



RESOURCE AND PATIENT MANAGEMENT SYSTEM

e-Prescribing Productions

(BEPR)

Installation Guide and Release Notes

Version 1.0
March 2012

Office of Information Technology (OIT)
Division of Information Resource Management
Albuquerque, New Mexico

Table of Contents

1.0	Release Notes	1
2.0	Installation Notes	2
2.1	Contents of Distribution	2
2.2	Required Resources	2
2.3	Before You Begin: Installation Issues	2
2.3.1	Disk Space	2
3.0	Installation Instructions	4
3.1	e-Prescribing Namespace	4
3.2	Production Import	7
4.0	Sample Installations	10
4.1	Rx.Prod.Production Settings.....	10
4.2	Directory Download Settings	12
4.2.1	Service – Start DD.....	12
4.2.2	Process – Directory Download	14
4.2.3	Process – Ens.Alert.....	16
4.2.4	Operation – Email Alerts.....	17
4.2.5	Operation – GetFile	20
4.2.6	Operation – PlaceFile	22
4.3	Pass-Through Settings	23
4.3.1	Service – HL7 from RPMS	24
4.3.2	Service – HL7 from Ensemble	26
4.3.3	Process – HL7 Message Router.....	28
4.3.4	Operation – HL7 to RPMS	30
4.3.5	Operation – HL7 to Ensemble	32
4.4	Sample Cache Install.....	34
5.0	Installation Configuration	38
5.1	Map HL* Globals.....	38
5.2	Auto-Start Production Settings	40
5.3	Add Directory Download Task	41
	Glossary	53
	Contact Information	55

Preface

The purpose of this document is to provide IT personnel information about the e-Prescribing Productions for the Local Server. The Local version has a root package name of Rx and several sub-packages including but not limited to: DD (Directory Download), SPI (Surescripts® Provider Identifier), and NewRx (New electronic prescription) which hold code for the various functions of the Local production.

Further definition of these terms is included in the Glossary.

1.0 Release Notes

The Ensemble Interface Engine (EIE) provides a means to download a file containing pharmacies in the network (Directory Download), request and receive a Surescripts Prescriber ID (SPI), and electronically send a prescription (NewRx) to a pharmacy within the network through the Surescripts server.

The purpose of this document is to provide the user information on how to import the services, processes, and operations into Ensemble, the configuration of said imports, and the functions of the local server.

At this time the local server supports Directory Download, SPI requests and NewRx.

2.0 Installation Notes

Prefix: BEPR

Current Version: 1.0

2.1 Contents of Distribution

File	Description
bepr0100.xml	Server XML file
bepr010i.pdf	Installation Guide
bepr010u.pdf	User Guide
bepr010t.pdf	Technical Guide

2.2 Required Resources

- Ensemble 2009.1.3 or later release
- At least 10Mb disk space for the e-Prescribing namespace
- At least 75Mb disk space for Directory Download files
- Electronic Health Record, v1.1, p9
- IHS Pharmacy Modifications, v7.0, p1012
- AVA 9320.21

2.3 Before You Begin: Installation Issues

A directory for the Directory Download should to be created on the server where it is accessible to the Ensemble production and complies with site security restrictions. There is no PHI contained in the downloaded files.

The site will need a decompression tool such as 7zip or gzip installed for Directory Download.

2.3.1 Disk Space

2.3.1.1 e-Prescribing Namespace

The initial size is 10Mb but can be installed as small as a 1Mb size.

2.3.1.2 Directory Download

The site should have enough free disk space in the download directory which will hold the Directory Download. The compressed versions of the Directory Downloads range from are 1Kb to 4.7 Mb and the decompressed versions range from approximately 1Kb to 50Mb in size. The larger of the files is the weekly download with the smaller files being the nightly download. The default setting for archiving of these files is 14. Only the compressed files are archived and only one file remains decompressed at any given time.

3.0 Installation Instructions

3.1 e-Prescribing Namespace

This section describes the process of creating the e-Prescribing namespace that will contain the e-Prescribing Ensemble production.

1. From Ensemble Cube, open the **System Management Portal**.
2. Select **Configure Namespaces** from the **Go to** list shown in Figure 3-1:

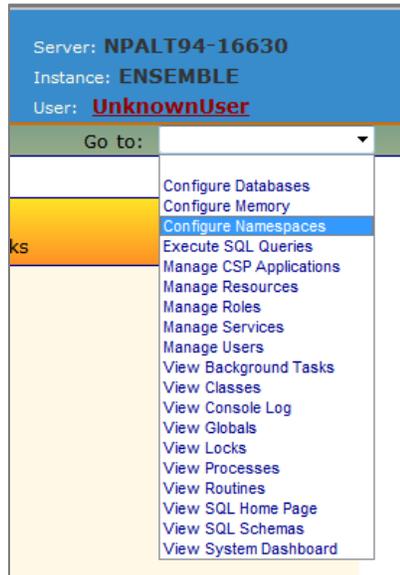


Figure 3-1: Go to list

3. Select **Configure Namespaces** from the **Go to** list displayed in Figure 3-2:

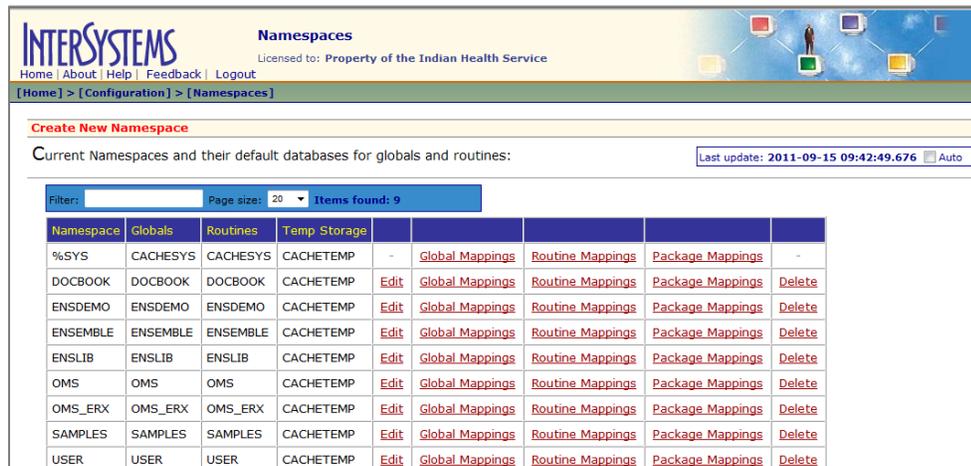


Figure 3-2: Namespaces window

4. Select **Create New Namespace** (Figure 3-3):

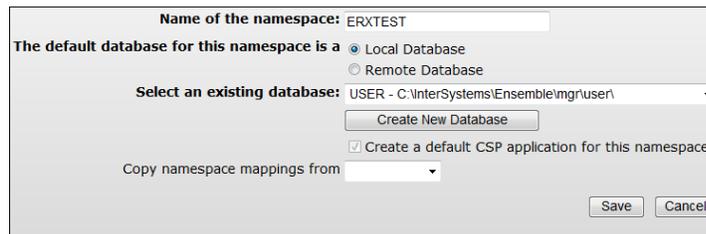


Figure 3-3: **Create New Namespace** dialog

5. Type the name of the e-Prescribing database in the **Name of the namespace** field. The recommended naming convention is “ERX” followed by the site namespace, (for example: ERXTEST).
6. Click **Create New Database**.
7. Type the name of the e-Prescribing database as shown in Figure 3-4:

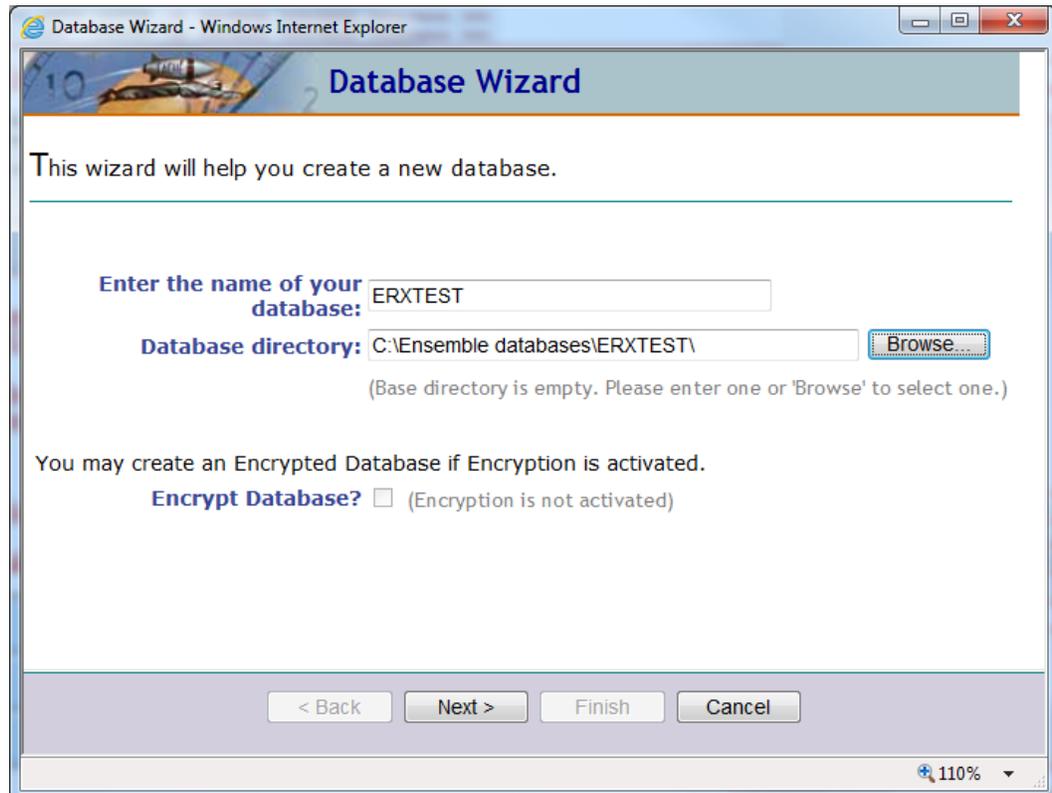


Figure 3-4: **Database Wizard** dialog

8. Click **Browse** and navigate to the location where the site stores its RPMS databases.
9. Type the name of the e-Prescribing database at the end of the directory path.

10. Click **Next**. The **Enter Details about the database** window displays as in Figure 3-5:

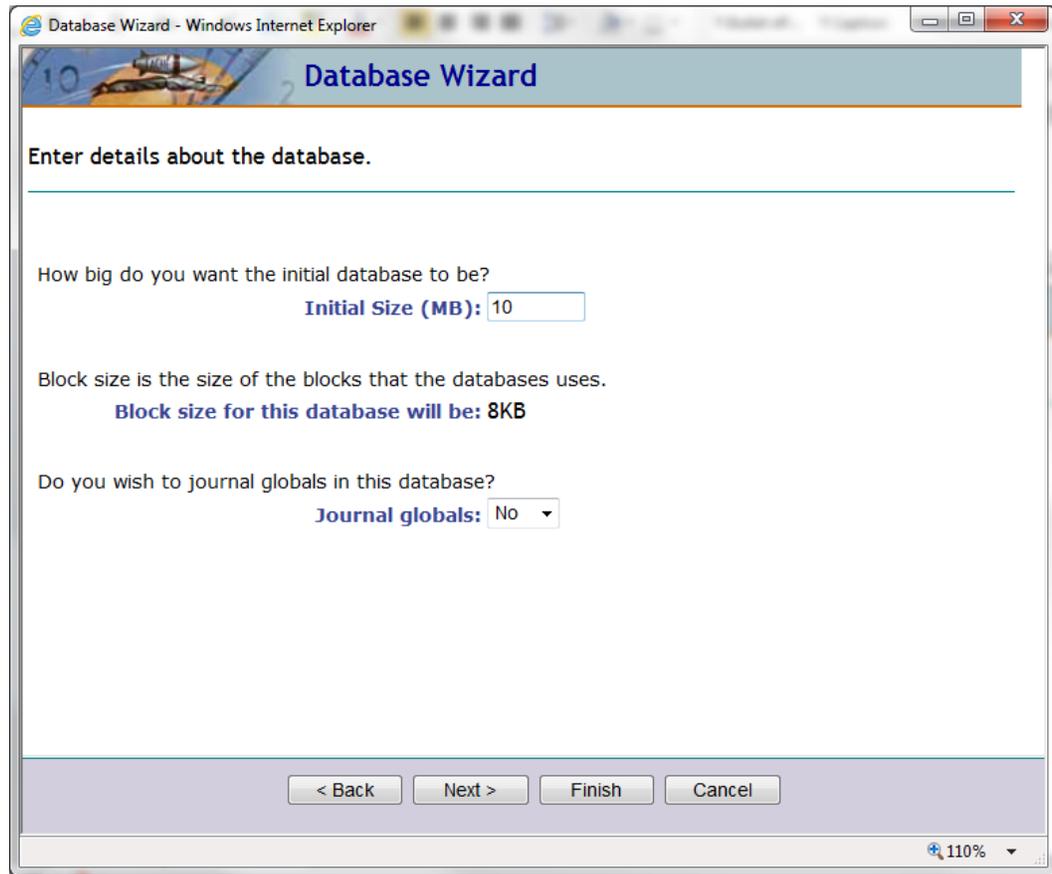


Figure 3-5: **Database Wizard** dialog

11. Type the database settings:
- Initial Size (MB): **10**
 - Journal globals: **No**
12. Click **Next** to display the **Database Wizard** window shown in (Figure 3-6):

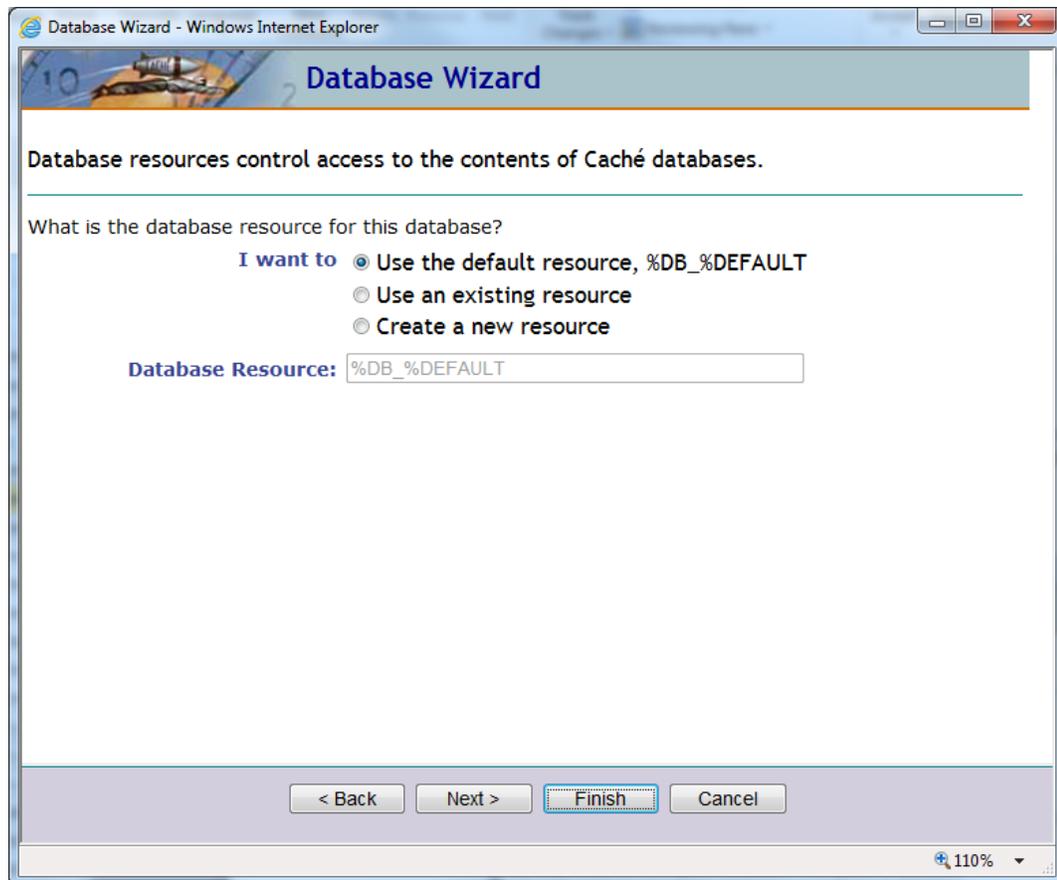


Figure 3-6: Database Wizard dialog

13. Click **Finish**. The **Create New Namespace** dialog displays as shown in (Figure 3-7):

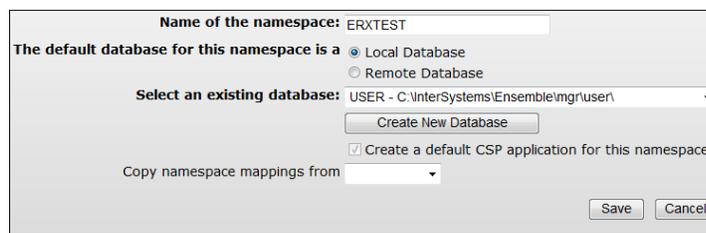


Figure 3-7: Create New Namespace dialog

14. Click **Save**.

3.2 Production Import

This section describes the process of importing the ‘Local’ Server code from the XML document.

1. From Ensemble Cube, open Studio and select **File/Change Namespace**.

2. Select the namespace created from Section 3.1.
3. Select **Import Local** from the **Tools** menu as shown in Figure 3-8.

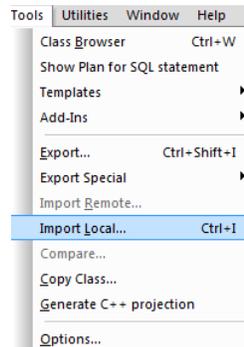


Figure 3-8: **Central Ensemble Production Tools** menu

4. The **Open** dialog displays as shown in Figure 3-9:

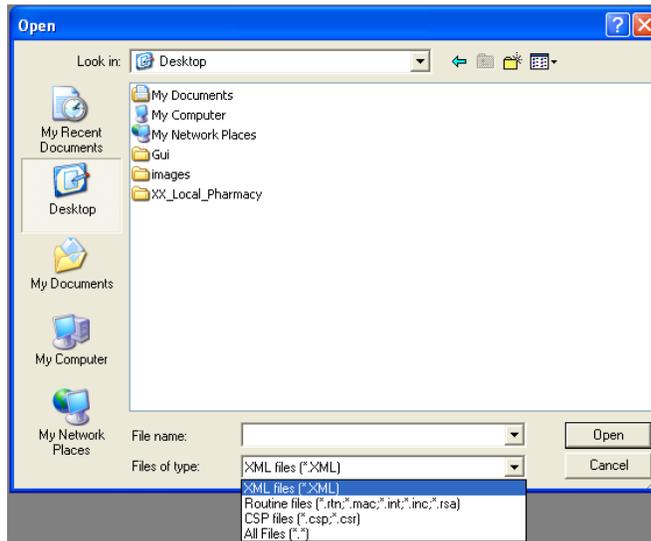


Figure 3-9: **Open** dialog showing navigation to Import file

5. Navigate to the file, bepr0100.xml.
6. Select the file to import and click **Open** to display the **Import** dialog shown in Figure 3-10:

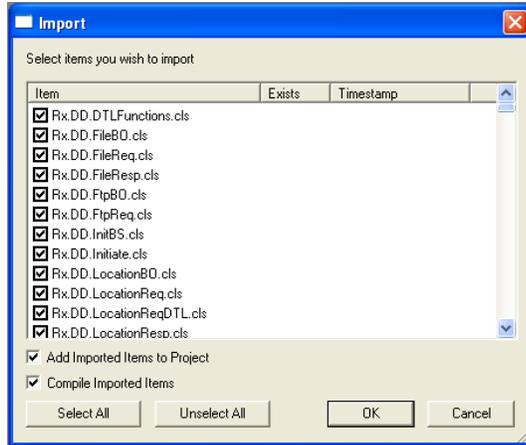


Figure 3-10: **Import** dialog showing chosen items

7. Click **OK** and proceed to Section 4.0.

4.0 Sample Installations

4.1 Rx.Prod.Production Settings

The settings described in this section were configured during implementation to the values specified at that time. Except as otherwise described herein, do not change these settings without conferring with the National e-Prescriptions Deployment Team.

When the production is installed, the settings listed below must be configured before the production can be run.

Note: The settings listed in Table 4-1 are the only settings that should be changed. All other settings are configured correctly and should not be changed.

Table 4-1: Setting to be configured

Business Host	Host Type	Setting
HL7 from Ensemble	Business Service	Allowed IP Addresses
HL7 to Ensemble	Business operation	IPAddress
HL7 to RPMS	Business operation	StationNumber
PlaceFile	Business operation	OS
PlaceFile	Business operation	ZipDirectory
PlaceFile	Business operation	File Path
Email Alerts	Business operation	Recipient
Email Alerts	Business operation	From

1. From Ensemble Cube, open the **System Management Portal**.
 - Click **Ensemble Management Portal**
 - From **Namespace** dropdown select the e-Prescribing namespace
 - Click **Productions**
 - Click **Configure**

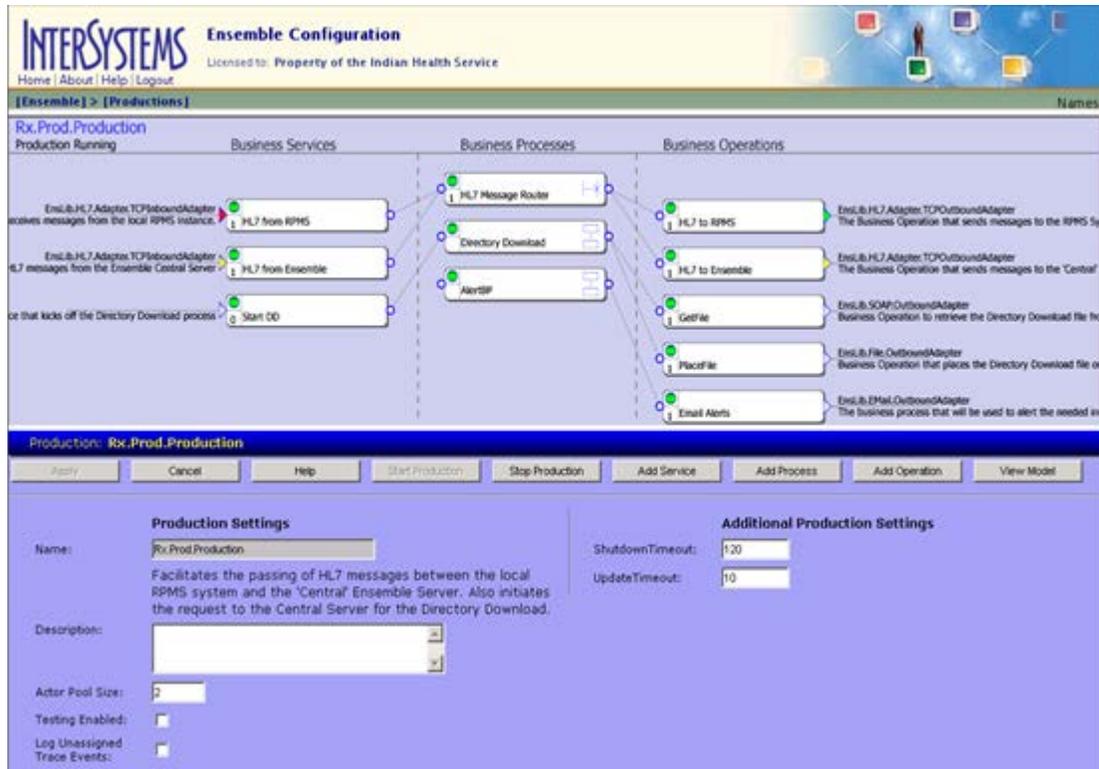


Figure 4-1: Rx.Prod.Production settings

The Production Settings in the lower left of the **Rx.Prod.Production** window are listed in Table 4-2. The Additional Production Settings in the lower right of the window are listed in Table 4-3.

Table 4-2: Rx.Prod.Production Production Settings

Setting	Value	Description
Name	Rx.Prod.Production	Rx package name, Prod sub-folder and Production name
Description	(blank)	The description of the production is given in the class definition and is displayed on the production screen.
Actor Pool Size	2	The number of Actor jobs available to execute Business Process instances.
Testing Enabled	Unchecked	When checked it enables the use of the Testing Service for this Production, for a production environment this is normally not checked.
Log Unassigned Trace Events	Unchecked	When checked trace events that do not belong to any Configuration Item will be logged.

Table 4-3: Rx.Prod.Production Additional Production Settings

Setting	Value	Description
Shutdown Timeout	Set to the default value of 120	The amount of time to wait for a click on Stop Production to succeed.
Update Timeout	Set to the default value of 10	The amount of time to wait for Production updates to succeed.

4.2 Directory Download Settings

The Directory Download process of the Ensemble Production is used to download a daily list of participating Surescripts Pharmacies. The list of pharmacies becomes available from EHR as the provider completes the medication ordering process. The following sections review the settings for Directory Download on the production side.

The settings described in this section were configured during implementation to the values specified at that time. Except as otherwise described herein, do not change these settings without conferring with the National e-Prescriptions Deployment Team.

4.2.1 Service – Start DD

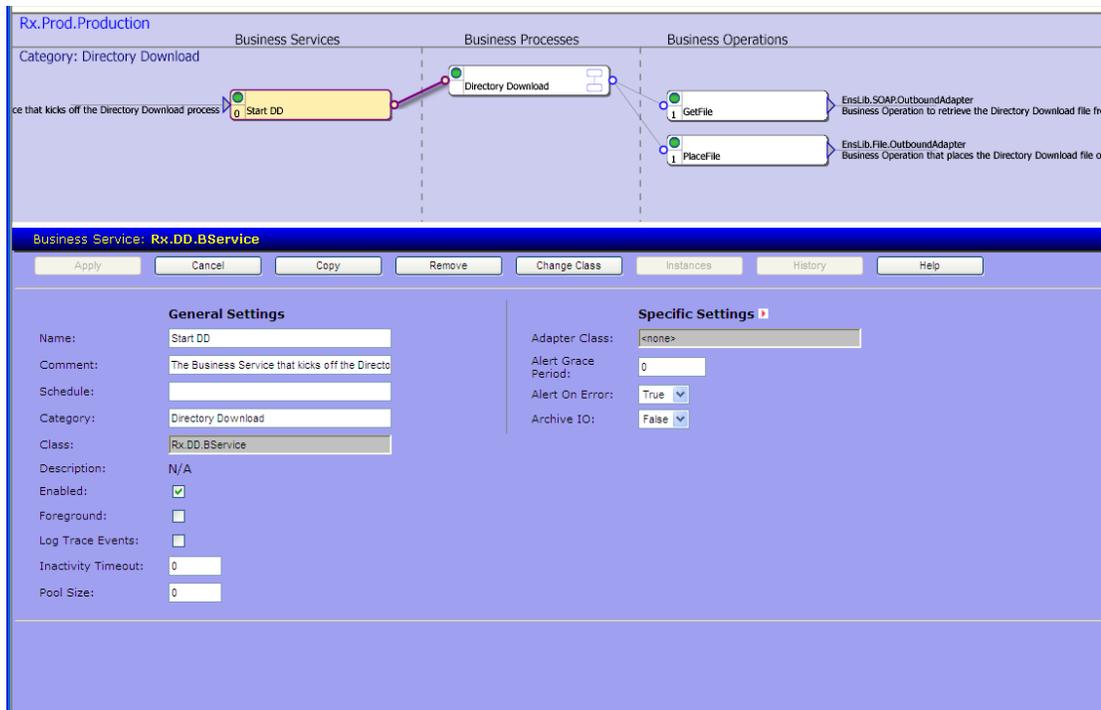


Figure 4-2: Service – Start DD settings

The Production Settings in the lower left of the **Start DD** window are listed in Table 4-4. The Additional Production Settings in the lower right of the window are listed in Table 4-5.

Table 4-4: Start DD general settings

Setting	Value	Description
Name	Start DD	
Comment	The Business Service that kicks off the Directory Download process	
Schedule	(blank)	This is the Start/Stop schedule for the business service
Category	Directory Download	
Class	Rx.DD.BService (Rx Package, DD Sub-Directory, BService Name)	
Description	N/A	
Enabled	Checked	Item is enabled at production start up
Foreground	Not checked	This item is not run in the foreground
Log Trace Events	Not checked	Do not Log trace events for this item
Inactivity Timeout	0	Time (in seconds) that can elapse without an activity before this item is marked as being inactive. Setting this to 0 disables the inactivity timeout
Pool Size	0	The default for this type of Business Service. The Number of jobs created to host this item.

Table 4-5: Start DD Specific Settings

Setting	Value	Description
Adapter Class	<None>	This is an adapter less Business Service.
Alert Grace Period	0	Always send an alert if there's an error
Alert On Error	True	Always send an alert if there's an error
Archive IO	False	Do not log each input and output communication with the external system

4.2.2 Process – Directory Download

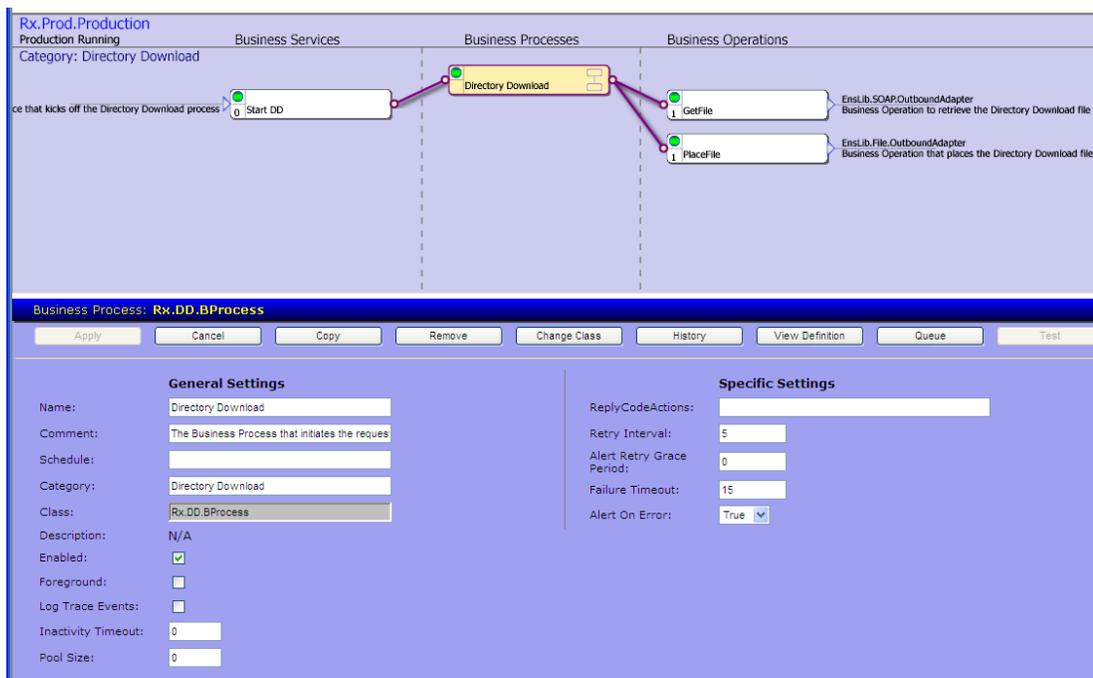


Figure 4-3: Process – Directory Download settings

The Production Settings in the lower left of the **Directory Download** window are listed in Table 4-6. The Additional Production Settings in the lower right of the window are listed in Table 4-7.

Table 4-6: Directory Download General Settings

Setting	Value	Description
Name	Directory Download	
Comment	The Business Process that initiates the request for the Directory Download file and sends the file to be saved locally.	
Schedule	(blank)	This is the Start/Stop schedule for the business process.
Category	Directory Download	
Class	Rx.DD.BProcess	(Rx Package, DD Sub-Directory, BProcess Name)
Description	N/A	
Enabled	Checked	Item is enabled at production start up
Foreground	Not checked	This item is not run in the foreground
Log Trace Events	Not checked	Do not Log trace events for this item

Setting	Value	Description
Inactivity Timeout	0	Time (in seconds) that can elapse without an activity before this item is marked as being inactive. Setting this to 0 disables the inactivity timeout
Pool Size	0	The default for this type of Business Service. The Number of jobs created to host this item.

Table 4-7: Directory Download Specific Settings

Setting	Value	Description
ReplyCodeActions	(blank)	A comma-separated list of codes specifying what action this Process will take on various reply status conditions.
Retry Interval	5 (the default value)	How frequently to retry access to the output system.
Alert Grace Period	0	Always send an alert if there's an error
FailureTimeout	15 (the default value)	How long to keep retrying before giving up and returning an error code.
Alert On Error	True	Send an alert if there's an error with this Business Process.

4.2.3 Process – Ens.Alert

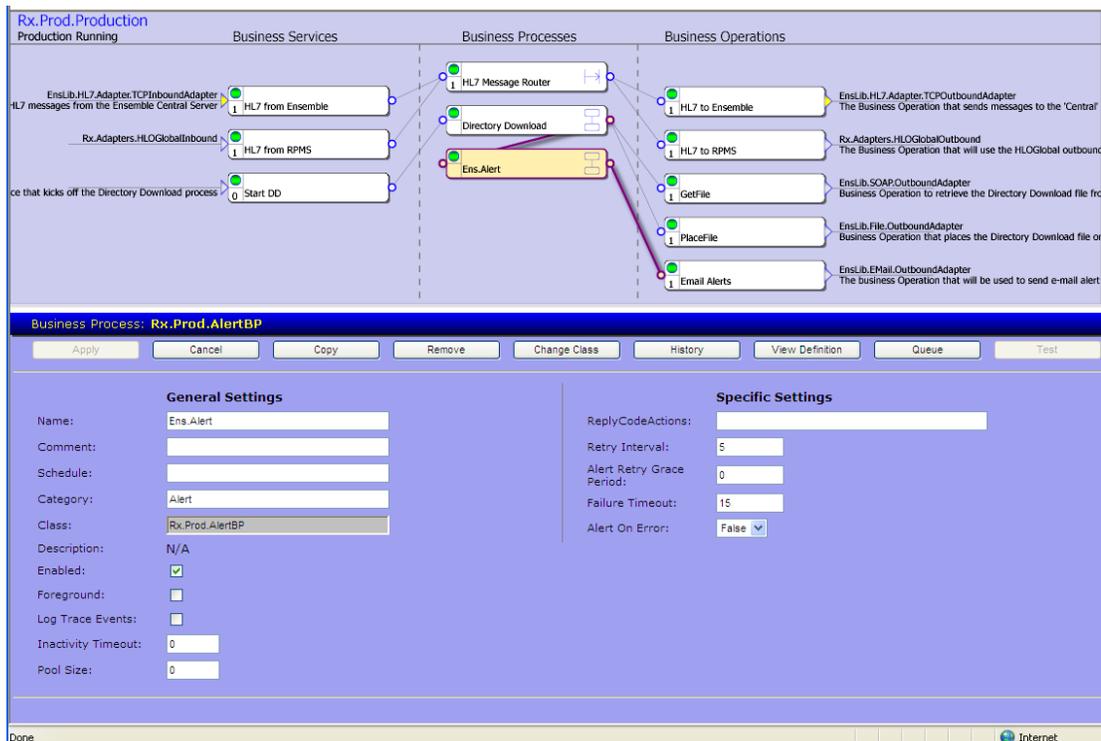


Figure 4-4: Process – Ens.Alert settings

The Production Settings in the lower left of the **Ens.Alert** window are listed in Table 4-8. The Additional Production Settings in the lower right of the window are listed in Table 4-9.

Table 4-8: Ens.Alert General Settings

Setting	Value	Description
Name	Ens.Alert	
Comment	(blank)	
Schedule	(blank)	This is the Start/Stop schedule for the business process.
Category	Alert	
Class	Rx.Prod.AlertBP	(Rx Package, DD Sub-Directory, BProcess Name)
Description	N/A	
Enabled	Checked	Item is enabled at production start up
Foreground	Not checked	This item is not run in the foreground
Log Trace Events	Not checked	Do not Log trace events for this item

Setting	Value	Description
Inactivity Timeout	0	Time (in seconds) that can elapse without an activity before this item is marked as being inactive. Setting this to 0 disables the inactivity timeout.
Pool Size	0	The Number of jobs created to host this item.

Table 4-9: Ens.Alert Specific Settings

Setting	Value	Description
ReplyCodeActions	(blank)	A comma-separated list of codes specifying what action this Process will take on various reply status conditions.
Retry Interval	5 (the default value)	How frequently to retry access to the output system.
Alert Grace Period	0	Always send an alert if there's an error
FailureTimeout	15 (the default value)	How long to keep retrying before giving up and returning an error code.
Alert On Error	False	Send an alert if there's an error with this Business Process.

4.2.4 Operation – Email Alerts

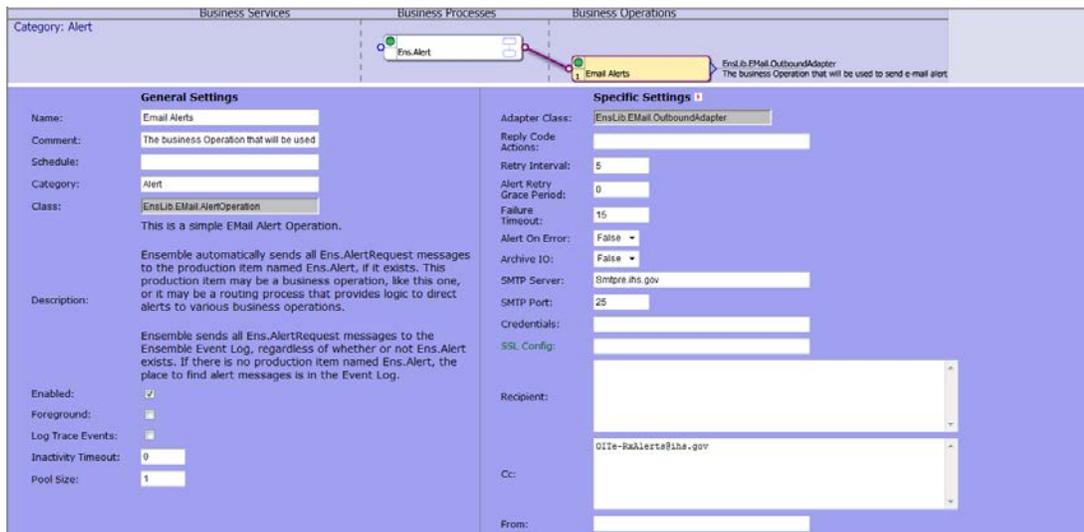


Figure 4-5: Operation – Email Alerts settings

The Production Settings in the lower left of the **Email Alerts** window are listed in Table 4-10. The Additional Production Settings in the lower right of the window are listed in Table 4-11.

Table 4-10: Email Alerts General Settings

Setting	Value	Description
Name	Email Alerts	
Comment	Business operation used to send email alerts messages.	
Schedule	(blank)	This is the Start/Stop schedule for the business process.
Category	Alert	
Class	EnsLib.EMail.AlertOperation	(Rx Package, DD Sub-Directory, BProcess Name)
Description	<p>Ensemble automatically sends all Ens.AlertRequest messages to the production item named Ens.Alert, if it exists. This production item may be a business operation, like this one, or it may be a routing process that provides logic to direct alerts to various business operations.</p> <p>Ensemble sends all Ens.AlertRequest messages to the Ensemble Event Log, regardless of whether or not Ens.Alert exists. If there is no production item named Ens.Alert, the place to find alert messages is in the Event Log.</p>	
Enabled	Checked	Item is enabled at production start up
Foreground	Not checked	This item is not run in the foreground
Log Trace Events	Not checked	Do not Log trace events for this item
Inactivity Timeout	0	Time (in seconds) that can elapse without an activity before this item is marked as being inactive. Setting this to 0 disables the inactivity timeout.
Pool Size	1	The Number of jobs created to host this item.

Table 4-11: Email Alerts Specific Settings

Setting	Value	Description
Adapter Class	EnsLib.EMail.OutboundAdapter	
ReplyCodeActions	(blank)	A comma-separated list of codes specifying what action this Process will take on various reply status conditions.
Retry Interval	5 (the default value)	How frequently to retry access to the output system.
Alert Grace Period	0	Always send an alert if there's an error
FailureTimeout	15 (the default value)	How long to keep retrying before giving up and returning an error code.
Alert On Error	False	Send an alert if there's an error with this Business Process.
Archive IO	False	
SMTP Server	Smtppre.ihs.gov	*If not using IHS email use the site's SMTP server.
SMTP Port	25	
Credentials	(blank)	
SSL Config	(blank)	
Recipient	Email addresses of Local and Area IT personnel responsible for Local Server Production (addresses are separated by a semicolon or comma)	
Cc	OITe-RxAlerts@ihs.gov	Additional Cc'd recipients can be added as needed.
From		

4.2.5 Operation – GetFile

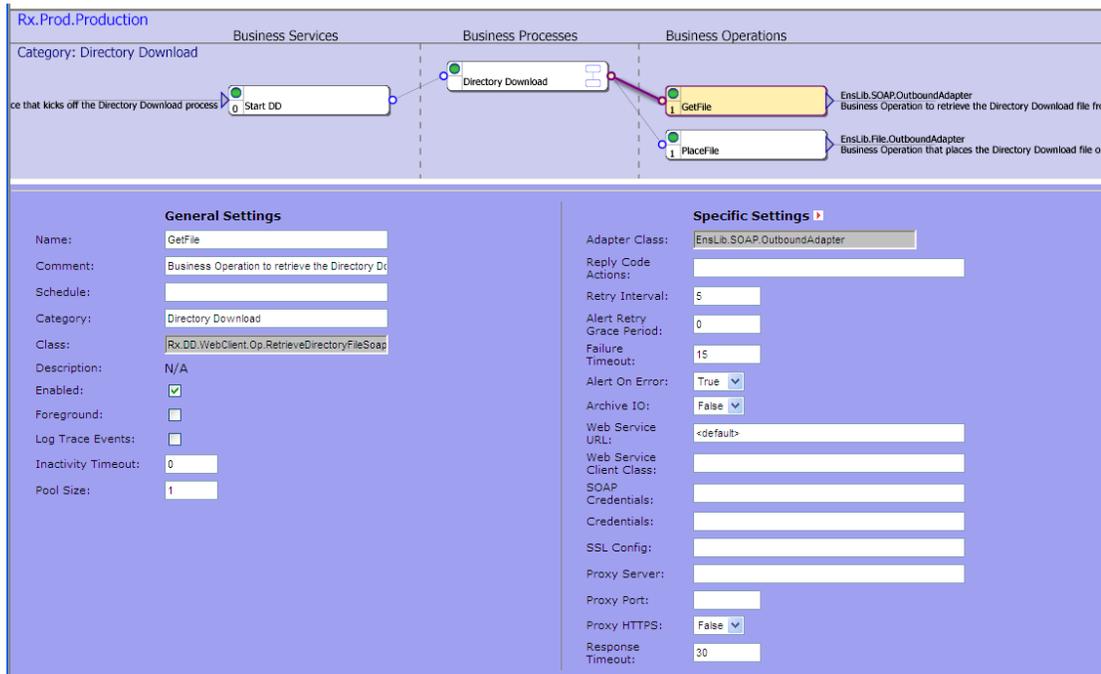


Figure 4-6: Operation – GetFile settings

The Production Settings in the lower left of the **GetFile** window are listed in Table 4-12. The Additional Production Settings in the lower right of the window are listed in Table 4-13.

Table 4-12: GetFile General Settings

Setting	Value	Description
Name	GetFile	
Comment	Business Operation to retrieve the Directory Download file from the Central Server	
Schedule	(blank)	This is the Start/Stop schedule for the business process.
Category	Directory Download	
Class	Rx.DD.WebClient.Op.RetrieveDirectoryFileSoap	(Rx Package, DD Sub-Directory, BProcess Name)
Description	N/A	
Enabled	Checked	Item is enabled at production start up
Foreground	Not checked	This item is not run in the foreground

Setting	Value	Description
Log Trace Events	Not checked	Do not Log trace events for this item
Inactivity Timeout	0	Time (in seconds) that can elapse without an activity before this item is marked as being inactive. Setting this to 0 disables the inactivity timeout.
Pool Size	1	The Number of jobs created to host this item.

Table 4-13: GetFile Specific Settings

Setting	Value	Description
Adapter Class	EnsLib.SOAP.OutboundAdapter	
ReplyCodeActions	(blank)	A comma-separated list of codes specifying what action this Process will take on various reply status conditions.
Retry Interval	5 (the default value)	How frequently to retry access to the output system.
Alert Grace Period	0	Always send an alert if there's an error
FailureTimeout	15 (the default value)	How long to keep retrying before giving up and returning an error code.
Alert On Error	True	Send an alert if there's an error with this Business Process.
Archive IO	False	
Web Service URL	<default>	
Web Service Client Class	(blank)	
SOAP Credentials	(blank)	
Credentials:	(blank)	
SSL Config	(blank)	
Proxy Server	(blank)	
Proxy Port	(blank)	
Proxy HTTPS	False	
Response Timeout	30	

4.2.6 Operation – PlaceFile

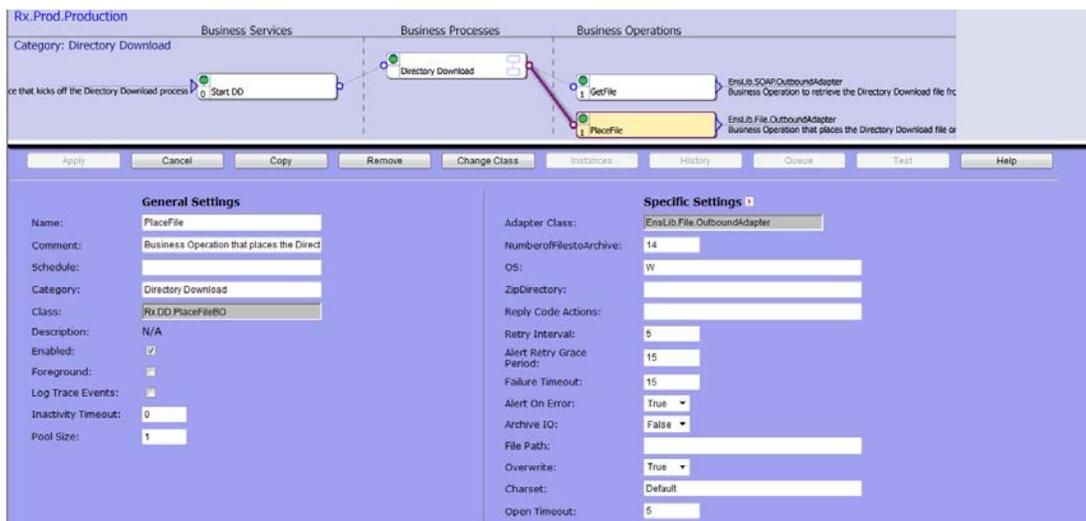


Figure 4-7: Operation - PlaceFile settings

The Production Settings in the lower left of the **PlaceFile** window are listed in Table 4-14. The Additional Production Settings in the lower right of the window are listed in Table 4-15.

Table 4-14: PlaceFile General Settings

Setting	Value	Description
Name	PlaceFile	
Comment	Business Operation that places the Directory Download file onto the local server.	
Schedule	(blank)	This is the Start/Stop schedule for the business process.
Category	Directory Download	
Class	Rx.DD.PlaceFileBO	(Rx Package, DD Sub-Directory, BProcess Name)
Description	N/A	
Enabled	Checked	Item is enabled at production start up
Foreground	Not checked	This item is not run in the foreground
Log Trace Events	Not checked	Do not Log trace events for this item
Inactivity Timeout	0	Time (in seconds) that can elapse without an activity before this item is marked as being inactive. Setting this to 0 disables the inactivity timeout.
Pool Size	1	The Number of jobs created to host this item.

Table 4-15: PlaceFile Specific Settings

Setting	Value	Description
Adapter Class	EnsLib.File.OutboundAdapter	
NumberOfFilestoArchive	14	The number of Directory Download files to be archived.
OS	W	Must be populated with either a "W" for Windows or a "U" for Unix
ZipDirectory		Populate with the path to the decompression software. Example: c:\Program Files\7Zip. If this is a Unix environment please use gzip.
ReplyCodeActions	(blank)	
Retry Interval	5	.
Alert Retry Grace Period	15	
Failure Timeout	15	
Alert On Error	True	
Archive IO	False	
File Path		(configurable by the Site, must match RPMS Directory Download configuration)
Overwrite	True	
Charset	Default	
Open Timeout	5	

4.3 Pass-Through Settings

The delivery of HL7 messages between the local RPMS system and the Central Server process of the Ensemble Production.

The settings described in this section were configured during implementation to the values specified at that time. Except as otherwise described herein, do not change these settings without conferring with the National e-Prescriptions Deployment Team.

4.3.1 Service – HL7 from RPMS

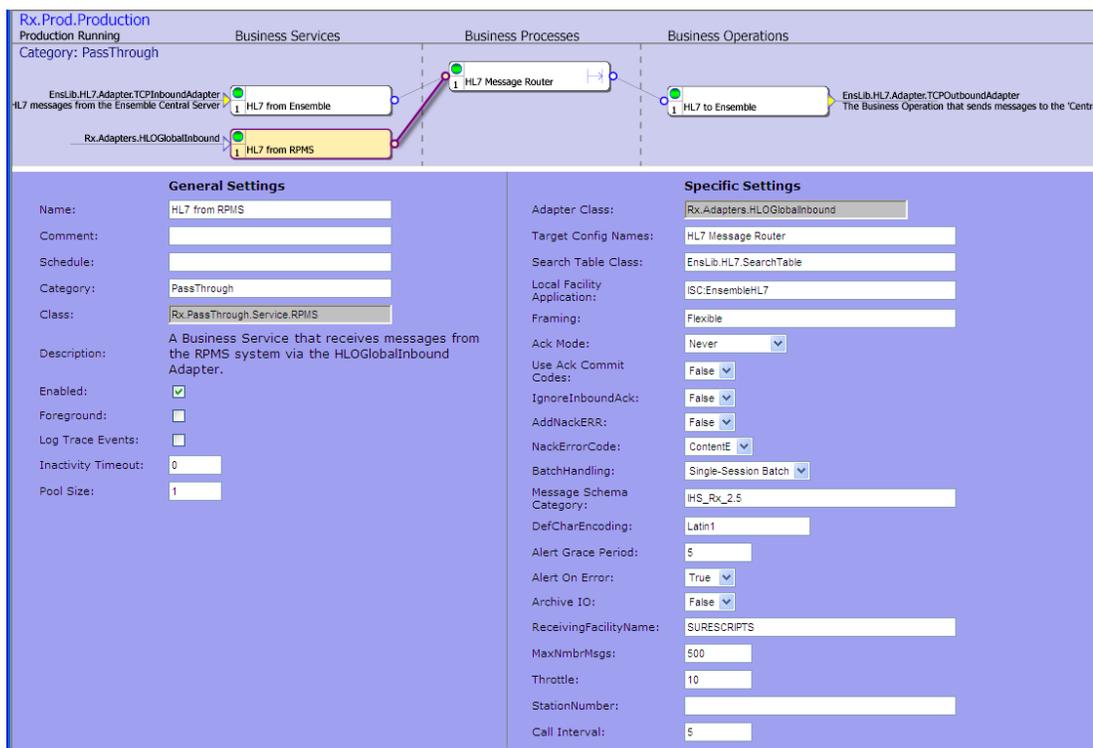


Figure 4-8: Service – HL7 from RPMS settings

The Production Settings in the lower left of the **HL7 from RPMS** window are listed in Table 4-16. The Additional Production Settings in the lower right of the window are listed in Table 4-17.

Table 4-16: HL7 from RPMS General Settings

Setting	Value	Description
Name	HL7 from RPMS	
Comment	(blank)	
Schedule	(blank)	This is the Start/Stop schedule for the business process.
Category	PassThrough	
Class	Rx.PassThrough.Service.RPMS	(Rx Package, DD Sub-Directory, BProcess Name)
Description	A Business Service that receives messages from the RPMS system via the HLOGlobalInbound Adapter.	
Enabled	Checked	Item is enabled at production start up

Setting	Value	Description
Foreground	Not checked	This item is not run in the foreground
Log Trace Events	Not checked	This item logs trace events and should only be used for troubleshooting purposes.
Inactivity Timeout	0	Time (in seconds) that can elapse without an activity before this item is marked as being inactive. Setting this to 0 disables the inactivity timeout.
Pool Size	1	The Number of jobs created to host this item.

Table 4-17: HL7 from RPMS Specific Settings

Setting	Value
Adapter Class	Rx.Adapters.HLOGlobalinbound
Target Config Names	HL7 Message Router
Search Table Class	EnsLib.HL7.SearchTable
Local Facility Application	ISC:EnsembleHL7
Framing	Flexible
Ack Mode	Never
Use Ack Commit Codes	False
Ignore Inbound Ack	False
Add Nack ERR	False
Nack Error Codes	ContentE
Batch Handling	Single-Session Batch
Message Schema Category	IHS_Rx_2.5
Def Char Encoding	Latin 1
Alert Grace Period	5
Alert On Error	True
Archive IO	False
Receiving Facility Name	SURESCRIPTS
Max Nmbr Msgs	500
Throttle	10
Station Number	(blank)
Call Interval	5

4.3.2 Service – HL7 from Ensemble

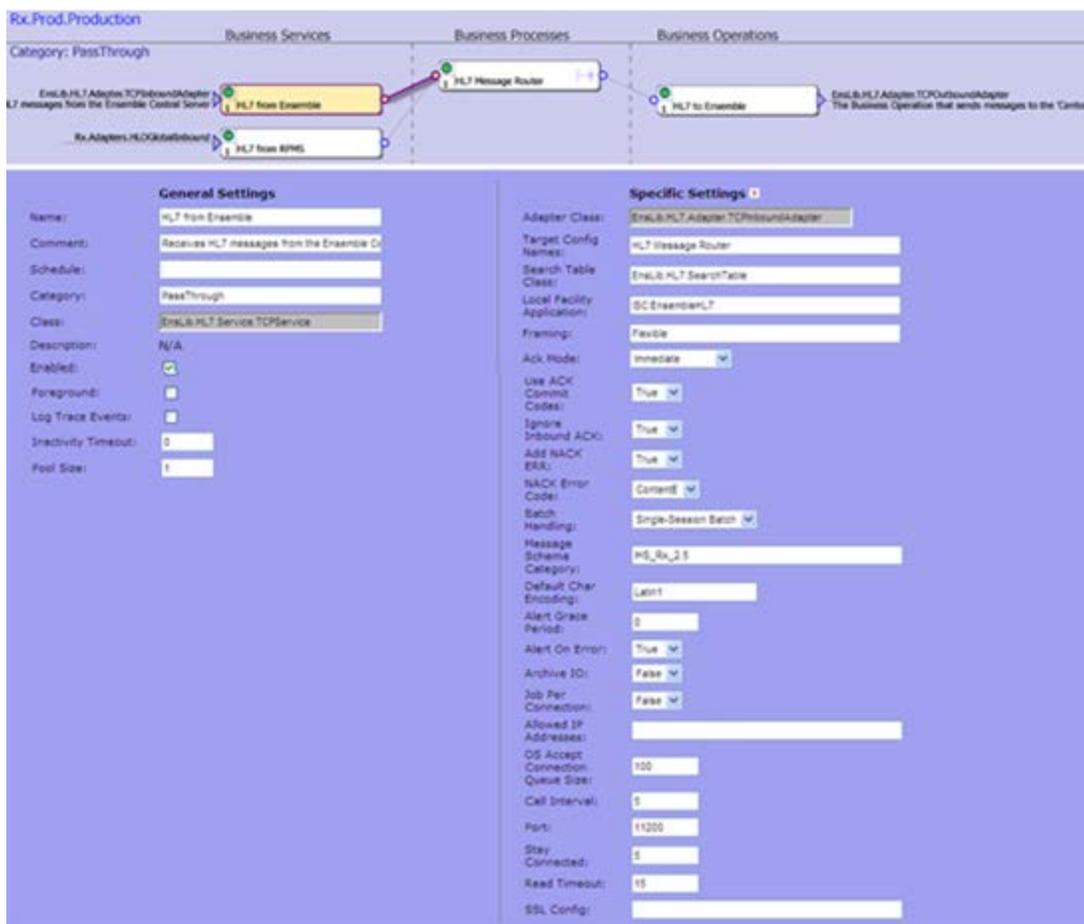


Figure 4-9: HL7 from Ensemble settings

The Production Settings in the lower left of the **HL7 from Ensemble** window are listed in Table 4-18. The Additional Production Settings in the lower right of the window are listed in Table 4-19.

Table 4-18: HL7 from Ensemble General Settings

Setting	Value	Description
Name	HL7 from Ensemble	
Comment	Receives HL7 messages from the Ensemble Central Server	
Schedule	(blank)	This is the Start/Stop schedule for the business process.
Category	PassThrough	
Class	EnsLib.HL7.Service.TCPService	(Rx Package, DD Sub-Directory, BProcess Name)

Setting	Value	Description
Description	N/A	
Enabled	Checked	Item is enabled at production start up
Foreground	Not checked	This item is not run in the foreground
Log Trace Events	Not checked	This item logs trace events and should only be used for troubleshooting purposes.
Inactivity Timeout	0	Time (in seconds) that can elapse without an activity before this item is marked as being inactive. Setting this to 0 disables the inactivity timeout.
Pool Size	1	The Number of jobs created to host this item.

Table 4-19: HL7 from Ensemble Specific Settings

Setting	Value
Adapter Class	EnsLib.HL7.Adapter.TCPI inboundAdapter
Target Config Names	HL7 Message Router
Search Table Class	EnsLib.HL7.SearchTable
Local Facility Application	ISC:EnsembleHL7
Framing	Flexible
Ack Mode	Immediate
Use Ack Commit Codes	True
Ignore Inbound Ack	True
Add Nack ERR	True
Nack Error Codes	ContentE
Batch Handling	Single-Session Batch
Message Schema Category	IHS_Rx_2.5
Def Char Encoding	Latin 1
Alert Grace Period	0
Alert On Error	True
Archive IO	False
Job per Connection	False
Allowed IP Addresses	Insert IP address of the Central server
OS Accept Connection Queue Size	100
Call Interval	5
Port	11200

Setting	Value
Stay Connected	5
Read Timeout	15
SSL Config	(blank)

4.3.3 Process – HL7 Message Router

Figure 4-10: **Process – HL7 Message Router** settings

The Production Settings in the lower left of the **HL7 Message Router** window are listed in Table 4-20. The Additional Production Settings in the lower right of the window are listed in Table 4-21.

Table 4-20: HL7 Message Router General Settings

Setting	Value	Description
Name	HL7 Message Router	
Comment	(blank)	
Schedule	(blank)	This is the Start/Stop schedule for the business process.
Category	PassThrough	

Setting	Value	Description
Class	EnsLib.HL7.MsgRouter.RoutingEngine	(Rx Package, DD Sub-Directory, BProcess Name)
Description	N/A	
Enabled	Checked	Item is enabled at production start up
Foreground	Not checked	This item is not run in the foreground
Log Trace Events	Not checked	This item logs trace events and should only be used for troubleshooting purposes.
Inactivity Timeout	0	Time (in seconds) that can elapse without an activity before this item is marked as being inactive. Setting this to 0 disables the inactivity timeout.
Pool Size	1	The Number of jobs created to host this item.

Table 4-21: HL7 Message Router General Settings

Setting	Value
Local Facility Application	ISC:EnsembleHL7
Ack Type	Application
Nack Code	Error
Add Nack ERR	False
Validation	dm-z
Business Rule Name	Rx.MRR.PassThrough
Alert On Bad Message	True
Bad Message Handler	(blank)
Response From	(blank)
Response Target Config Names	(blank)
Response Timeout	-1
Force Sync Send	False
Reply Code Actions	(blank)
Retry Interval	5
Alert Retry Grace Period	0
Failure Timeout	15
Alert On Error	False

4.3.4 Operation – HL7 to RPMS



Figure 4-11: Operation – HL7 to RPMS settings

The Production Settings in the lower left of the **HL7 to RPMS** window are listed in Table 4-22. The Additional Production Settings in the lower right of the window are listed in Table 4-23.

Table 4-22: HL7 to RPMS General Settings

Setting	Value	Description
Name	HL7 to RPMS	
Comment	The Business Operation that will use the HLOGlobal outbound adapter to write HL7 messages into the HLO global nodes.	
Schedule	(blank)	This is the Start/Stop schedule for the business process.
Category	(blank)	
Class	Rx.PassThrough.Operation.RPMS	(Rx Package, DD Sub-Directory, BProcess Name)
Description	N/A	
Enabled	Checked	Item is enabled at production start up
Foreground	Not checked	This item is not run in the foreground

Setting	Value	Description
Log Trace Events	Not checked	This item logs trace events and should only be used for troubleshooting purposes.
Inactivity Timeout	0	Time (in seconds) that can elapse without an activity before this item is marked as being inactive. Setting this to 0 disables the inactivity timeout.
Pool Size	1	The Number of jobs created to host this item.

Table 4-23: HL7 to RPMS Specific Settings

Setting	Value
Adapter Class	Rx.Adapters.HLOGlobalOutbound
Separators	^~\&
Search Table Class	(blank)
Def Char Encoding	Latin 1
Reply Code Actions	(blank)
Retry Interval	5
Alert Retry Grace Period	5
Failure Timeout	25
Alert On Error	True
Archive IO	False
Framing	MLLP
Station Number	<Insert Site Station Number>
LLink	APSP RPMS
ACKTypes	(blank)

4.3.5 Operation – HL7 to Ensemble

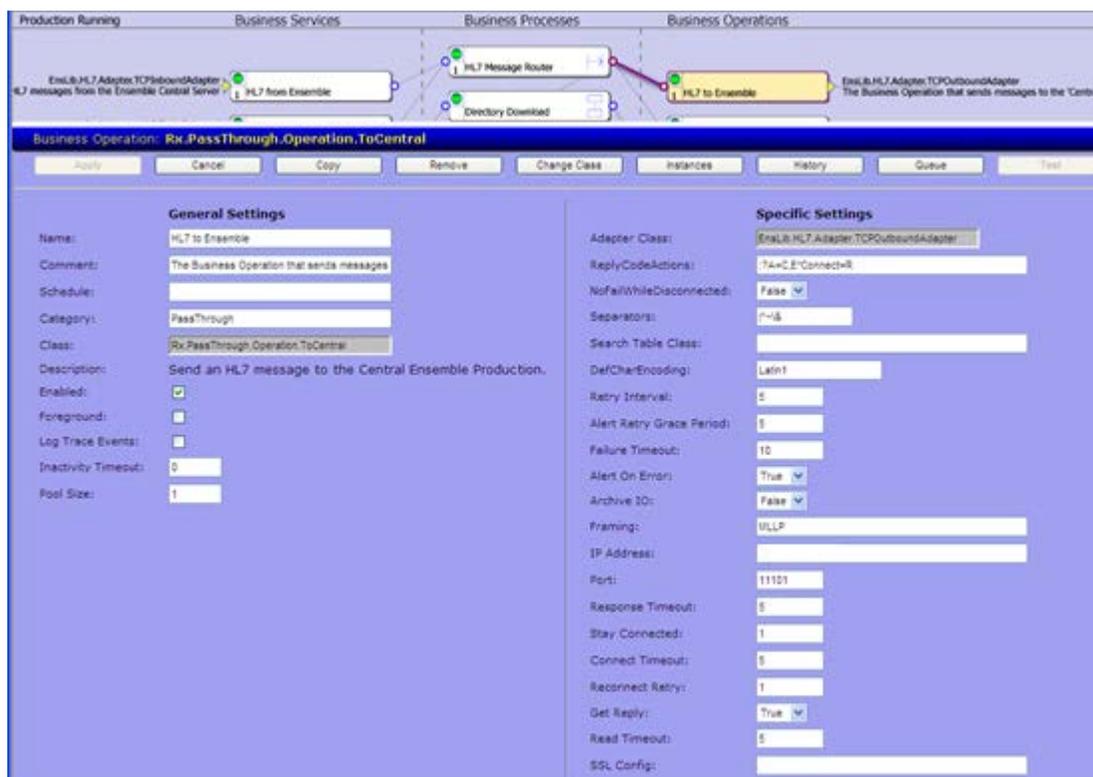


Figure 4-12: Operation – HL7 to Ensemble settings

The Production Settings in the lower left of the **HL7 to Ensemble** window are listed in Table 4-24. The Additional Production Settings in the lower right of the window are listed in Table 4-25.

Table 4-24: HL7 to Ensemble General Settings

Setting	Value	Description
Name	HL7 to Ensemble	
Comment	The Business Operation that sends messages to the 'Central' Ensemble Server.	
Schedule	(blank)	This is the Start/Stop schedule for the business process.
Category	PassThrough	
Class	Rx.PassThrough.Operation.ToCentral	(Rx Package, DD Sub-Directory, BProcess Name)
Description	Send an HL7 message to the Central Ensemble Production.	

Setting	Value	Description
Enabled	Checked	Item is enabled at production start up
Foreground	Not checked	This item is not run in the foreground
Log Trace Events	Not checked	This item logs trace events and should only be used for troubleshooting purposes.
Inactivity Timeout	0	Time (in seconds) that can elapse without an activity before this item is marked as being inactive. Setting this to 0 disables the inactivity timeout.
Pool Size	1	The Number of jobs created to host this item.

Table 4-25: HL7 to Ensemble Specific Settings

Setting	Value
Adapter Class	Rx.Adapters.HLOGlobalOutbound
Reply Code Actions	:?A=C,E*Connect=R
No Fail While Disconnected	False
Separators	^~\&
Search Table Class	(blank)
Def Char Encoding	Latin 1
Retry Interval	5
Alert Retry Grace Period	5
Failure Timeout	10
Alert On Error	True
Archive IO	False
Framing	MLLP
IP Address	<IP of "Central" server>
Port	11101
Stay Connected	1
Connect Timeout	5
Reconnect retry	1
Get Reply	True
Response timeout	5
Read Timeout	5
SSL Config	(blank)

4.4 Sample Cache Install

1. From Ensemble Cube, open the System Management Portal.
2. Select **Configure Namespaces** from the **Go to** list shown in Figure 4-13:

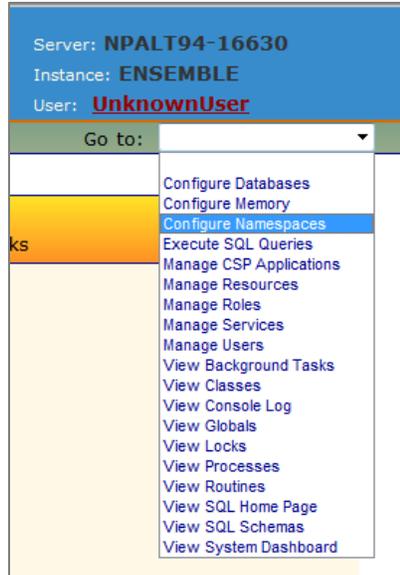


Figure 4-13: Go to list

3. Select **Configure Namespaces** from the **Go to** list displayed in Figure 4-14:

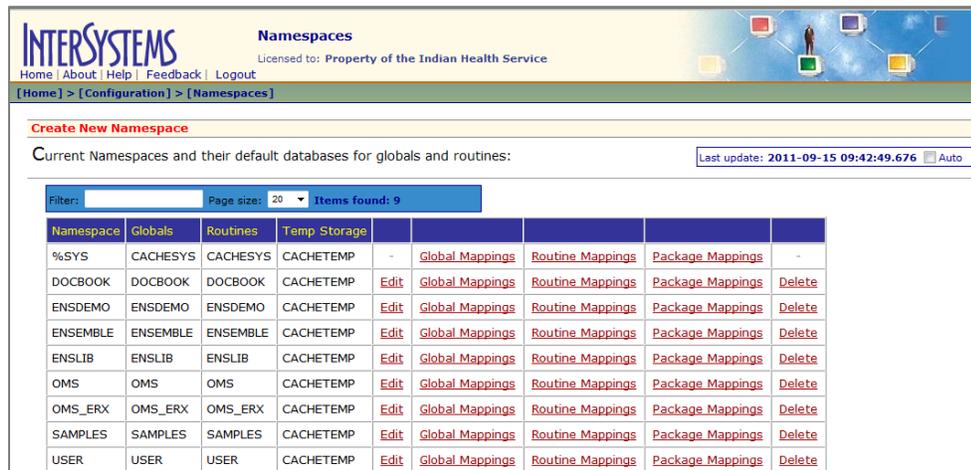
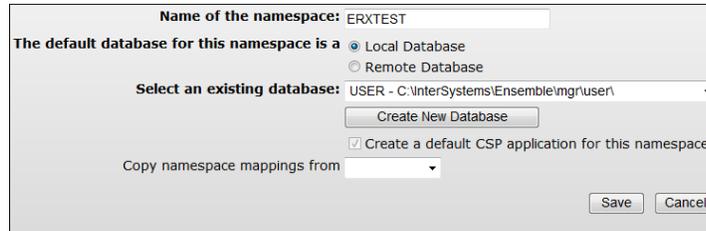


Figure 4-14: Namespaces window

4. Select **Create New Namespace** as shown in Figure 4-15:

Figure 4-15: **Create New Namespace** dialog

5. Type the name of the e-Prescribing database in the **Name of the namespace** field. The recommended naming convention is “ERX” followed by the site namespace (for example: ERXTEST).
6. Click **Create New Database**.
7. Type the name of the e-Prescribing database used as shown in (Figure 4-16):

Figure 4-16: **Database Wizard** dialog

8. Click **Browse** and navigate to the location where the site stores its RPMS databases.
9. Type the name of the e-Prescribing database at the end of the directory path.

10. Click **Next**. The **Enter details about the database** window displays as shown in Figure 4-17:

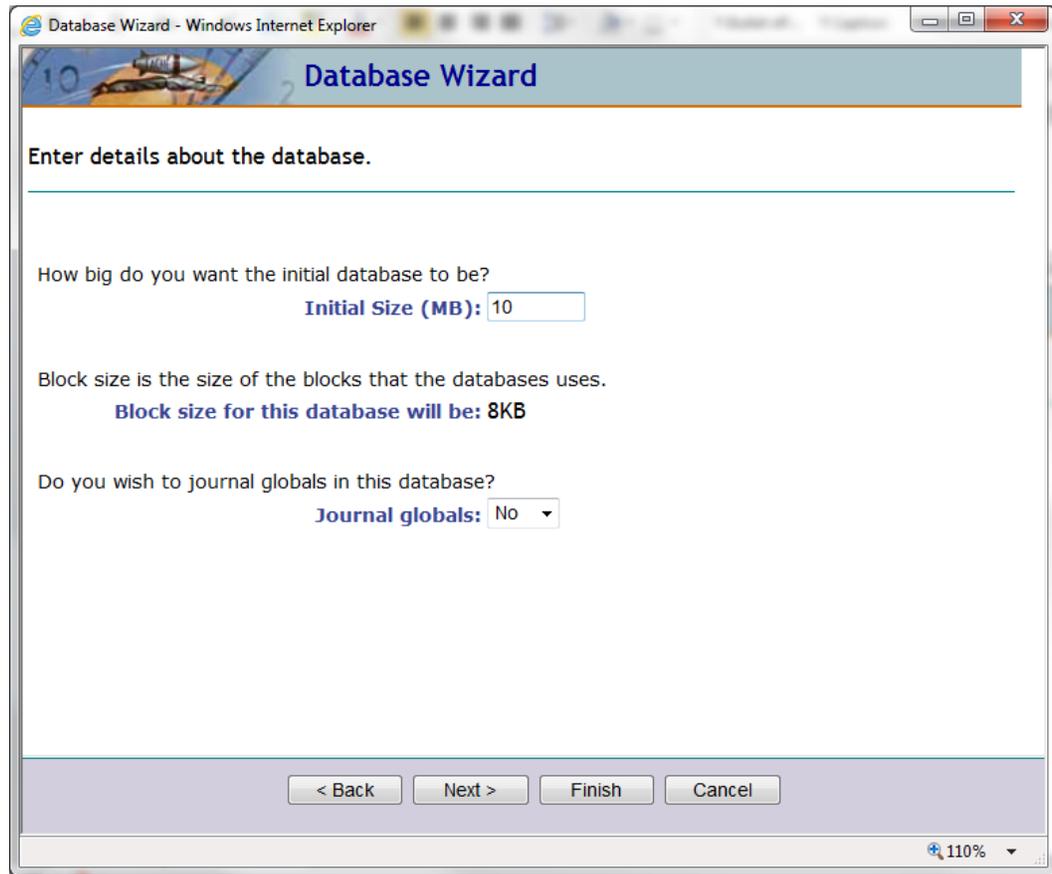


Figure 4-17: **Database Wizard** dialog

11. Type the database settings:
- Initial Size (MB): **10**
 - Journal globals: **No**
12. Click **Next** and the **Database Wizard** window displays as shown in Figure 4-18:

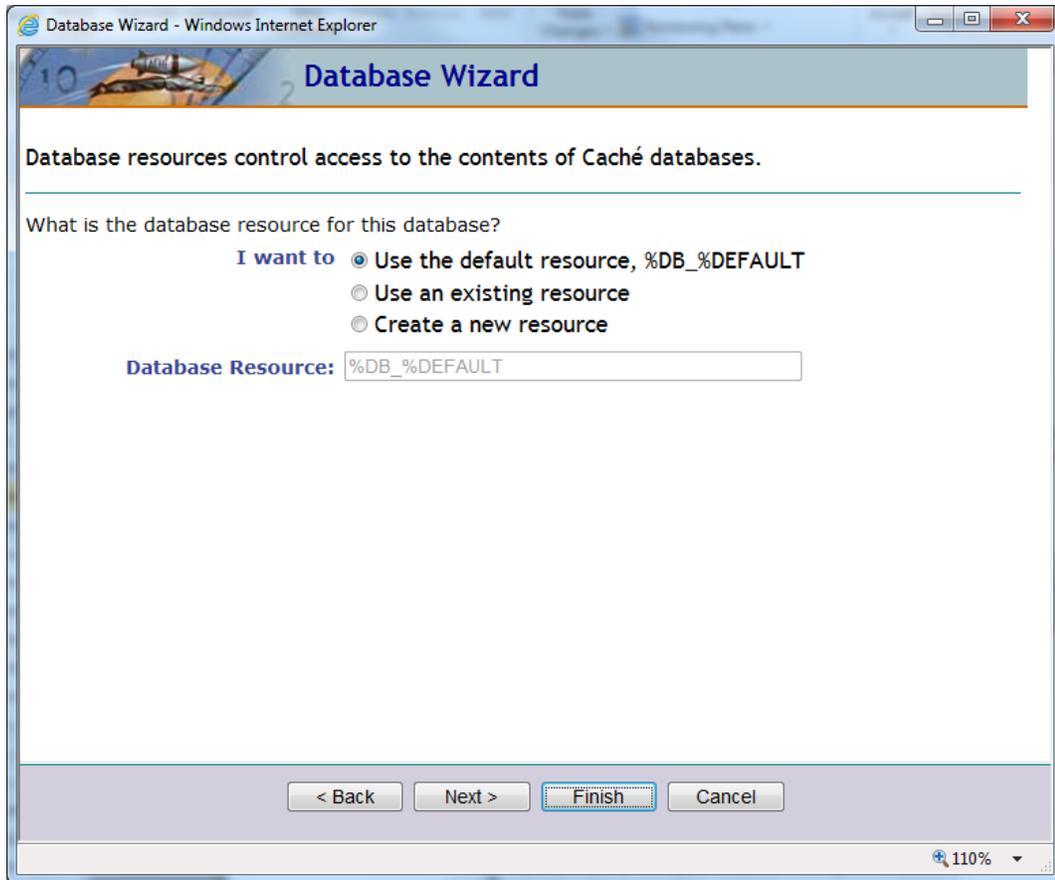


Figure 4-18: Database Wizard dialog

13. Click **Finish**. The **Create New Namespace** dialog displays (Figure 4-19).

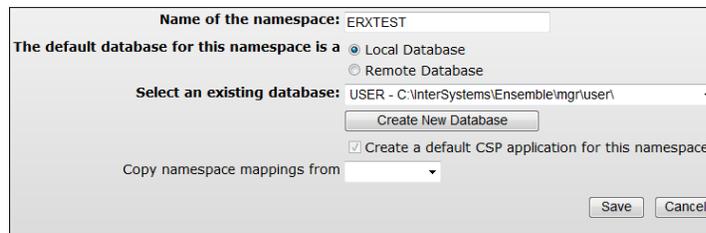


Figure 4-19: Create New Namespace dialog

14. Click **Save**.

5.0 Installation Configuration

5.1 Map HL* Globals

In order for the HL7 messages to be transmitted to the central server, the HL Globals must be mapped.

1. From Ensemble Cube, open the **System Management Portal** shown in Figure 5-1:

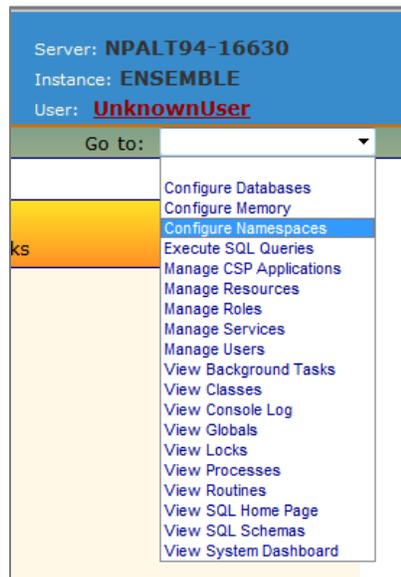


Figure 5-1: **Go to** list

2. Select **Configure Namespaces** from the **Go to** list displayed in Figure 5-2:

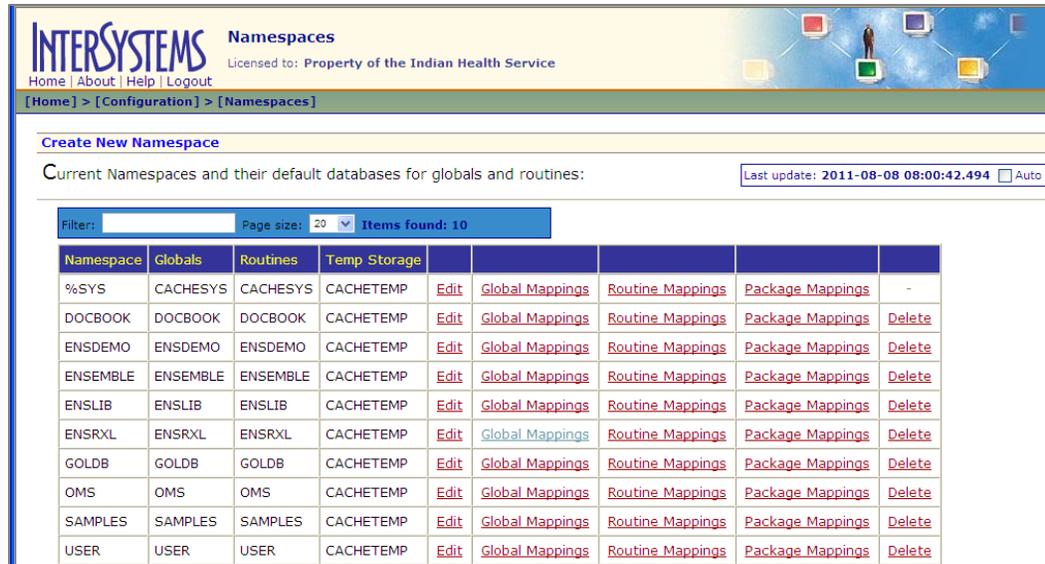


Figure 5-2: Namespaces window

3. Click **Global Mappings** on the row corresponding with the ePrescribing namespace as shown in Figure 5-3:

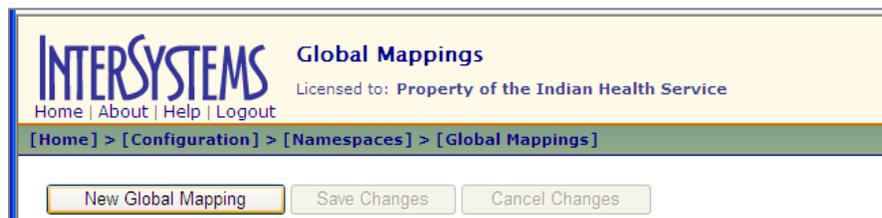


Figure 5-3: Global Mappings window, upper left portion

4. Click **New Global Mapping** (Figure 5-4).

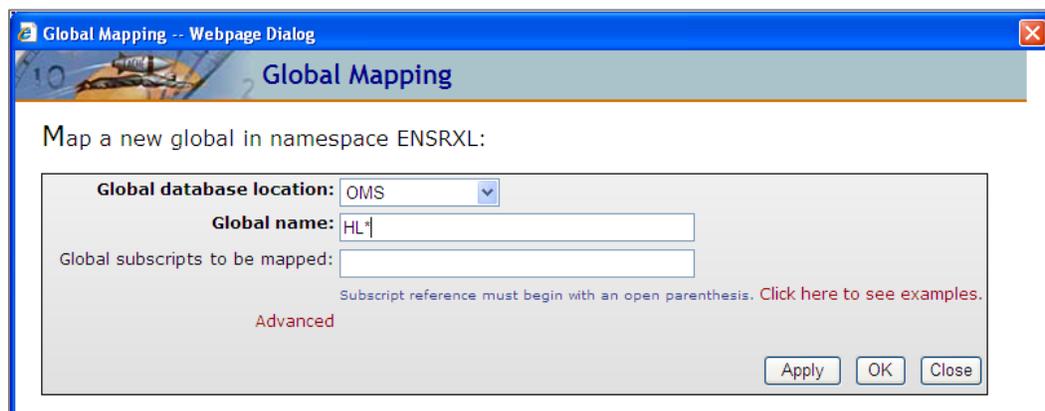


Figure 5-4: Global Mapping dialog

5. From the dropdown at the “Global database location” prompt select the site database that will be used for EHR:
 - Global database location: <RPMS namespace>
 - Global name: HL*
6. Click **OK**. The **Global Mappings** window (Figure 5-5) displays.



Figure 5-5: **Global Mappings** window, after changes.

7. Click **Save Changes**.

5.2 Auto-Start Production Settings

This enables Ensemble to automatically start the production at start-up:

1. Open the **Ensemble Management Portal** window as shown in Figure 5-6:

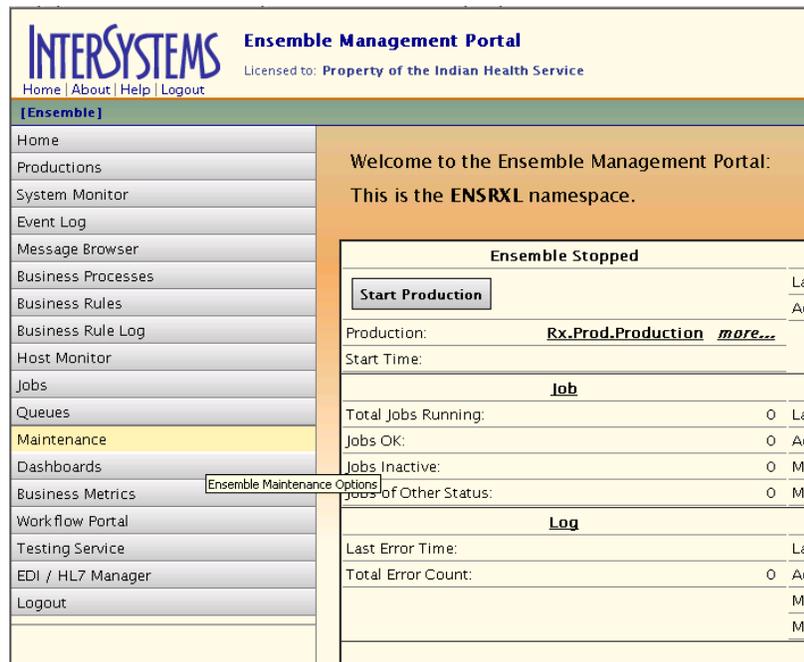


Figure 5-6: **Ensemble Management Portal** window

2. Select the **Maintenance** menu shown in Figure 5-7.

Choose a function you want to perform from the menu.

Current Ensemble Version is 2009.1.4.803

Management Auto Timeout

Check here if you want Ensemble pages to automatically close and return to the Login page after a page is inactive for 28800 seconds.

Auto-Refresh Rate seconds

This rate is used to auto-refresh the Ensemble pages, when applicable. Enter 0 for no Refresh.

Auto-Start Production

You may select a production to start automatically at system startup.

Modification Saved.

Figure 5-7: Maintenance menu

3. Select **Rx.Prod.Production** from the **Auto-Start Production** list.
4. Click **Save**.

5.3 Add Directory Download Task

1. Open the **Task Manager** window shown in Figure 5-8:



Figure 5-8: Task Manager window

2. Select **Schedule New Task**. Figure 5-9 shows the **Task Scheduler Wizard** dialog.

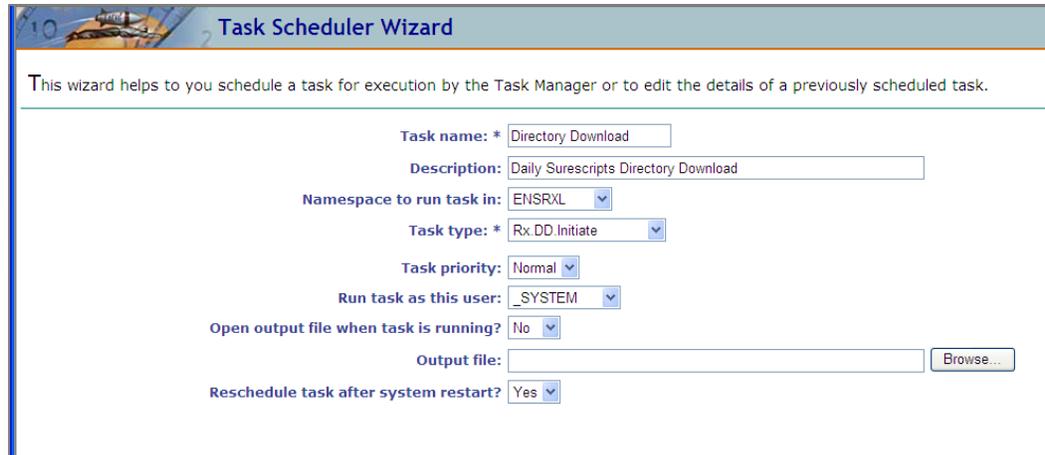


Figure 5-9: Task Scheduler Wizard dialog

3. Type the required information for the task shown in Table 5-1:

Table 5-1: Task Scheduler settings, page 1

Label	Setting
Task Name	Directory Download
Namespace in which to run task	<Select the e-Prescribing namespace created for the site>
Task type	Rx.DD.Initiate
Run task as this user	_SYSTEM
Open output file when task is running	No
Output file	(blank)
Reschedule system after restart	Yes

4. Click **Next** to display the Task Scheduler Wizard (Figure 5-10).

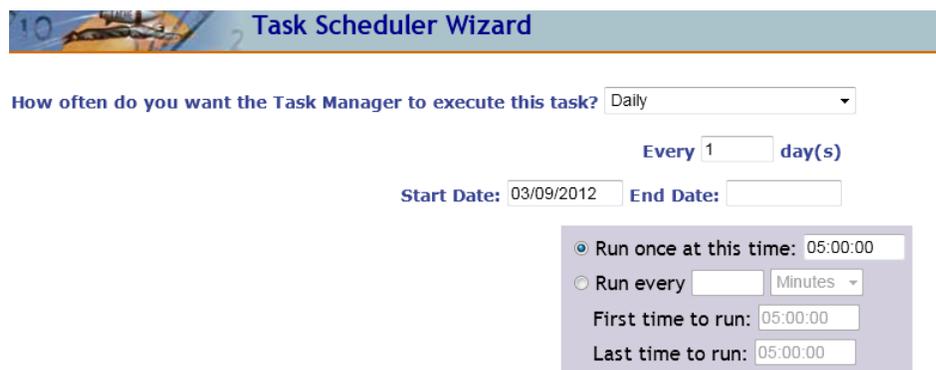


Figure 5-10: Task Scheduler Wizard dialog

5. Type the schedule information as shown in Table 5-2:

Table 5-2: Task Scheduler settings, page 2

Setting	Value	Description
How often do you want the Task Manager to execute this task?	Daily	
Run once at this time	05:00	This must be scheduled to run after the 'Central' Server runs its nightly download, the 'Central' production is scheduled to run at 04:30 ET A.M.

6. Click **Finish** to add the task to the schedule.

Appendix A: 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 Rules of Behavior 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 web site,

<http://security.ihs.gov/>

The Rules of Behavior 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.
- Not 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, superuser, 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.
- Not release any sensitive agency or patient information.

Glossary

Central Server

The central server is the communications hub between Indian Health Service (IHS) sites and Surescripts.

Directory Download

The Directory Download is a flat file with lists of the pharmacies and prescribers registered within the network.

As stated in Surescripts Directories Guide 4.0 Q4 2007.pdf:

Network participants can download flat file lists of the pharmacies and prescribers registered within the network. The lists are filtered based on the access of the network participant performing the download. Surescripts requires all network participants to update directory information nightly and to do full update at least once a week. Surescripts network participants must not block incoming messaging based on local directory information. Surescripts maintains the integrity of the directory information and will validate current participants. Full download files are generated every night at midnight and contain every pharmacy \ prescriber available to the network participant performing the download. Nightly download files are generated every night at midnight and are a delta file of the records that changed during the course of that specific day.

Ensemble Cube

The Cube is an instance of Ensemble running in the system tray in a Windows environment.

Local Server

The Local server is the site server that initiates and is the final destination for messaging with Surescripts

NewRX

NewRx is used in reference to a message transaction for a new prescription from a Prescriber. As stated in RxHub PRN Implementation Guide.pdf:

This NCPDP SCRIPT transaction is a request for a new prescription and is sent from the prescriber via the Physician System to the pharmacy of the patient's choice. A Status message is sent to indicate whether it was accepted or whether there was an error.

SPI

As stated in Surescripts Directories Guide 4.0 Q4 2007.pdf:

The Surescripts Prescriber ID (SPI) consists of an SPI root and a location ID.

$SPI = SPI\ Root + Location\ ID$

The SPI Root is generated by Surescripts and is a ten-digit numeric value. Each prescriber will be assigned a unique SPI Root and SPI location ID. Since a prescriber can prescribe from more than one location, the Location ID is used to distinguish between multiple locations for the same prescriber. The Location ID is a three-digit numeric value.

Contact Information

If you have any questions or comments regarding this distribution, please contact the OIT Help Desk (IHS).

Phone: (505) 248-4371 or (888) 830-7280 (toll free)

Fax: (505) 248-4363

Web: <http://www.ihs.gov/GeneralWeb/HelpCenter/Helpdesk/index.cfm>

Email: support@ihs.gov