemble – view all production messages

2. The **Message Viewer** page opens (Figure 5-2).

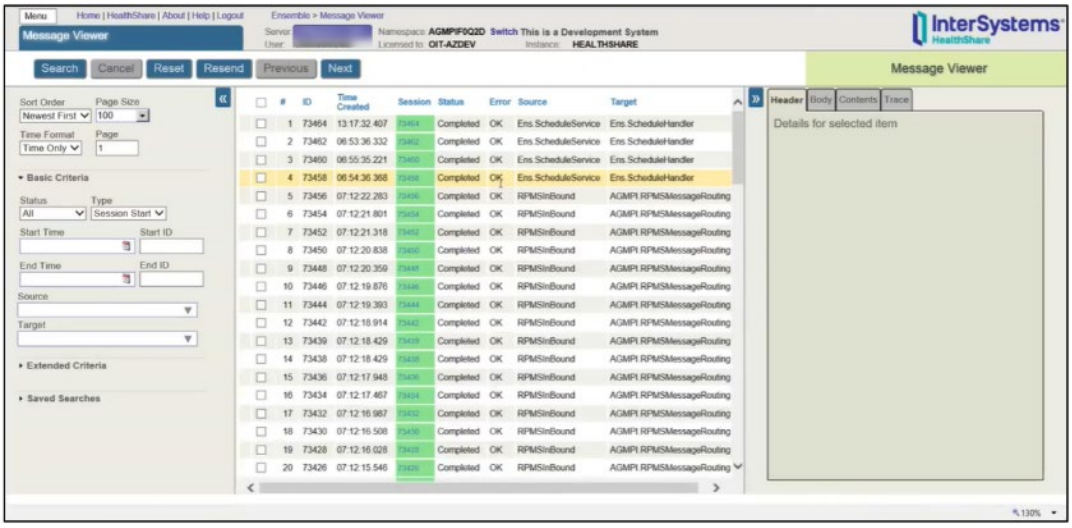

Figure 5-2: Message Viewer

3. Click on a message to see the details for that message (Figure 5-3).

4. Click on the **Contents** tab to see the HL7 message (Figure 5-3, green arrow). The HL7 message opens (Figure 5-4).

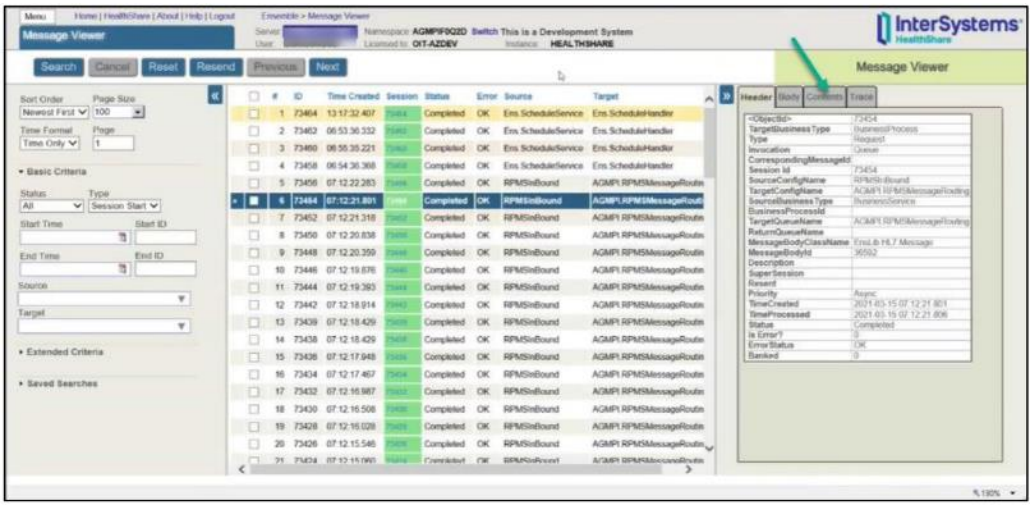

Figure 5-3: Message details

5. To view the content detail of the HL7 message, click on **View Full Contents** or **View Raw Contents** (Figure 5-4).

> **Note**: **View Full Contents** shows the HL7 message with links to supporting documentation explaining the elements. **View Raw Contents** shows only the unformatted data.

6. Click on the **Trace** tab (Figure 5-4, green arrow) to see the flow of the message through Ensemble.

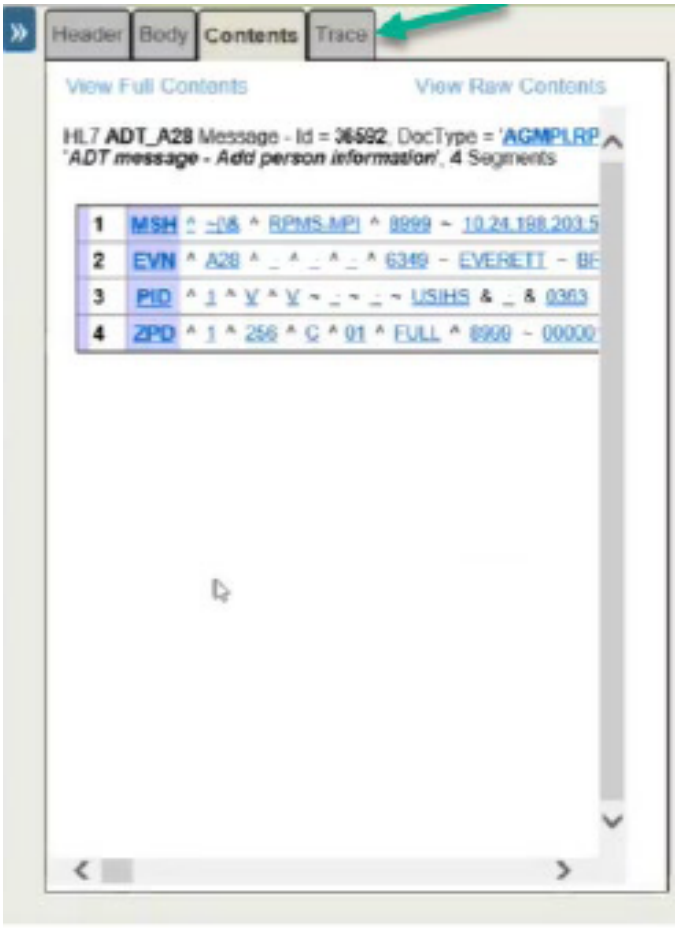

Figure 5-4: HL7 message

7. Click on **View Full Trace** (Figure 5-5, green arrow) to see details.

Figure 5-5: Message flow through Ensemble

8. The **Visual Trace** window has two panes (Figure 5-6). The left pane shows the trace and displays a graphic representation of the **Services**, **Processes**, and **Operations** related to the selected message. Clicking on any of the elements in the trace brings up the details for that element. The right pane shows one of three tabs: **Header**, **Body**, **Contents**.

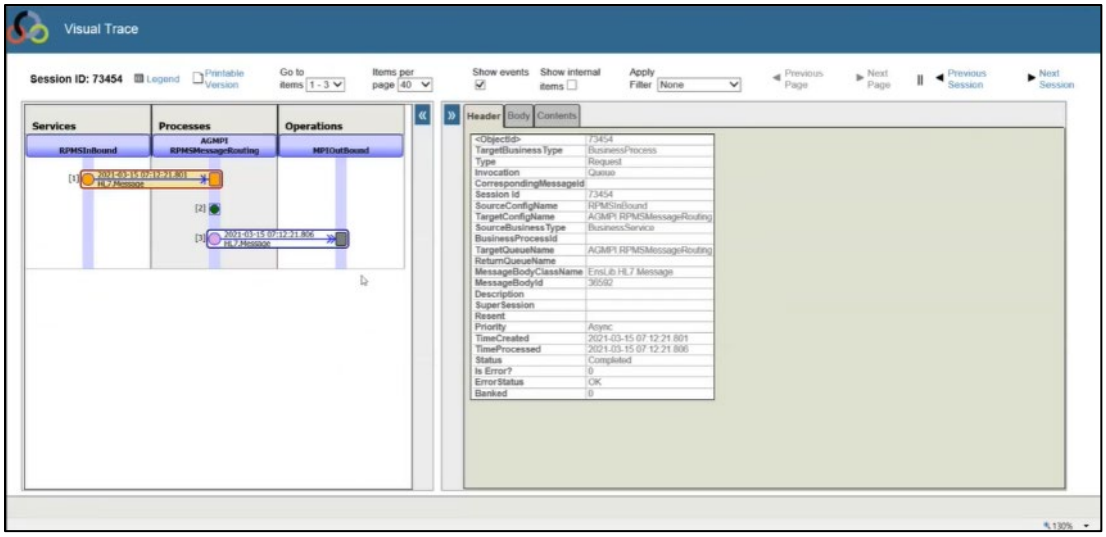

Figure 5-6: Visual Trace window

9. Click on **Contents** (or another tab) to see details (Figure 5-7).

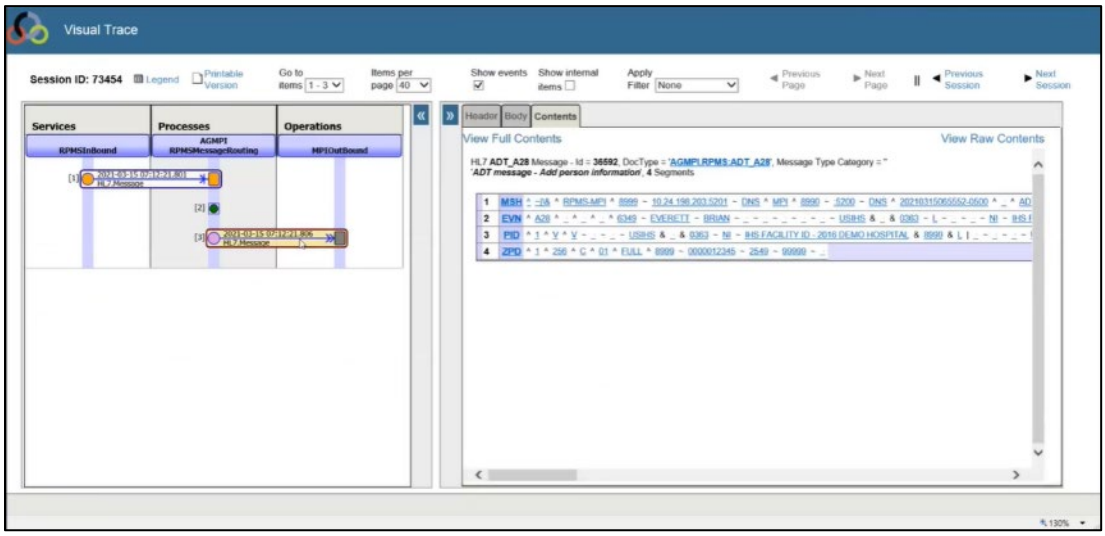

Figure 5-7: Visual Trace window - Contents tab selected

6.0 View Events

The Ensemble event log does not provide any information about Ensemble system events. The event log collects certain types of text messages generated by Ensemble host classes. A developer or system administrator can view event log entries from the **Event Log** page.

Events listed in the event log are color-coded using the colors shown below.

Table 6-1: Colors associated with event status in the Event Log

Event Status	Color
Alert	Yellow
Error	Red
Warning	Orange
Info	Green
User Trace	Blue

6.1 Event Log

Start at the **HEALTHSHARE - Home** page (see Section 3.2 for navigation tips).

1. Click on **Ensemble**, **View** and then **Event log** (Figure 6-1).

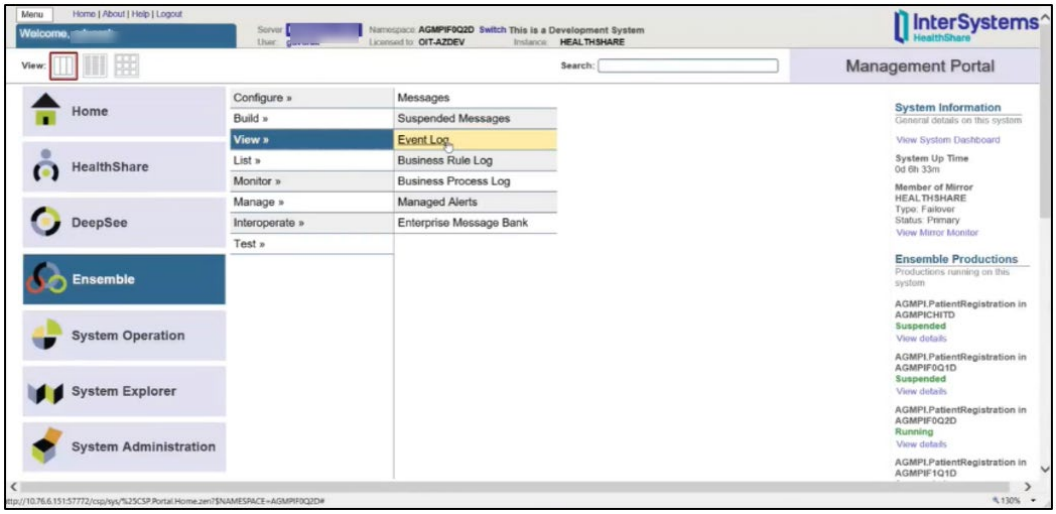

Figure 6-1: Open Event Log

2. The Event Log can be searched in three ways: **Quick Search**, **Event Types**, and **Search Events By…** (Figure 6-2).

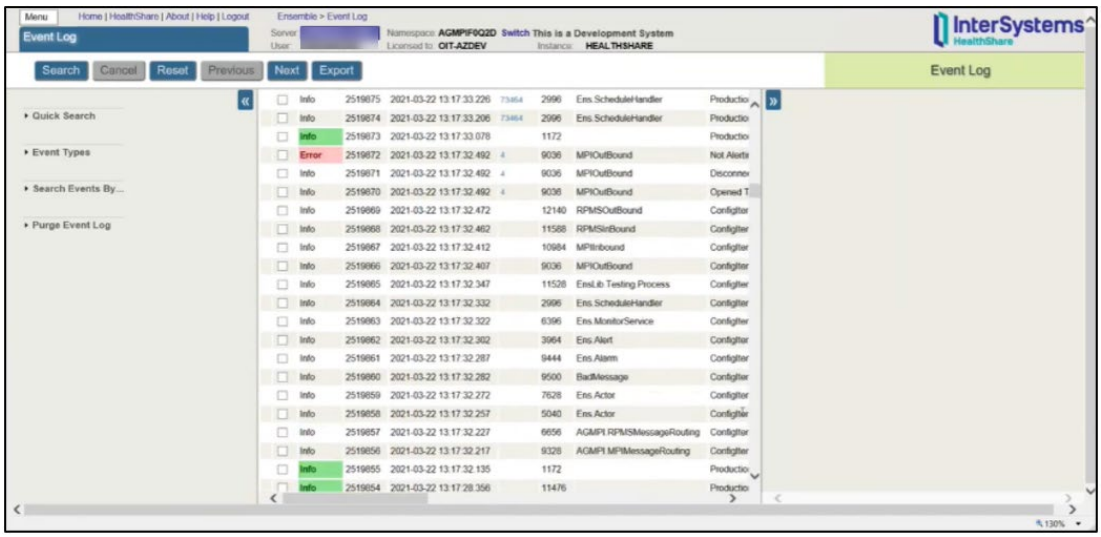

Figure 6-2: Events Log

3. Click on **Quick Search** (Figure 6-2). The search details are visible and parameters for the search can be chosen by clicking on the drop-down menus (Figure 6-3).

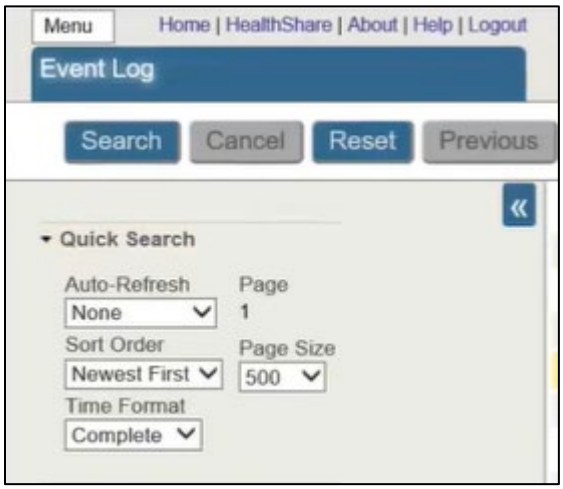

Figure 6-3: Quick Search parameters

4. Click on **Event Types** (Figure 6-2).

5. All types are selected by default. Check only the boxes next to the type that will be viewed (Figure 6-4). In this case, Error is chosen, and the message list only displays error messages.

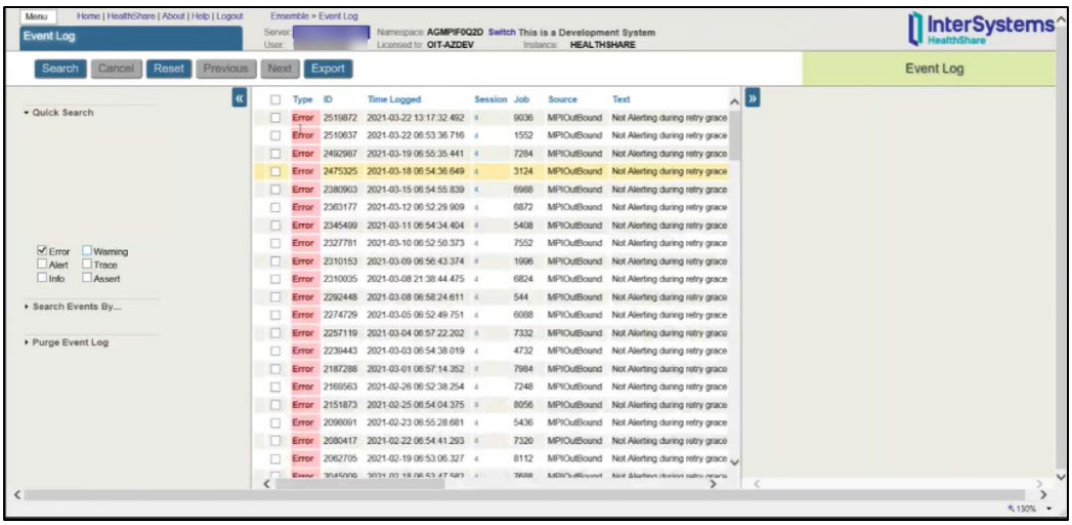

Figure 6-4: Event Types

7.0 Credentials Page

Ensemble stores and uses login credentials in place of the username and password to access remote systems.

Each login credential is associated with a unique ID supplied during configuration that identifies the role of the user and is associated with that user's username and password.

Using the unique ID, an adapter retrieves the username and password from the Credentials table, and then sends them to the remote system with a request to login.

Credentials can only be created or edited by navigating to the Credentials page (Figure 7-1).

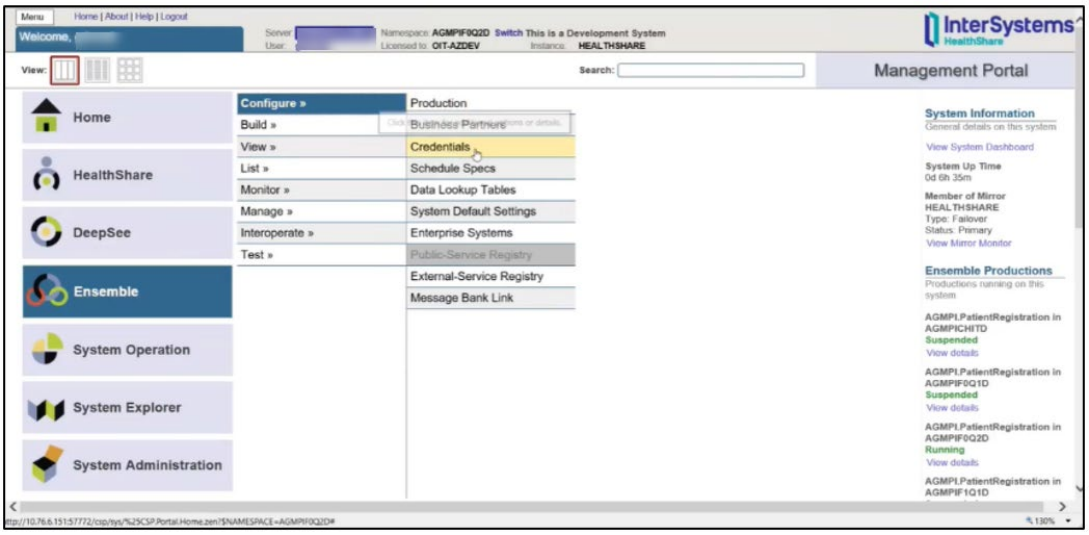

Figure 7-1: Navigate to Credentials

Credentials can be created or removed from within the **Credentials Viewer** (Figure 7-2).

Figure 7-2: Credentials Viewer

Note: Detailed instructions for configuring a production using the configuration pages, including specifying **credentials**, are found in the *Patient Registration MPI Interface/Ensemble (AG) Installation Guide and Release Notes* (ag__0720.01o_ens2012.pdf).

8.0 Starting and Stopping a Production

Only one production can be run at a time. If it is necessary to change productions, see Section 3.3.

8.1 Start Production

1. Enter Ensemble following the steps in Section 2.0. If the production is running (Figure 8-1, golden arrow), it must be stopped before another can be started. Click **Stop** (Figure 8-1, green arrow).

   a. If a stopped or suspended production is initially opened, click **Start** (Figure 8-4, green arrow).

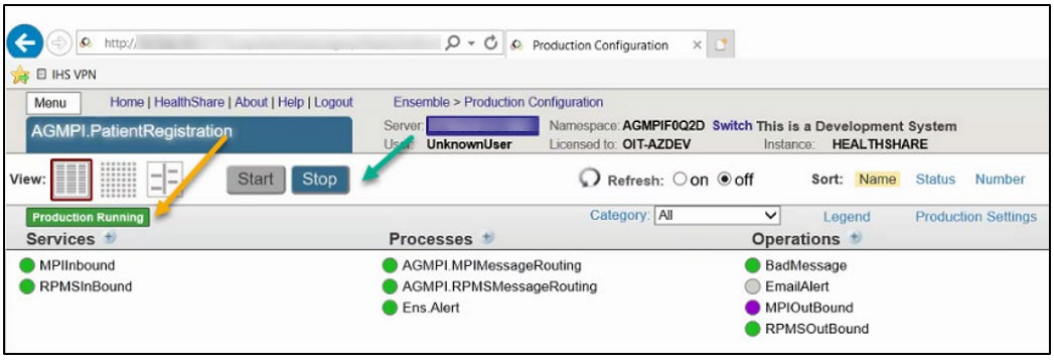

Figure 8-1: Production Configuration page – production running

2. A dialog box opens with the question **Do you want to start this Production?** Click **OK** (Figure 8-2).

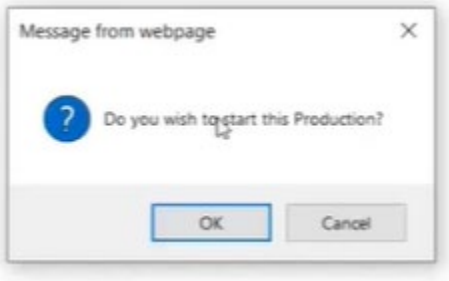

Figure 8-2: Dialog box – start production

3. The **Start Production** window opens. Click **OK** (Figure 8-3).

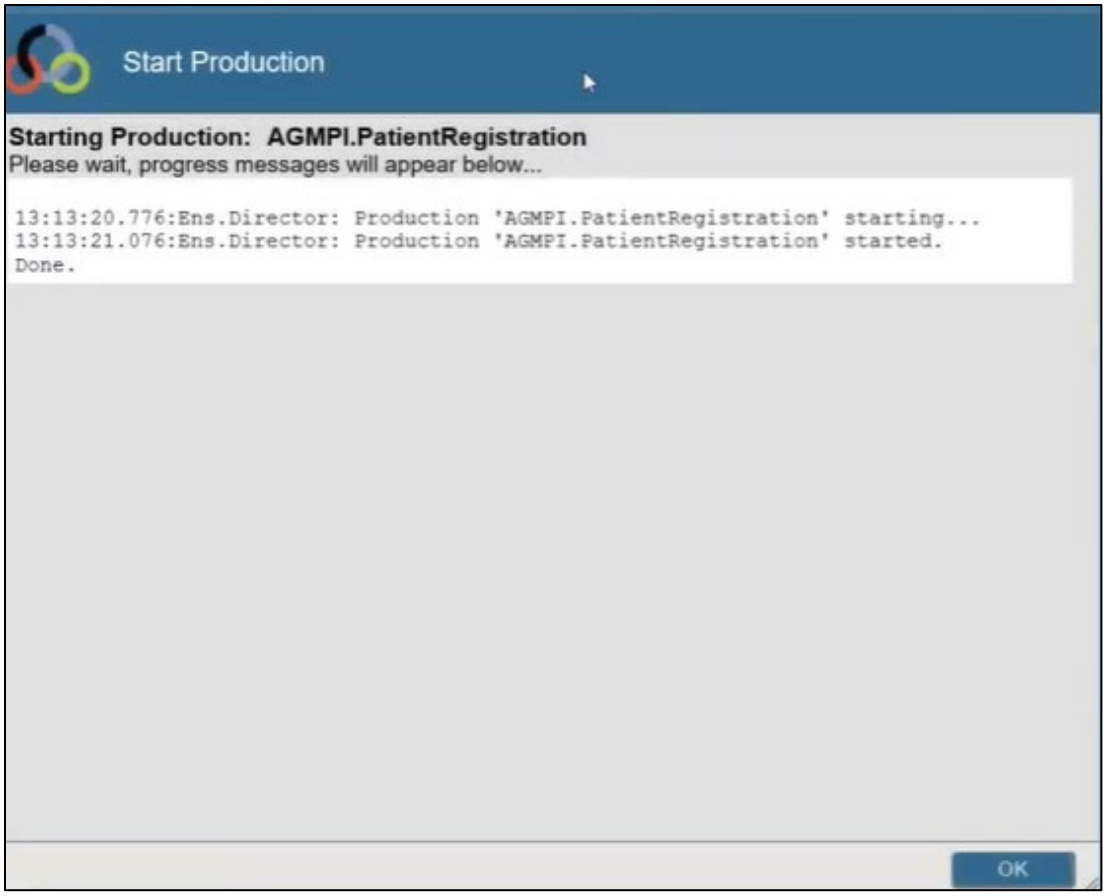

Figure 8-3: Start Production window

8.2 Stop Production

1. Choose a new namespace (see Section 3.1). Click **Start** (Figure 8-4, green arrow).

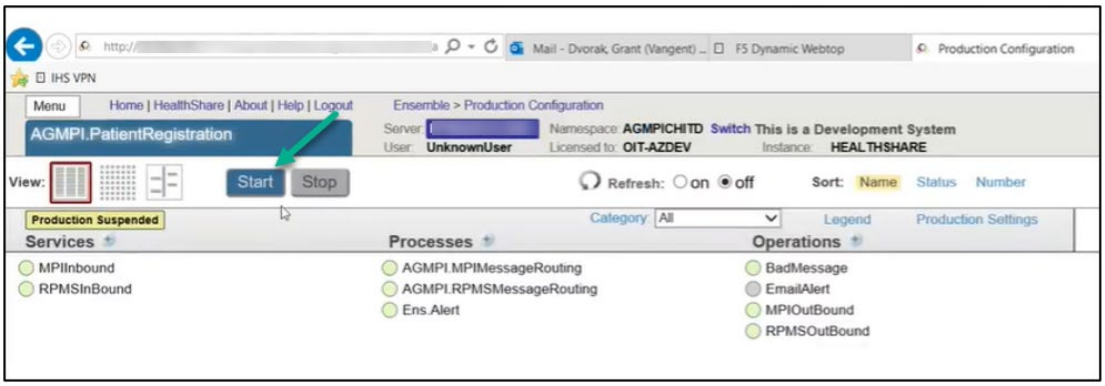

Figure 8-4: Production Configuration page - production suspended

2. A dialog box opens with the question **Do you want to stop this Production?** Click **OK**.

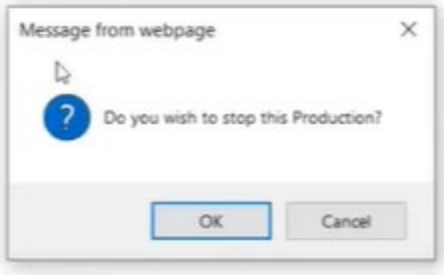

Figure 8-5: Dialog box - stop production

3. The **Stop Production** window opens. Click **OK** (Figure 8-6).

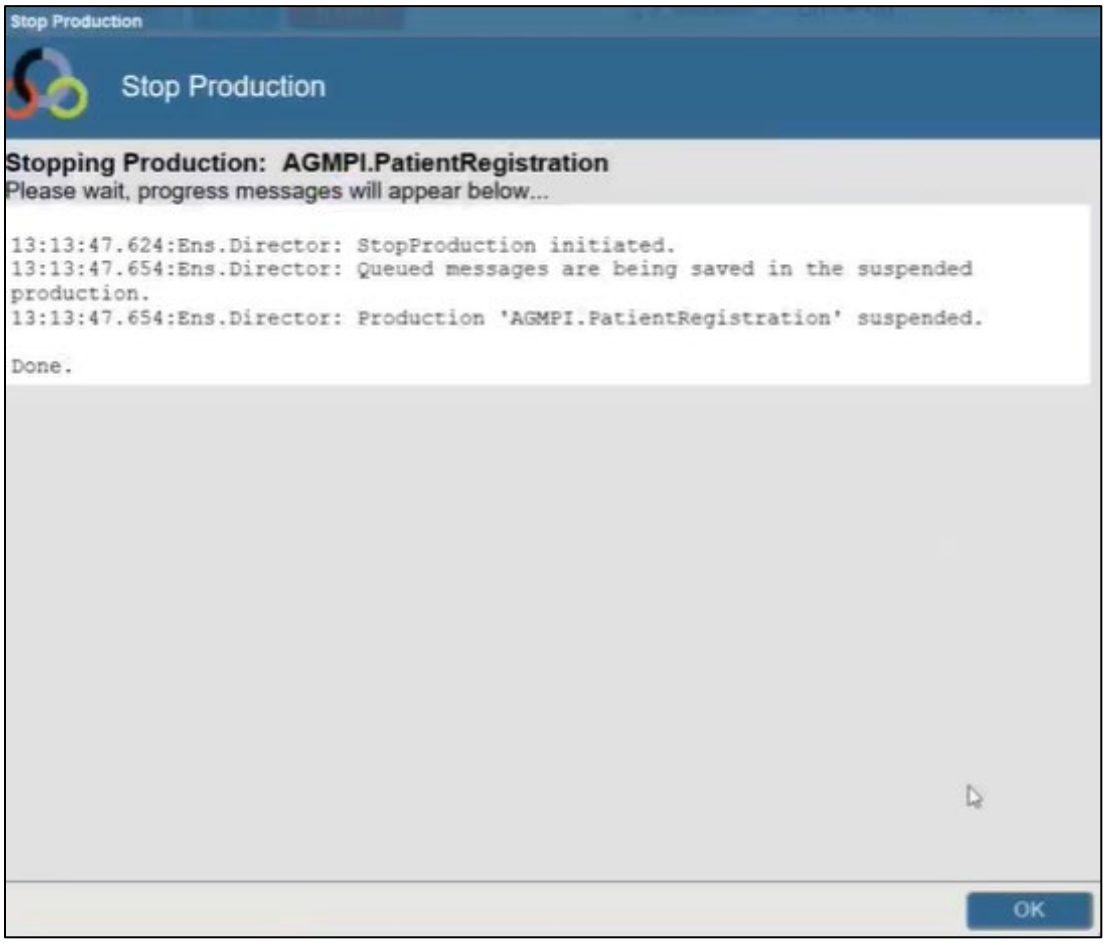

Figure 8-6: Stop Production window

8.3 Auto-Start Production

Production starts may be scheduled.

1. From the **Management Portal**, click on **Ensemble** and **Manage**, then **Auto-Start Production** (Figure 8-7).

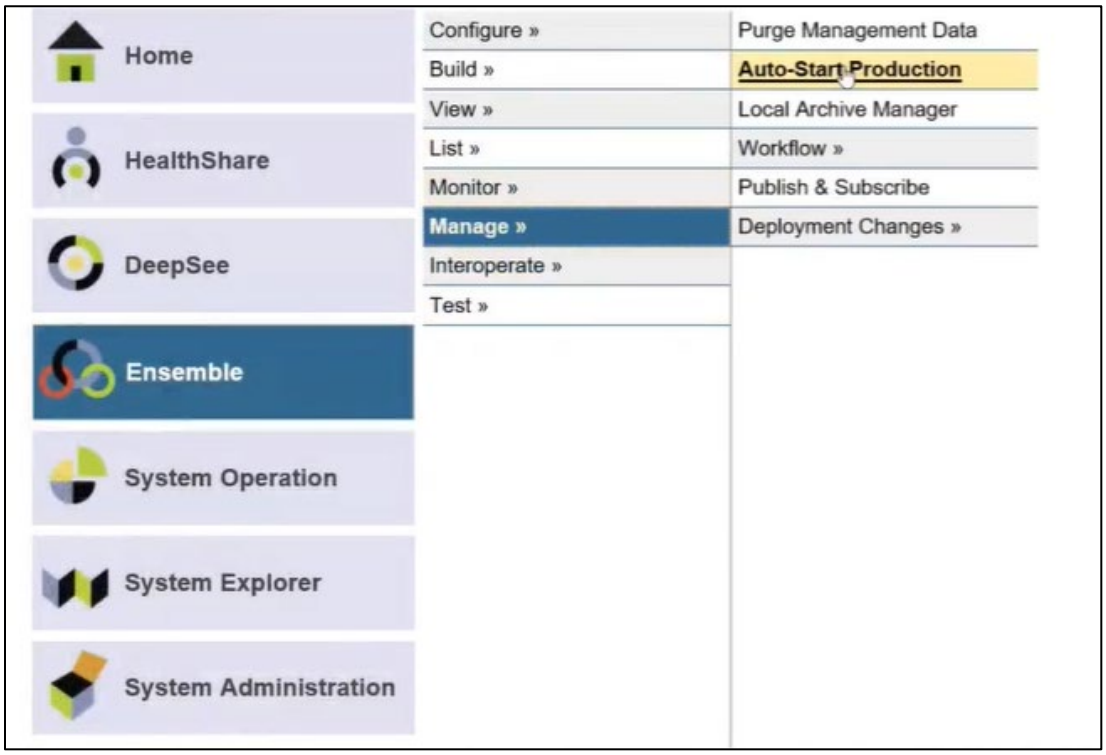

Figure 8-7: Management Portal

2. On the **Auto-Start Production** page, click the drop-down menu and select **AGMPI.PatientRegistration**.

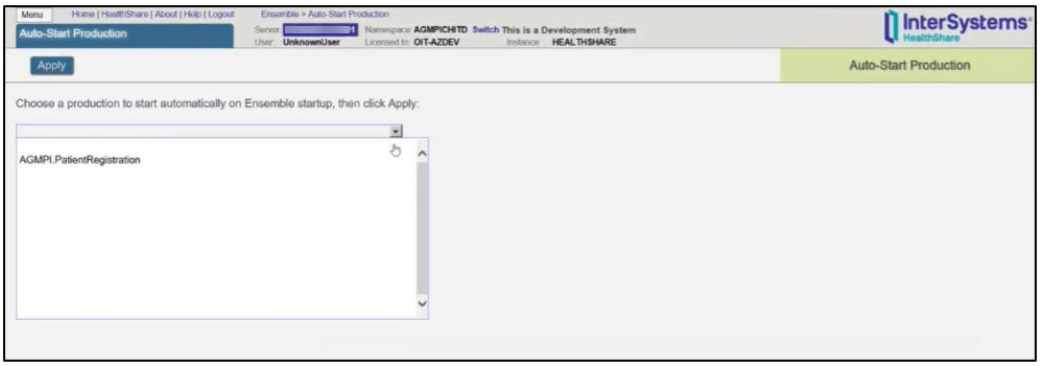

Figure 8-8: Auto-Start Production page

3. Click the **Apply** button.

Figure 8-9: Auto-Start Production page - Apply

9.0 Purge Management

Follow the procedure for purging in the *Patient Registration MPI Interface/Ensemble (AG) Installation Guide and Release Notes* (ag__0720.01o_ens2012.pdf).

10.0 System Monitor

The **System Monitor** page displays real-time status information about the currently running production in a condensed, one-page format.

1. On the **Management Portal** page, click **Ensemble** and **Monitor**, then **System Monitor** (Figure 10-1).

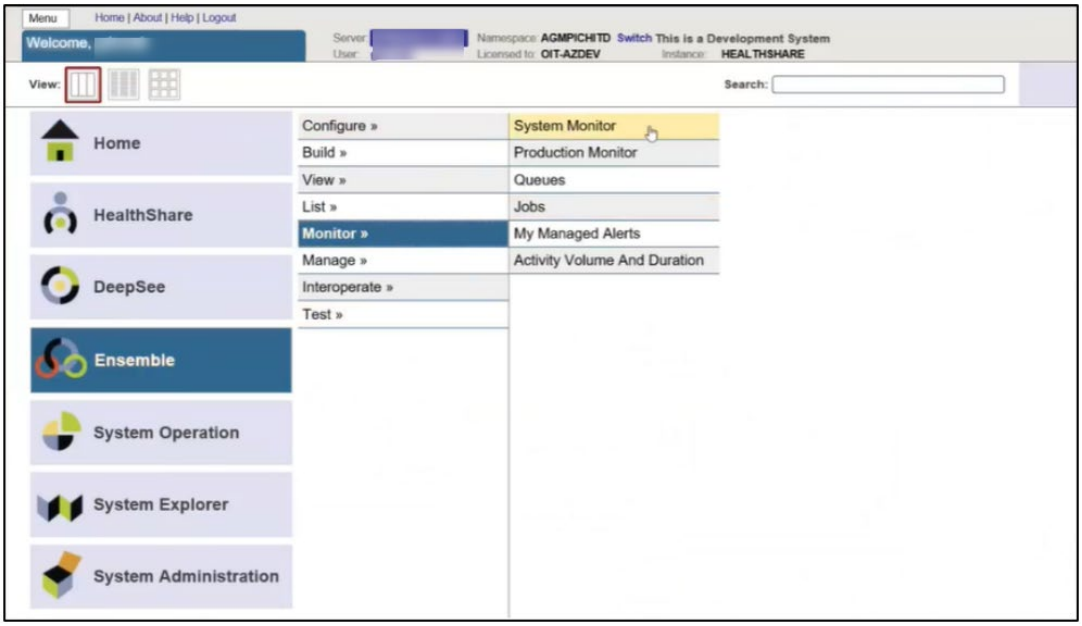

Figure 10-1: System Monitor

2. The **System Monitor** page opens. It is a real-time monitor only. Configurations cannot be changed from this page (Figure 10-2).

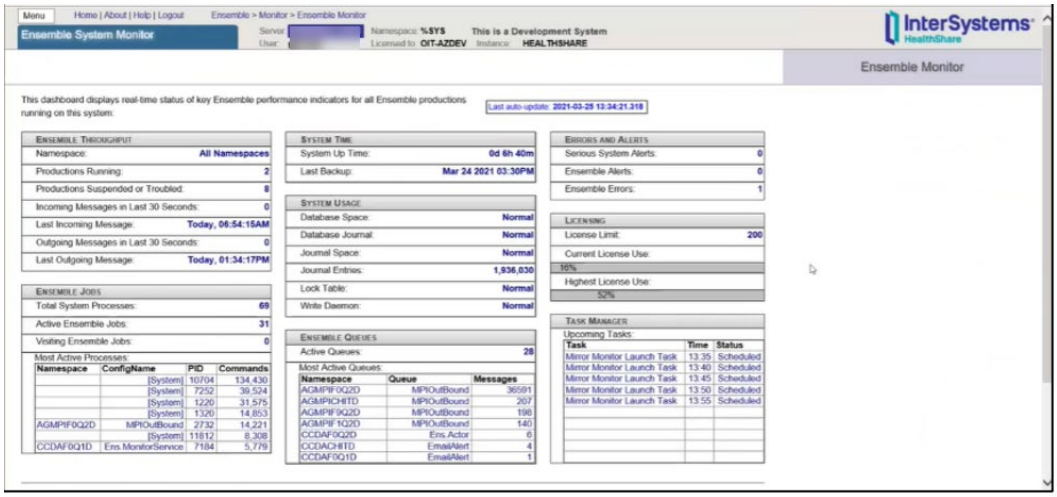

Figure 10-2: Systems Monitor page

11.0 Ensemble E-Mail Alerts

If there is an error within the Ensemble production, e-mail alerts are sent to individuals listed in the Ensemble e-mail alert configuration.

The messages in this section will come to the user's email account and may have a different format, however the content of the messages will be the same across applications.

> **Note:** Detailed instructions for configuring e-mail alerts and recipients in Ensemble are found in Section 4.12 of the *Patient Registration MPI Interface/Ensemble (AG) Installation Guide and Release Notes* (ag__0720.01o_ens2012.pdf).

11.1 Erroneous messages

Erroneous alerts from **MPIInbound** can be ignored (Figure 11-1). The MPIInbound alert indicates that the listener is not receiving messages within 5 seconds from initially receiving a message.

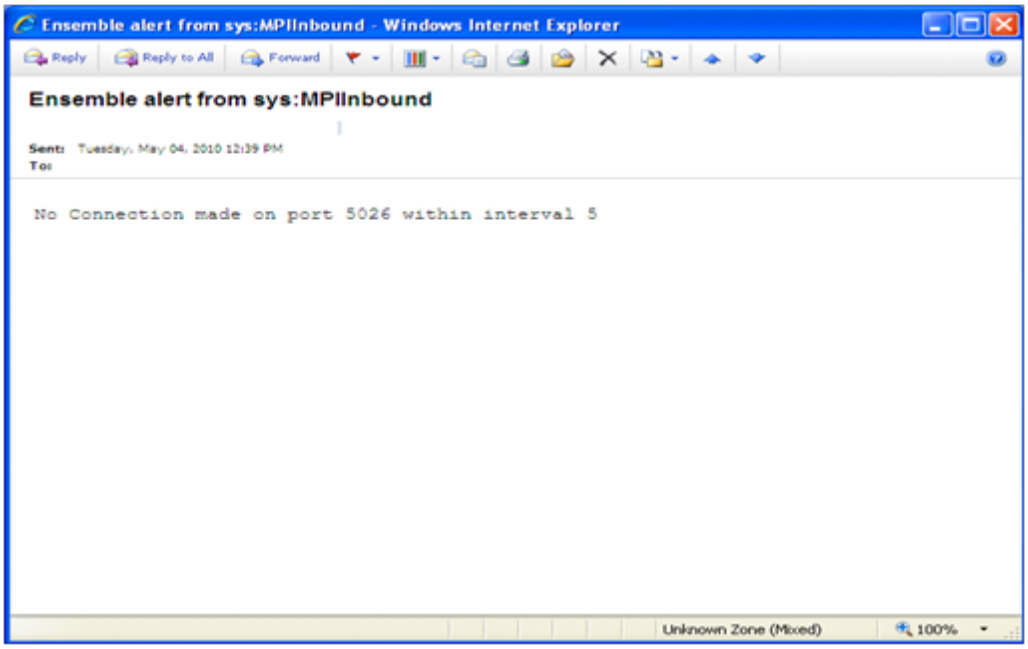

Figure 11-1: Ensemble e-mail alert for MPIInbound

11.2 Segment undefined or unknown

Contact IT support for assistance with this alert (Figure 11-2).

Phone: (888) 830-7280 (toll free)

Web: https://www.ihs.gov/itsupport/

Email: itsupport@ihs.gov

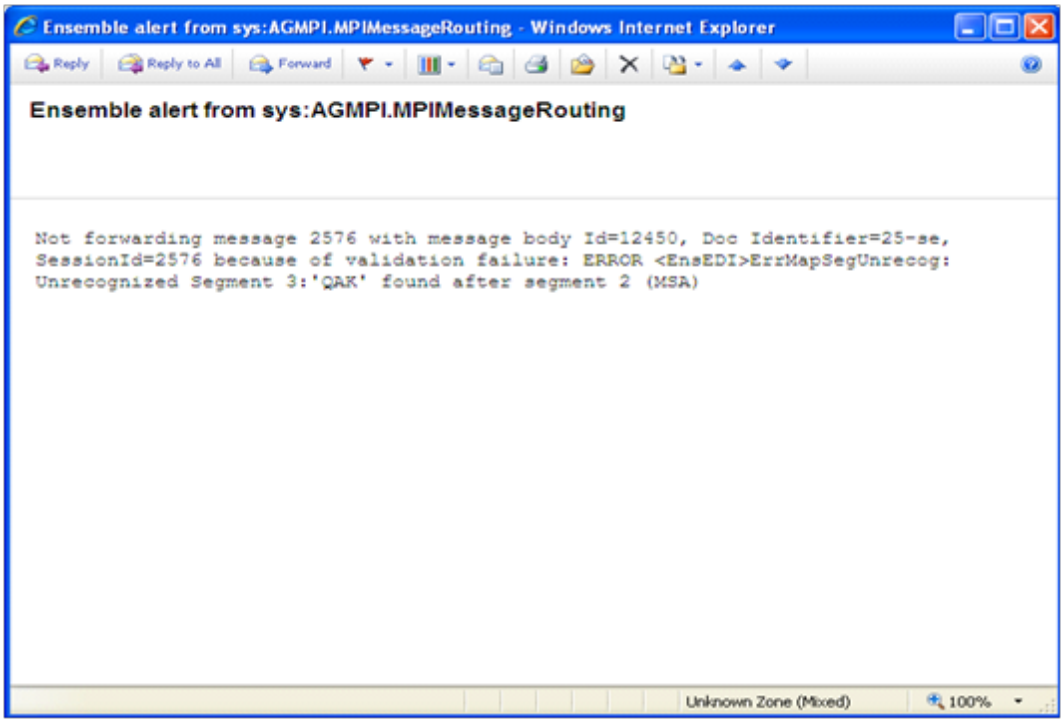

Figure 11-2: Ensemble e-mail alert for AGMPI.MPIMessageRouting

11.3 Other Message Types

RPMS AGMP routine had an error (Figure 11-3).

```
From: Ensemble_AGMPI@HLOMPI_rpms [Ensemble_AGMPI@HLOMPI_rpms]
Sent: Friday, May 07, 2010 9:20 AM
To:
Subject: Ensemble alert from sys:RPMSInBound

There is an issue obtaining a lock on the HLB global in the
HLOGlobalInbound Adapter:
```

Figure 11-3: Ensemble e-mail error alert

Figure 11-4 through Figure 11-23 show e-mail alerts that may be sent from Ensemble.

> **Note**: If any of the following e-mail alerts are received, notify IT Support:

Phone: (888) 830-7280 (toll free)

Web: https://www.ihs.gov/itsupport/

Email: itsupport@ihs.gov

```
"ERROR in Configuration"
```

Figure 11-4: Configuration Error Message

```
"There is an issue obtaining a lock on the HLB global in the
HLOGlobalInbound Adapter:"
```

Figure 11-5: HLB global Error Message

```
"There is an issue obtaining a lock on the HLA global in the
HLOGlobalInbound Adapter:"
```

Figure 11-6: HLA global Error Message

```
"There was an issue creating a valid HL7 message in the HLOGlobalInbound
Adapter: "
```

Figure 11-7: HL7 Error Message

```
"There was an error in the HLOGlobalInbound Adapter:"
```

Figure 11-8: HLOGlobalInbound Adapter Error Message

```
"There is an issue obtaining a lock on the HLB global in the
HLOGlobalOutbound Adapter:"
```

Figure 11-9: HLB global in the HLOGlobalOutbound Error Message

```
"There is an issue obtaining a lock on the HLA global in the
HLOGlobalOutbound Adapter:"
```

Figure 11-10: HLA global in the HLOGlobalOutbound Error Message

```
"Failure: The HLOGlobalOutbound adapter failed to Process Message (an ACK)
because it did not contain a Message Control ID:"
```

Figure 11-11: ACK without a Message Control ID Error Message

```
"Failure: The HLOGlobalOutbound adapter failed to Process Message (an ACK)
because the 'B' reference node did not exist for Message Control ID"
```

Figure 11-12: L ACK without a B reference node Error Message

```
"Alert: The HLOGlobalOutbound adapter received message (an ACK message)
that did not contain an 'AA' or 'CA' Acknowledgment Code: The
MessageControl ID is”
```

Figure 11-13: Missing AA or CA ACK Code Error Message

```
"Failure: The HLOGlobalOutbound adapter failed to find an open IEN after
100 tries"
```

Figure 11-14: Failure to find an open IEN Error Message

```
"Failure: The HLOGlobalOutbound adapter failed while looping though an HL7
message segments: MessageID="
```

Figure 11-15: Failure with MessageID in HL7 Error Message

```
"Failure: The HLOGlobalOutbound adapter failed: Error="
```

Figure 11-16: HLOGlobalOutbound adapter Error Message

```
"Failure: The HLOGlobalOutbound adapter failed: Error="
```

Figure 11-17: HLOGlobal Patient Record Number Error Message

```
"MPI DFN="_DFN_" :: "_"ERROR WHEN CREATING A01"
```

Figure 11-18: Patient Record Number Error Message for A01

```
"MPI DFN="_DFN_" :: "_"ERROR WHEN CREATING A03"
```

Figure 11-19: Patient Record Number Error Message for A03

Warning: An e-mail alert containing the message “The HLOGlobalOutbound adapter failed” indicates that a programming error occurred within the adapter. This error must be reported to OIT. The Ensemble production should be shut down until the error is investigated.

```
Failure: The HLOGlobalOutbound adapter failed: Error= 0
```

Figure 11-20: HLOGlobalOutbound adapter error

This error occurs when the MPI sends an unusually large ERR segment back to the client.

```
TCP Read timeout (5) expired waiting for terminator SegTerminatorAscii=13,
on |TCP|8899|2984, data received =''
```

Figure 11-21: TCP Read timeout error

Warning: If a TCP Connect timeout error is occurring repeatedly, the MPI is down, and IT Support must be notified immediately.

Phone: (888) 830-7280 (toll free)

Web: https://www.ihs.gov/itsupport/

Email: itsupport@ihs.gov

```
TCP Connect timeout period (5) expired for 161.223.90.106:8899
```

Figure 11-22: TCP Connect timeout error

This Ensemble email alert message indicates that the site might not be receiving AA messages from the MPI. If a site receives several of these messages, check Ensemble settings or contact OIT. This could be an indication that there is a problem with the station number, or it could mean that the network or MPI server is not responding quickly.

```
No Connection made on port 5026 within interval 5
```

Figure 11-23: No connection error

The IP address set in the HLO SYSTEMS PARAMETER file is incorrectly setup for another system.

```
Failure: The HLOGlobalOutbound adapter failed to Process Message 308834 (an
ACK) because the 'B' reference node did not exist for Message Control ID
14752 345:::
```

Figure 11-24: Failure to process message error

Appendix A RPMS Rules of Behavior

The Resource and Patient Management (RPMS) system is a United States Department of Health and Human Services (HHS), Indian Health Service (IHS) information system that is ***FOR OFFICIAL USE ONLY***. The RPMS system is subject to monitoring; therefore, no expectation of privacy shall be assumed. Individuals found performing unauthorized activities are subject to disciplinary action including criminal prosecution.

All users (Contractors and IHS Employees) of RPMS will be provided a copy of the Rules of Behavior (ROB) and must acknowledge that they have received and read them prior to being granted access to a RPMS system, in accordance IHS policy.

- For a listing of general ROB for all users, see the most recent edition of *IHS General User Security Handbook* (SOP 06-11a).
- For a listing of system administrators/managers rules, see the most recent edition of the *IHS Technical and Managerial Handbook* (SOP 06-11b).

Both documents are available at this IHS website:
https://home.ihs.gov/security/index.cfm.

> **Note**: Users must be logged on to the IHS D1 Intranet to access these documents.

The ROB listed in the following sections are specific to RPMS.

A.1 All RPMS Users

In addition to these rules, each application may include additional RoBs that may be defined within the documentation of that application (e.g., PCC, Dental, Pharmacy).

A.1.1 Access

RPMS users shall

- Only use data for which you have been granted authorization.
- Only give information to personnel who have access authority and have a need to know.
- Always verify a caller's identification and job purpose with your supervisor or the entity provided as employer before providing any type of information system access, sensitive information, or non-public agency information.
- Be aware that personal use of information resources is authorized on a limited basis within the provisions *Indian Health Manual* Part 8, "Information Resources Management," Chapter 6, "Limited Personal Use of Information Technology Resources."

RPMS users shall not

- Retrieve information for someone who does not have authority to access the information.
- Access, research, or change any user account, file, directory, table, or record not required to perform your OFFICIAL duties.
- Store sensitive files on a PC hard drive, or portable devices or media, if access to the PC or files cannot be physically or technically limited.
- Exceed their authorized access limits in RPMS by changing information or searching databases beyond the responsibilities of their job or by divulging information to anyone not authorized to know that information.

A.1.2 Information Accessibility

RPMS shall restrict access to information based on the type and identity of the user. However, regardless of the type of user, access shall be restricted to the minimum level necessary to perform the job.

RPMS users shall

- Access only those documents they created and those other documents to which they have a valid need-to-know and to which they have specifically granted access through an RPMS application based on their menus (job roles), keys, and FileMan access codes. Some users may be afforded additional privileges based on the function they perform such as system administrator or application administrator.
- Acquire a written preauthorization in accordance with IHS policies and procedures prior to interconnection to or transferring data from RPMS.

A.1.3 Accountability

RPMS users shall

- Behave in an ethical, technically proficient, informed, and trustworthy manner.
- Logout of the system whenever they leave the vicinity of their PC.
- Be alert to threats and vulnerabilities in the security of the system.
- Report all security incidents to their local Information System Security Officer (ISSO).
- Differentiate tasks and functions to ensure that no one person has sole access to or control over important resources.
- Protect all sensitive data entrusted to them as part of their government employment.
- Shall abide by all Department and Agency policies and procedures and guidelines related to ethics, conduct, behavior, and IT information processes.

A.1.4 Confidentiality

RPMS users shall

- Be aware of the sensitivity of electronic and hardcopy information and protect it accordingly.
- Store hardcopy reports/storage media containing confidential information in a locked room or cabinet.
- Erase sensitive data on storage media, prior to reusing or disposing of the media.
- Protect all RPMS terminals from public viewing at all times.
- Abide by all HIPAA regulations to ensure patient confidentiality.

RPMS users shall not

- Allow confidential information to remain on the PC screen when someone who is not authorized to that data is in the vicinity.
- Store sensitive files on a portable device or media without encrypting.

A.1.5 Integrity

RPMS users shall

- Protect your system against viruses and similar malicious programs.
- Observe all software license agreements.

- Follow industry standard procedures for maintaining and managing RPMS hardware, operating system software, application software, and/or database software and database tables.
- Comply with all copyright regulations and license agreements associated with RPMS software.

RPMS users shall not

- Violate Federal copyright laws.
- Install or use unauthorized software within the system libraries or folders
- Use freeware, shareware, or public domain software on/with the system without your manager's written permission and without scanning it for viruses first.

A.1.6 System Logon

RPMS users shall

- Have a unique User Identification/Account name and password.
- Be granted access based on authenticating the account name and password entered.
- Be locked out of an account after 5 successive failed login attempts within a specified time period (e.g., one hour).

A.1.7 Passwords

RPMS users shall

- Change passwords a minimum of every 90 days.
- Create passwords with a minimum of eight characters.
- If the system allows, use a combination of alpha, numeric characters for passwords, with at least one uppercase letter, one lower case letter, and one number. It is recommended, if possible, that a special character also be used in the password.
- Change vendor-supplied passwords immediately.
- Protect passwords by committing them to memory or store them in a safe place (do not store passwords in login scripts, or batch files.
- Change password immediately if password has been seen, guessed, or otherwise compromised; and report the compromise or suspected compromise to your ISSO.
- Keep user identifications (ID) and passwords confidential.

RPMS users shall not

- Use common words found in any dictionary as a password.

- Use obvious readable passwords or passwords that incorporate personal data elements (e.g., user's name, date of birth, address, telephone number, or social security number; names of children or spouses; favorite band, sports team, or automobile; or other personal attributes).
- Share passwords/IDs with anyone or accept the use of another's password/ID, even if offered.
- Reuse passwords. A new password must contain no more than five characters per 8 characters from the previous password.
- Post passwords.
- Keep a password list in an obvious place, such as under keyboards, in desk drawers, or in any other location where it might be disclosed.
- Give a password out over the phone.

A.1.8 Backups

RPMS users shall

- Plan for contingencies such as physical disasters, loss of processing, and disclosure of information by preparing alternate work strategies and system recovery mechanisms.
- Make backups of systems and files on a regular, defined basis.
- If possible, store backups away from the system in a secure environment.

A.1.9 Reporting

RPMS users shall

- Contact and inform your ISSO that you have identified an IT security incident and you will begin the reporting process by providing an IT Incident Reporting Form regarding this incident.
- Report security incidents as detailed in the *IHS Incident Handling Guide* (SOP 05-03).

RPMS users shall not

- Assume that someone else has already reported an incident. The risk of an incident going unreported far outweighs the possibility that an incident gets reported more than once

A.1.10 Session Timeouts

RPMS system implements system-based timeouts that back users out of a prompt after no more than 5 minutes of inactivity.

RPMS users shall

- Utilize a screen saver with password protection set to suspend operations at no greater than 10-minutes of inactivity. This will prevent inappropriate access and viewing of any material displayed on your screen after some period of inactivity.

A.1.11 Hardware

RPMS users shall

- Avoid placing system equipment near obvious environmental hazards (e.g., water pipes).
- Keep an inventory of all system equipment.
- Keep records of maintenance/repairs performed on system equipment.

RPMS users shall not

- Eat or drink near system equipment

A.1.12 Awareness

RPMS users shall

- Participate in organization-wide security training as required.
- Read and adhere to security information pertaining to system hardware and software.
- Take the annual information security awareness.
- Read all applicable RPMS Manuals for the applications used in their jobs.

A.1.13 Remote Access

Each subscriber organization establishes its own policies for determining which employees may work at home or in other remote workplace locations. Any remote work arrangement should include policies that

- Are in writing.
- Provide authentication of the remote user through the use of ID and password or other acceptable technical means.
- Outline the work requirements and the security safeguards and procedures the employee is expected to follow.
- Ensure adequate storage of files, removal, and non-recovery of temporary files created in processing sensitive data, virus protection, intrusion detection, and provides physical security for government equipment and sensitive data.

- Establish mechanisms to back up data created and/or stored at alternate work locations.

Remote RPMS users shall

- Remotely access RPMS through a virtual private network (VPN) whenever possible. Use of direct dial in access must be justified and approved in writing and its use secured in accordance with industry best practices or government procedures.

Remote RPMS users shall not

- Disable any encryption established for network, internet, and web browser communications.

A.2 RPMS Developers

RPMS developers shall

- Always be mindful of protecting the confidentiality, availability, and integrity of RPMS when writing or revising code.
- Always follow the IHS RPMS Programming Standards and Conventions (SAC) when developing for RPMS.
- Only access information or code within the namespaces for which they have been assigned as part of their duties.
- Remember that all RPMS code is the property of the U.S. Government, not the developer.
- Shall not access live production systems without obtaining appropriate written access, shall only retain that access for the shortest period possible to accomplish the task that requires the access.
- Shall observe separation of duties policies and procedures to the fullest extent possible.
- Shall document or comment all changes to any RPMS software at the time the change or update is made. Documentation shall include the programmer's initials, date of change and reason for the change.
- Shall use checksums or other integrity mechanism when releasing their certified applications to assure the integrity of the routines within their RPMS applications.
- Shall follow industry best standards for systems they are assigned to develop or maintain; abide by all Department and Agency policies and procedures.
- Shall document and implement security processes whenever available.

RPMS developers shall not

- Write any code that adversely impacts RPMS, such as backdoor access, "Easter eggs," time bombs, or any other malicious code or make inappropriate comments within the code, manuals, or help frames.
- Grant any user or system administrator access to RPMS unless proper documentation is provided.
- Release any sensitive agency or patient information.

A.3 Privileged Users

Personnel who have significant access to processes and data in RPMS, such as, system security administrators, systems administrators, and database administrators have added responsibilities to ensure the secure operation of RPMS.

Privileged RPMS users shall

- Verify that any user requesting access to any RPMS system has completed the appropriate access request forms.
- Ensure that government personnel and contractor personnel understand and comply with license requirements. End users, supervisors, and functional managers are ultimately responsible for this compliance.
- Advise the system owner on matters concerning information technology security.
- Assist the system owner in developing security plans, risk assessments, and supporting documentation for the certification and accreditation process.
- Ensure that any changes to RPMS that affect contingency and disaster recovery plans are conveyed to the person responsible for maintaining continuity of operations plans.
- Ensure that adequate physical and administrative safeguards are operational within their areas of responsibility and that access to information and data is restricted to authorized personnel on a need to know basis.
- Verify that users have received appropriate security training before allowing access to RPMS.
- Implement applicable security access procedures and mechanisms, incorporate appropriate levels of system auditing, and review audit logs.
- Document and investigate known or suspected security incidents or violations and report them to the ISSO, CISO, and systems owner.
- Protect the supervisor, super user, or system administrator passwords.
- Avoid instances where the same individual has responsibility for several functions (i.e., transaction entry and transaction approval).

- Watch for unscheduled, unusual, and unauthorized programs.
- Help train system users on the appropriate use and security of the system.
- Establish protective controls to ensure the accountability, integrity, confidentiality, and availability of the system.
- Replace passwords when a compromise is suspected. Delete user accounts as quickly as possible from the time that the user is no longer authorized system. Passwords forgotten by their owner should be replaced, not reissued.
- Terminate user accounts when a user transfers or has been terminated. If the user has authority to grant authorizations to others, review these other authorizations. Retrieve any devices used to gain access to the system or equipment. Cancel logon IDs and passwords and delete or reassign related active and back up files.
- Use a suspend program to prevent an unauthorized user from logging on with the current user's ID if the system is left on and unattended.
- Verify the identity of the user when resetting passwords. This can be done either in person or having the user answer a question that can be compared to one in the administrator’s database.
- Shall follow industry best standards for systems they are assigned to; abide by all Department and Agency policies and procedures.

Privileged RPMS users shall not

- Access any files, records, systems, etc., that are not explicitly needed to perform their duties
- Grant any user or system administrator access to RPMS unless proper documentation is provided.
- Release any sensitive agency or patient information.

Glossary

Archiving

The storing of historical or little-used data off-line (often on tape).

Configuration Diagram

A graphical representation of the business hosts in a production.

Entry Point

Entry point within a routine that is referenced by a “DO” or “GOTO” command from a routine internal to a package.

File

A set of related records or entries treated as a single unit.

FileMan

The database management system for RPMS.

Flowsheet

A tabular format for organizing and displaying data in a special section of the health summary.

Global

In MUMPS, “global” refers to a variable stored on disk (global variable) or the array to which the global variable may belong (global array).

INDEX (%INDEX)

A Kernel utility used to verify routines and other MUMPS code associated with a package. Checking is done according to current ANSI MUMPS standards and RPMS programming standards.

This tool can be invoked through an option or from direct mode (>D ^%INDEX).

Kernel

The set of MUMPS software utilities that function as an intermediary between the host operating system and application packages, such as Laboratory and Pharmacy. The Kernel provides a standard and consistent user and programmer interface between application packages and the underlying MUMPS implementation. These utilities provide the foundation for RPMS.

Menu

A list of choices for computing activity. A menu is a type of option designed to identify a series of items (other options) for presentation to the user for selection. When menu-type options are displayed, the prompt includes the name of the menu preceded by the word "Select" and followed by the word "option," as in "Select Menu Management option" (the menu's "Select" prompt).

Namespace

A unique set of two to four alpha characters assigned by the database administrator to a software application.

Option

An entry in the Option file. As an item on a menu, an option provides an opportunity for users to select it, thereby invoking the associated computing activity. Options may also be scheduled to run in the background, non-interactively, by TaskMan.

Production

The unit of delivery for Ensemble-based development projects.

Production Table

Contains information about the currently running production.

Panel

A tabular format for presenting a series of clinical measurements or results in the health summary.

Queuing

Requesting that a job be processed at a later time rather than within the current session.

Routine

A program or sequence of instructions called by a program that may have some general or frequent use. MUMPS routines are groups of program lines that are saved, loaded, and called as a single unit via a specific name.

Utility

A callable routine line tag or function. A universal routine usable by anyone.

Acronym List

Acronym	Term Definition
AG	Namespace for Patient Registration
EIE	Ensemble Integration Engine
ICD	International Classification of Diseases.
IHS	Indian Health Service
IEN	Internal Entry Number. The number used to identify an entry within a file. Every record has a unique internal entry number.
IRM	Information Resource Management. The IHS personnel responsible for information systems management and security.
MPI	Master Patient Index
RPMS	Resource and Patient Management System. A series of integrated software components that includes clinical, administrative, and financial functions.
HLO	HL7-Optimized (interface)
ADT	Admission, Discharge, Transfer
OIT	Office of Information Technology

Contact Information

If you have any questions or comments regarding this distribution, please contact the IHS IT Service Desk.

Phone: (888) 830-7280 (toll free)

Web: https://www.ihs.gov/itsupport/

Email: itsupport@ihs.gov