# limprivata<sup>®</sup>

## **Product Documentation**

Imprivata PatientSecure High Availability Support for Load Balancing

Imprivata PatientSecure<sup>®</sup> 6.10

© 2024 Imprivata, Inc. All Rights Reserved.

## Table of Contents

High Availability Support	
Architecture	
Terminology	
PatientSecure Services Supported for High Availability	
Before You Begin	
Review System Requirements	
Gather Server Information	
Review Additional References	
Review the PatientSecure Communication Ports	
Installation Sequence	
Step 1: Obtain and Import Certificate Authority to the Load Balancer Server	
Step 2: Install Required Software on Load Balancer Server	
Microsoft IIS and ARR	
Citrix ADC	
F5 BIG-IP GTM/LTM Load Balancer	
Step 3: Install PatientSecure Server Console on the Load Balancer Server	
Step 4: Add the Application Servers to PatientSecure Server Console	
Configure the Load Balancer Server	
Microsoft IIS with ARR	
Step 1: Configure IIS	
Step 2: Configure the PatientSecure Identity Server	
Step 2a: Install the PatientSecure Identity Server on the Application Servers	
Step 2b: Configure Advanced Settings	
Step 2c: Create a Server Farm for the Identity Server	
Step 2d: Configure Failover for Identity Service	
Step 3: Configure PatientSecure Web Services	
Step 3a: Install PatientSecure Web Services on the Application Servers	
Step 3b: Configure Advanced Settings Step 3c: Create a Server Farm for the PatientSecure Web Service	
Step 3d: Configure Failover for Web Services	
Step 4: Configure the User Interface Server	
Step 4: Install the PatientSecure User Interface Server on the Application Servers	
Step 4a. Instantine Patient Secure Oser Interface Server on the Application Servers	
Step 40: Comigare Advanced Settings	
Step 4d: Configure Failover of the User Interface Server	
Step 5: Configure the Admin Console	
Step 5: Install the Admin Console on the Application Servers	
Step 5b: Create a Server Farm for the Admin Console	
Step 5c: Configure Failover for the Admin Console.	
Step 6: Configure the Reporting Service	
Step 6a: Install the Reporting Service on the Application Servers	
Step 6b: Configure Advanced Settings	
Step 6c: Create a Server Farm for the Reporting Service	
Step 7: Configure the PatientSecure Emergency Search & Authentication Service Server	
Step 7a: Install the Emergency Search & Authentication Service on the Application Servers	
Step 7b: Configure Advanced Settings	
Step 7c: Create a Server Farm for the Emergency Search & Palm Vein Authentication Service	
Step 8: Configure the PatientSecure System Health Service	
Step 8a: Install the System Health Service on the Application Servers	
Step 8b: Configure Advanced Settings	
Step 8c: Create a Server Farm for the System Health Service	
Step 9: Install the HL7 Service on the Application Servers	
Step 10: Configure the FHIR Service	
Step 10a: Install the FHIR Service on the Application Servers	
Step 10b: Add Third-Party Certificate to Application Servers	
Step 10c: Configure Advanced Settings	
Step 10d: Create a Server Farm for the FHIR Service	

Step 11: Configure the EMPI Service	. 30
Step 11a: Install the EMPI Service on the Application Servers	30
Step 11b: Add Third-Party Certificate to Application Servers	. 31
Step 11c: Configure Advanced Settings	31
Step 11d: Create a Server Farm for the EMPI Service	31
Citrix ADC (formerly Netscaler)	. 32
Step 1: Add Application Servers to the Load Balancer	. 32
Step 2: Add Service Groups	32
Step 3: Add Virtual Servers	
Step 4: Configure the PatientSecure Identity Server	. 34
Step 5: Configure the PatientSecure Admin Console	
Step 6: Configure the PatientSecure Web Services	. 35
Step 7: Configure the User Interface Server	
Step 8: Configure the Reporting Service	
Step 9: Configure the Emergency Search Service & Palm Vein Auth Service	
Step 10: Configure the PatientSecure System Health Service	
Step 11: Install the HL7 Service on the Application Servers	. 37
Step 12: Configure the FHIR Service	
Step 13: Configure the EMPI Service	
F5 BIG-IP GTM/LTM	
Step 1: Add Application Servers to the Load Balancer	
Step 2: Configure Traffic Groups and Rules	
Step 3: Configure the VIP	
Step 4: Configure the PatientSecure Identity Server	
Step 5: Configure the PatientSecure Web Services	
Step 6: Configure the User Interface Server	
Step 7: Configure the Admin Console	
Step 8: Configure the Reporting Service	
Step 9: Configure the Emergency Search Service & Palm Vein Auth Service	
Step 10: Configure the PatientSecure System Health Service	
Step 11: Install the HL7 Service on the Application Servers	
Step 12: Configure the FHIR Service	
Step 13: Configure the EMPI Service	
Connect Clients to a High Availability Environment	
Update Connection Strings	
Troubleshooting	
Microsoft IIS	. 45

## High Availability Support

This document describes how to configure a sample load balancing configuration and failover support for many of the Imprivata PatientSecure services.

In this configuration, the load balancer server serves two purposes:

- Directing incoming PatientSecure requests to a server farm, which allows Imprivata PatientSecure to handle a greater volume of requests by balancing the load.
- Ensuring higher PatientSecure service uptime with failover clusters.

Imprivata PatientSecure supports high availability configurations using the following technologies:

- Application Request Routing (ARR) on Microsoft's IIS web server
- Citrix ADC (formerly Netscaler) appliance with the ADC management GUI
- F5 BIG-IP GTM/LTM load balancers and their management UI

#### **IMPORTANT:**

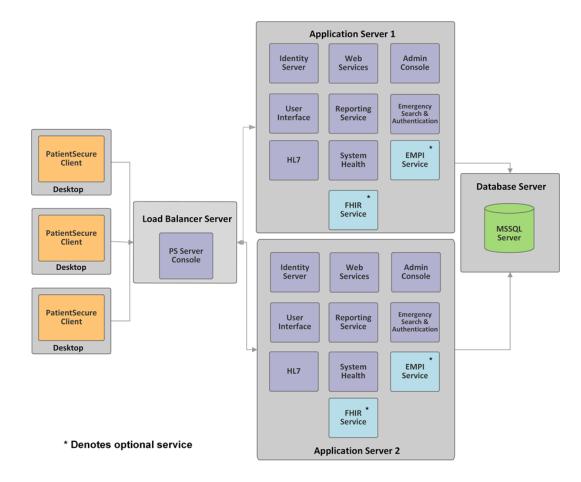
Imprivata has tested the high availability configurations documented in the procedures below. Use them as guidance when configuring high availability, adjusting as necessary to meet your organization's high availability strategies and policies.

For detailed information, see your load balancer vendor's documentation.

## Architecture

(i)

The following diagram represents the Imprivata PatientSecure service components deployed in a loadbalanced configuration, with one Load Balancer server, two application servers and one database server.



## Terminology

In this guide, the following terms are used, especially in the configuration steps and examples:

- Load Balancer server the server runs the PatientSecure Server Console component and one of the supported load balancer technologies:
  - ° Microsoft Internet Information Services (IIS) with Application Request Routing (ARR).
  - ° Citrix ADC (formerly Netscaler) appliance
  - F5 BIG-IP GTM/LTM F5's GTM (global traffic managers) provide load balancing services between two or more sites. F5's LTM (local traffic managers) provide load balancing services between two or more servers/applications in the event of a local system failure.
- **Application Server 1** the server running the PatientSecure service components as the **first** application server in the configuration.
- Application Server 2 the server running the PatientSecure service components as the second application server in the configuration.

## PatientSecure Services Supported for High Availability

Imprivata PatientSecure supports the deployment of the following components in a load-balancing configuration:

- PatientSecure Identity Server
- PatientSecure Web Services
- PatientSecure Reporting Service
- PatientSecure User Interface
- PatientSecure Admin Console
- PatientSecure Emergency Search & Palm Vein Authentication Service
- PatientSecure System Health Service
- PatientSecure HL7 Services (HL7 Listener, HL7 Processor, and HL7 Sender) keep the patient data in your Imprivata PatientSecure database in sync with the data in your EMR application.

The HL7 services are designed for failover support. They are not designed for the load balancing of connections. The HL7 services use TCP/IP protocols for communication.

° HL7 Sender and Processor services.

The services automatically pick an application server to be their active server, and switch to another healthy server when they detect that the current active server has stopped sending messages.

• HL7 Listener service.

The Listener service should only be actively managing traffic on one application server at a time. When the HL7 Listener service fails on Application server 1, you must re-route traffic to Application server 2.

Depending on your environment needs, the optional PatientSecure components can be deployed in a load-balancing configuration:

- PatientSecure EMPI Service. Allows PatientSecure to integrate with EMPIs such as Verato MPI or IBM Initiate.
- PatientSecure FHIR Service.

## Before You Begin

Before you begin, consider the following items:

## **Review System Requirements**

Review the system requirements and required software for the Load Balancer and PatientSecure application servers on the <u>Imprivata Environment Reference</u> portal.

## Gather Server Information

Gather application server information for your PatientSecure environment, including server names, fully qualified domain names (FQDNs) and administrator credentials for the two Application servers.

## **Review Additional References**

We strongly encourage you to review the following documentation on load balancer servers.

#### Microsoft's ARR Documentation

ARR allows for a great deal of customization, and understanding this functionality will help you use it to its full potential.

Download and install the IIS ARR module	https://www.iis.net/downloads/microsoft/application-request-routing
Guide for configuring ARR from Microsoft Learning	https://www.iis.net/learn/extensions/planning-for-arr
Additional Microsoft resources on configuring a web farm	https://technet.microsoft.com/en-us/library/jj129385(v=ws.11).aspx

#### **Citrix ADC Documentation**

https://docs.citrix.com/en-us/citrix-adc/

#### F5 BIG-IP GTM/LTM Documentation

https://my.f5.com/manage/s/tech-documents

## Review the PatientSecure Communication Ports

Review the default PatientSecure communication port values.

#### NOTE:

(**i**)

The values may change based on the ports you use for installation in subsequent steps and the order in which you install various components.

PatientSecure Component	Default Port	Туре
Identity Server	7001	HTTPS
Web Services	7002	HTTPS
User Interface	7003	нттрѕ
Reporting Service	7004	HTTPS

PatientSecure Component	Default Port	Туре
Admin Console	80, 443	Port 443 must be
	(i) NOTE: These ports cannot change.	HTTPS.
Emergency Search & Palm Vein Authentication Service	7005 and 7006	HTTPS
System Health Service	7007	нттрѕ
HL7 Listener Services	2244	TCP/IP
FHIR Service (optional)	7008	нттрѕ
EMPI Service (optional)	7009	HTTPS



#### IMPORTANT:

HTTPS bindings require a valid certificate.

Ensure that the correct certificate is bound to the associated port.

## Installation Sequence

## Step 1: Obtain and Import Certificate Authority to the Load Balancer Server

Obtain the certificate authority used to sign the application servers' certificates and import it to the local machine's trusted root authority on the load balancer server.

Third-party certificates used by the load balancer must have a Subject Alternative Name (SAN).

#### **IMPORTANT:**

(i)

Production PatientSecure environments must use third-party SSL certificates. Self-signed certificates generated by PatientSecure should only be used in test environments.

For more information on importing certificates to your load balancer server, see your load balancer server's platform documentation.

 Citrix ADC: Import the certificate using the Traffic Management > Load Balancing > SSL > Certificates > Client Certificate workflow.

## Step 2: Install Required Software on Load Balancer Server

Install the required software onto the Load Balancer server.

## Microsoft IIS and ARR

- Microsoft IIS configured. Review the Microsoft documentation that corresponds to the version of Windows Server and IIS Manager in your environment.
- Application Request Routing 3.0 module installed.

## Citrix ADC

For system requirements, see your Citrix ADC documentation.

## F5 BIG-IP GTM/LTM Load Balancer

For system requirements, see your F5 BIG-IP GTM/LTM documentation.

## Step 3: Install PatientSecure Server Console on the Load Balancer Server

## (i) NOTE:

Imprivata recommends that the PatientSecure Server Console be installed on the Load Balancer server to keep it separate from the PatientSecure application servers, to ensure service reliability.

To install Imprivata PatientSecure on the Load Balancer server:

- 1. Install the Imprivata PatientSecure Server Console.
  - a. Download the PSI package provided by your Imprivata PatientSecure representative.
  - b. Click PatientSecureServerSetup.exe, and then click Run.

The InstallShield Wizard opens.

- c. Follow the wizard prompts to install the PatientSecure Server Console.
  - i. To set up the environment as a Production environment, select **Production**.
  - ii. To set up the environment as a test or other non-production environment, select **Non-Production**.

This setting is used in coordination with the PatientSecure Site Monitoring (PSSM) component to collect data as either a production or test environment.

- ii. When the installation is complete, you see a success or failure message.
  - The Launch Imprivata PatientSecure Server Console checkbox is selected by default, so you can continue installing Imprivata PatientSecure components when you exit the Installer.
  - To launch the Server Console later, clear the Launch Imprivata PatientSecure Server Console checkbox and make a note of the address provided on the screen.

- To review log entries for the installation when you exit the Installer, select the **Show the Windows Installer log** checkbox.
- iii. Click Finish.



**TIP**: If you selected the **Launch Imprivata PatientSecure Server Console** checkbox and the Server Console does not launch successfully, refresh your browser.

- 2. Click + Set up new installation and follow the instructions on the screen to complete the initial setup of the database and Active Directory.
- 3. On the Installation Type page, select Advanced.

The Server Dashboard opens.

Next, add the two PatientSecure Application servers to the Server Console.

## Step 4: Add the Application Servers to PatientSecure Server Console

To add the two application servers in PatientSecure Server Console:

- 1. On the Server Dashboard page, in the Server Status section, click Add a Server.
  - a. Type the **fully-qualified domain name** (FQDN) for Application Server 1 and click **Next**.
  - b. Enter the Windows administrator credentials for the server, and then click Confirm.
  - c. Complete the certificate workflow. Select an existing one for the application server's hostname in FQDN.
  - d. When you are done, click **Save**.

The server is added to the Server Dashboard.

2. Click the server row for Application Server 1 to open its Server Details page.

a. Click **Download Certificate Authority** to download the certificate to the Load Balance server.

PatientSecure Server Console Dasht	ooard Advanced Settings	;	Logout
Server Info			
Hostname arr-02.example.eng	Username Integrated Security	<b>Operating System</b> Microsoft Windows Server 2012 R2 Datacenter	
Computer Name ARR-02	Version 6.6.000.1		
Delete Server		Reload Detai	ils
SSL Info			
Certificate Thumbprint 411CBDB5756F85E683EF8732C826B1840C8	1075A		
Download Certificate Authority		Edit SSL In	fo
PatientSecureCertApfx ^		Sh	now all

- b. Install and trust the downloaded certificate, selecting **Local Machine** in the Certificate Import Wizard, then clicking **Next** several times to complete the wizard.
- a. Click **Dashboard** at the top of the page to return to the Server Dashboard.
- 3. Repeat Steps 1 through 2 of this procedure for Application Server 2.

The two application servers are added to the Server Status section. The Services column in the table is empty, indicating that there are no PatientSecure services installed yet.

The Server Dashboard should look similar to the following example:

PatientSecure Server	Console Dashb	oard Advanced Settings		Logout
Server Status				
Add a Server				
Hostname	Computer Name	OS	Services	
arr-02.example.eng	ARR-02	Microsoft Windows Server 2012 R2 Datacenter		
arr-03.example.eng	ARR-03	Microsoft Windows Server 2012 R2 Datacenter		

## Configure the Load Balancer Server

The steps for configuring the load balancer server depend on the technology, as each have different interfaces.

Select the load balancer server technology you are configuring:

- Microsoft IIS with ARR
- Citrix ADC (formerly Netscaler)
- F5 BIG-IP GTM/LTM

## Microsoft IIS with ARR



**NOTE:** Screenshots of Microsoft IIS Manager are included as a courtesy to guide you through the configuration. The workflows may differ slightly depending on your operating system version.

## Step 1: Configure IIS

To configure the Load Balancer server with IIS:

1. In IIS Manager, navigate to the **Default Web Site**.

In the Actions page, edit Site Bindings to add port bindings for the services.

The default values are as follows:

PatientSecure Component	Default Port	Туре
Identity Server	7001	HTTPS
Web Services	7002	HTTPS
User Interface	7003	HTTPS
Reporting Service	7004	HTTPS
Admin Console	80, 443	Port 443 must be
	<b>NOTE</b> : These ports cannot change.	HTTPS.
Emergency Search & Palm Vein Authentication Service	7005 and 7006	HTTPS
System Health Service	7007	HTTPS
FHIR Service (optional)	7008	HTTPS
EMPI Service (optional)	7009	HTTPS

The following example illustrates the Default Web Site port bindings configured with default port

values:

Connections 🗟 • 🔚   🖄   象		Defaul	t Web S	ite Home		
Start Page ARR-01 (PS\Administrator)		Filter:	•		w All Group by: Area	- mi -
Application Pools ⊿ Sites				Site	Bindings	r i i i i i i i i i i i i i i i i i i i
🔺 😜 Default Web Site	Туре	Host Name	Port	IP Address	Binding Informa	Add
aspnet_client	http		80	*		
⊿ -∰ Server Farms	https		443	*		Edit
PatientSecure Admin Console	https		7001	*		
Servers	https		7002	*		Remove
A	https		7003	*		Browse
⊳ - 📲 🖥 Servers						
⊿ Borna PatientSecure Web Services ▷ Borna Servers						

## Step 2: Configure the PatientSecure Identity Server

Install the PatientSecure Identity Server component on the two application servers and create a server farm for the Identity Server on the Load Balance server.

Step 2a: Install the PatientSecure Identity Server on the Application Servers

To install the Identity Server component on the application servers:

- 1. Click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure Identity Server section, select the drive and port, and then click **Install PSIS**.



**NOTE:** The port setting must match the value configured for the <u>Load Balancer port</u> above. The default value is 7001.

- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat Steps 1 through 3 of this procedure for Application Server 2.

When you are done, the Server Dashboard should look similar to the following example:

atientSecure Server	Console Dashb	oard Advanced Settings		Logout
Server Status				
Add a Server				
Hostname	Computer Name	os	Services	
arr-02.example.eng	ARR-02	Microsoft Windows Server 2012 R2 Datacenter	PSIS	
arr-03.example.eng	ARR-03	Microsoft Windows Server 2012 R2 Datacenter	PSIS	

#### Step 2b: Configure Advanced Settings

Use the Advanced Settings page to configure the value for PatientSecure Identity Server.

1. Click Advanced Settings at the top of the page.

The Advanced Settings page lists the installed Imprivata PatientSecure components.

 a. Configure the value for PatientSecure Identity Server to match the following format: https://<LoadBalancingServer>:<ConfiguredPort>/identityserver
 For example: https://myLoadBalancer.mydomain.com:7001/identityserver

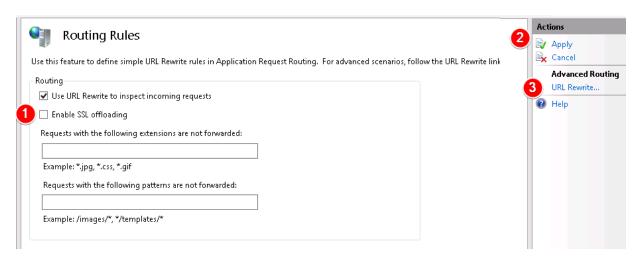
#### Step 2c: Create a Server Farm for the Identity Server

To create a server farm for the Identity Server:

- 1. On the Load Balance server, open IIS Manager and select **Server Farm > Create Server Farm**.
- 2. In the Server farm name box, type PatientSecure Identity Server.
- 3. Make sure that the **Online** checkbox is selected.
- 4. Click **Next** and add both of the application servers to the server farm.

Add Server         Server address:         Image: Constraint of the settings         Server Address         Status         Image: Constraint of the settings         Image: Constraint of the settings         Server Address         Status         Image: Constraint of the settings         Image: Constraint of the settings			Create Server Farm	? ×
Add       ✔ Online       Hide advanced settings       healthCheckAlternat 0       hostName       httpPort       80       httpsPort       7001       weight       100	Add Serve	r		
Add       ✔ Online       Hide advanced settings       healthCheckAlternat 0       hostName       httpPort       80       httpsPort       7001       weight       100				
✓ Online       Hide advanced settings       healthCheckAlternat 0       hostName       httpPort       80       httpSport       7001       weight       100	Server address:			
Hide advanced settings     Remove       healthCheckAlternat 0			Add	
healthCheckAlternat 0       hostName       httpPort       80       httpsPort       7001       weight       100	🖌 Online			
healthCheckAlternat 0       hostName       httpPort       80       httpsPort       7001       weight       100				
hostName httpPort 80 httpsPont 7001 weight 100 Server Address Status	Hide advanced settings	-	Remove	
httpPort     80       httpsPort     7001       weight     100	healthCheckAlt	ernat 0	<u>^</u>	
httpsPont     7001       weight     100				
httpsPont     7001       weight     100	httpPort	80	_	
weight     100       Server Address     Status		7001	=	
Server Address Status		100	_	
			~	
	C 411	<b>C</b> 1		
Previous Next Finish Cancel	Server Address	Status		
Previous Next Finish Cancel				
Previous Next Finish Cancel				
Previous Next Finish Cancel				
Previous Next Finish Cancel				
Previous Next Finish Cancel				
			Previous Next Fi	nish Cancel

- 5. Enter the information for the first server.
- 6. In the Advanced Settings section, configure the HTTPS port value to match the port specified for the Load Balancer and the application servers.
- 7. Click **Add** and repeat the procedure for additional servers.
- 8. Click Finish. A dialog displays with a request to create URL rewrite rules automatically. Click Yes.
- 9. From the Connections list, click the server farm name (PatientSecure Identity Server), and then click **Routing Rules**.



- 10. On the Routing Rules page, clear the **Enable SSL offloading** checkbox, and then click **Apply** in the Actions pane.
- 11. In the Advanced Routing pane, click **URL Rewrite**.

URL Rewrite				Actions	
				Add Rule(s)	
Provides rewriting capabilities based on rules for the requested URI	address and the content of	an HTTP response.		Manage Server Variab	les
Inbound rules that are applied to the requested URL address:				View Server Variables	
Name	Input	Match	Pattern	Manage Providers	
🕒 🗉 🧮 ARR_PatientSecure Identity Server_Ioadbalance_SSL	URL Path	Matches	*	View Rewrite Maps	
🕀 🛅 ARR_PatientSecure Identity Server_Ioadbalance	URL Path	Matches	*	View Providers	
				Conditions	
				Add	
				Inbound Rules	$\diamond$
				Edit	
				Rename	
			<b>Ľ</b>	Discle Rule	
				Disaele Rule	
< 111			>	👚 Move Up	
	1.770			🗣 Move Down	
Outbound rules that are applied to the headers or the content of a	n HTTP response:			Outbound Rules	

12. Select the rewrite rules that do not include SSL, and then click **Remove** in the Inbound Rules pane.

						Actions	
URL Rewrite						Add Rule(s)	
Provides rewriting capabilities bas Inbound rules that are applied to t		JRL address and the content of a	n HTTP response.			Manage Server Variab View Server Variables	les
Name ARR_PatientSecure Identity	/ Server_loadbalance_SSL	Input URL Path {HTTPS}	Match Matches Matches the Pat	ttern	Pattern * on	Manage Providers View Rewrite Maps View Providers Conditions	•
3	Condition input: [SERVER_PORT]	Add Condition	? <b>x</b>		•	Add Inbound Rules Edit Rename X Remove Disable Rule	۲
<ul> <li>Outbound rules that are applie</li> <li>Name</li> </ul>	Check if input string: Matches the Pattern Pattern: 7001 Ignore case		Test pattern Cancel	Stop Proce	> Entry Typ	Move Up Move Down Outbound Rules View Preconditions View Custom Tags P Help	۲

 Select the rewrite rule that includes SSL, and then click Add in the Conditions pane. The Add Condition dialog box opens.

- 14. In the **Condition Input** field, type {SERVER\_PORT}.
- 15. In the **Pattern** field, type the port configured for the **Identity Server**.

#### Step 2d: Configure Failover for Identity Service

To configure failover support within ARR for the Identity Server:

 On the Load Balance server, open IIS Manager, select Server Farms > PatientSecure Identity Server, and then click Health Test.

The URL Test form opens.

- 2. In the URL field, enter the PSIS address entered on the PatientSecure Server Console Advanced Settings.
- 3. In the Acceptable status codes field, enter 200-399.
- 4. In the **Response match** field, enter **IdentityServer4**.



**NOTE**: You can also add custom values for the Interval, which governs how often the test is performed, and the Time-out, which determines how long the health test will wait for a response. On slower configurations, the default settings may return false errors.

- 5. Click Verify URL Test.
- 6. In the **Minimum servers** field, enter 1.
- 7. Click Apply.
- From the Connections list, select Server Farms > PatientSecure Identity Server, and then click Monitoring and Management.
- 9. On the Monitoring and Management page, the entries in the Health Status column should be **Healthy**. There may be a brief delay (set by the Interval time) to update the server statuses.

Monitoring and Management

Use this feature to view the runtime statistics of Application Request Routing. Use Actions to manage the content servers.							
Group by: No Grouping							
Server 🔺	Availability	Health Status	Requests Per Second	Response Time (ms)	Current Requests		
	Available	Healthy	0	42	0		
	Available	Healthy	0	45	0		

## Step 3: Configure PatientSecure Web Services

Step 3a: Install PatientSecure Web Services on the Application Servers

To install PatientSecure Web Services (PSWS) on the application servers:

1. From the PatientSecure Server Dashboard, click the server row for Application Server 1 to open its Server Details page.

2. In the Services - PatientSecure Web Services section, select the drive and port, and then click **Install PSWS**.



**NOTE:** The port setting should match the value configured for the <u>Load Balancer port</u> above. The default value is 7002.

- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat Steps 1 through 3 of this procedure for Application Server 2.

#### Step 3b: Configure Advanced Settings

Use the Advanced Settings page to configure the value for PatientSecure Web Services.

1. Click Advanced Settings at the top of the page.

The Advanced Settings page lists the installed Imprivata PatientSecure components.

a. Configure the value for **PatientSecure Web Services** to match the following format: https://<LoadBalancingServer>:<ConfiguredPort>/psws/api

For example: https://myLoadBalancer.mydomain.com:7002/psws/api

When you are done, the Advanced Settings page should look similar to the example below:

PatientSecure Server Console	Dashboard	Advanced Settings	
Advanced Settings			
Any changes to these settings may requir	e reinstalling	services to propagate.	
PatientSecure Server Console	https:/	/arr-01.example.eng:7000	
PatientSecure Database	DataSo	urce=db.example.eng\PS;Initial Catalog=	
PatientSecure Identity Server	https://a	arr-01.example.eng:7001/identityserver	
PatientSecure Web Services	https://	arr-01.example.eng:7002/psws/api	
PatientSecure User Interface			
PatientSecure FHIR Service			
Edit settings			

#### Step 3c: Create a Server Farm for the PatientSecure Web Service

To create a server farm for the Web Service:

- 1. On the Load Balance server, open IIS Manager and select Server Farms > Create Server Farm.
- 2. In the **Server farm name** field, type PatientSecure Web Services.
- 3. Make sure that the **Online** checkbox is selected.
- 4. Click **Next** and add both of the application servers to the server farm.

		Add Server	L	? X
Server address:				
server auuress:				
			Add	
Online		_		
 Hide advanced set	tinas			
			Remove	
healthChe	eckAlternat 0	^		
hostName	e			
httpPort	80			
httpsPort	7002	=		
weight	100	~		
		·		
Server Address	Status			
Server Address	Status			
Server Address	Status			
Server Address	Status			
Server Address	Status			
Server Address	Status			
Server Address	Status			
Server Address	Status			
Server Address	Status			
Server Address	Status			
Server Address	Status			
Server Address	Status			
Server Address	Status			

- 5. Enter the information for Application Server 1.
- 6. In the Advanced Settings section, configure the HTTPS port value to match the port specified for the Load Balancer and the application servers.
- 7. Click **Add** and repeat the procedure for additional servers.
- 8. Click Finish. A dialog displays with a request to create URL rewrite rules automatically. Click Yes.
- 9. From the Connections list, click the server farm name (PatientSecure Web Services), and then click **Routing Rules**.
- 10. On the Routing Rules page, clear the **Enable SSL offloading** checkbox, and then click **Apply** in the Actions pane.
- 11. In the Advanced Routing pane, click **URL Rewrite**.

ų	💷 URL Rewrite				Actions	
	one norme				Add Rule(s)	
	Provides rewriting capabilities based on rules for the requested UR	L address and the content of	an HTTP response.		Manage Server Varial	bles
	Inbound rules that are applied to the requested URL address:				View Server Variables	-
	Name	Input	Match	Pattern	Manage Providers	
	ARR_PatientSecure Identity Server_Ioadbalance_SSL	URL Path	Matches	*	View Rewrite Maps	
4	🗉 🧮 ARR_Patient Secure Web Server_loadbalance_SSL	URL Path	Matches	*	View Providers	
C	🗷 🛅 ARR_Patient Secure Web Server_Ioadbalance	URL Path	Matches	*	Conditions	۲
Ĩ					Add	
					Inbound Rules	۲
					Edit	
					Rename	
					ZX Remove	
					Disable Rule	
	<			>	1 Move Up	
					Move Down	
	Outbound rules that are applied to the headers or the content of a	n HTTP response:			Outbound Rules	۲

12. Select the rewrite rules that do not include SSL, and then click **Remove** in the Inbound Rules pane.

	unit n				Actions	
🜗 URL Rev	vitte				Add Rule(s)	
rovides rewriting cap nbound rules that are	Manage Server Variable View Server Variables					
Name B CARR PatientSe	cure Identity Server_loadbalance_SSL	Input URL Path	Match Matches	Pattern	Manage Providers View Rewrite Maps	
	ecure Web Server_loadbalance_SSL	URL Path	Matches	*	View Providers	
		{HTTPS}	Matches the Pattern	on	Conditions	(
					2 Add	
	Add Condition	? X			Inbound Rules	
<b>3</b> {si	ondition input: ERVER_PORT} neck if input string:			>	Edit Rename X Remove Disable Rule	
utbound rule	atches the Pattern 🗸 🗸			7	<ul> <li>Move Up</li> <li>Move Down</li> </ul>	
Jame A	ttern: σz	Test pattern	Action Value Stop P	roce Entry Typ	Outbound Rules View Preconditions View Custom Tags	(
	Ignore case	Cancel			😧 Help	

- Select the rewrite rule that includes SSL, and then click Add in the Conditions pane. The Add Condition dialog box opens.
- 14. In the **Condition Input** field, type {SERVER\_PORT}.
- 15. In the **Pattern** field, enter the port configured for Web Services.
- 16. Return to the Connections list, click the server farm name (PatientSecure Web Services), and then click **Server Affinity**.
- 17. Select the **Client Affinity** checkbox, and then click **Apply**.

Step 3d: Configure Failover for Web Services

To configure failover support within ARR for Web Services:

1. On the Load Balance server, open IIS Manager, select **Server Farms > PatientSecure Web Services**, and then click **Health Test**.

The URL Test form opens.

2. In the URL field, enter the following URL:

https://<LoadBalanceServer>:<PSWS port>/psws/api/public/status

- 3. In the **Acceptable status codes** field, enter 200-302.
- 4. Click Verify URL Test.
- 5. In the **Minimum servers** field, enter 1 and click **Apply.**
- From the Connections list, select Server Farms > PatientSecure Web Services, and then click Monitoring and Management.
- 7. On the Monitoring and Management page, the entries in the Health Status column should be **Healthy**. There may be a brief delay (set by the Interval time) to update the server statuses.

## Step 4: Configure the User Interface Server

Install the User Interface Server component on the two application servers and create a server farm for the User Interface Server on the Load Balance server.

Step 4a: Install the PatientSecure User Interface Server on the Application Servers

To install the User Interface Server component on the application servers:

- 1. Click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure User Interface section, select the drive and port, and then click **Install CLIENT**.



**NOTE:** The port setting should match the value configured for the <u>Load Balancer port</u> above. The default value is 7003.

- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat Steps 1 through 3 of this procedure for Application Server 2.

#### Step 4b: Configure Advanced Settings

Use the Advanced Settings page to configure the value for PatientSecure User Interface.

1. Click Advanced Settings at the top of the page.

The Advanced Settings page lists the installed Imprivata PatientSecure components.

 Configure the value for PatientSecure User Interface Server to match the following format: https://<LoadBalancingServer>:<ConfiguredPort>
 For example: https://myLoadBalancer.mydomain.com:7003

#### Step 4c: Create a Server Farm for the User Interface Server

To create a server farm for the User Interface Server:

- 1. On the Load Balance server, open IIS Manager and select **Server Farm > Create Server Farm**.
- 2. In the **Server farm name** field, type PatientSecure User Interface Server.

- 3. Make sure that the **Online** checkbox is selected.
- 4. Click **Next** and add both of the application servers to the server farm.
- 5. Enter the information for the first server.
- 6. In the Advanced Settings section, configure the HTTPS port value to match the port specified for the Load Balancer and the application servers.
- 7. Click **Add** and repeat the procedure for additional servers.
- 8. Click **Finish**. A dialog displays with a request to create URL rewrite rules automatically. Click **Yes**.
- 9. From the Connections list, click the server farm name (PatientSecure User Interface Server), and then click **Routing Rules**.

Conting Rules	Actions
	🛃 🗟 Apply
Use this feature to define simple URL Rewrite rules in Application Request Routing. For advanced scenarios, follow the URL Rewrite link	🖹 Cancel
Routing	Advanced Routing
✓ Use URL Rewrite to inspect incoming requests	3 URL Rewrite
1  Enable SSL offloading	😢 Help
Requests with the following extensions are not forwarded:	
Example: *.jpg, *.css, *.gif	
Requests with the following patterns are not forwarded:	
Example: /images/*, */templates/*	

- 10. On the Routing Rules page, clear the **Enable SSL offloading** checkbox, and then click **Apply** in the Actions pane.
- 11. In the Advanced Routing pane, click **URL Rewrite**.
- 12. Select the rewrite rules that do not include SSL, and then click **Remove** in the Inbound Rules pane.
- Select the rewrite rule that includes SSL, and then click Add in the Conditions pane. The Add Condition dialog box opens.
- 14. In the **Condition Input** field, type {SERVER\_PORT}.
- 15. In the **Pattern** field, enter the port configured for the User Interface Server.
- 16. Return to the Connections list, click the server farm name (PatientSecure Admin Console), and then click **Server Affinity**.
- 17. Select the **Client Affinity** checkbox, and then click **Apply**.

#### Step 4d: Configure Failover of the User Interface Server

To configure failover support within ARR for the User Interface Server:

 On the Load Balance server, open IIS Manager, select Server Farms > PatientSecure User Interface Server, and then click Health Test.

The URL Test form opens.

- 2. In the URL field, enter the address entered on the PatientSecure Server Console Advanced Settings.
- 3. In the Acceptable status codes field, enter 200-399.
- 4. In the **Response match** field, enter **UserInterface3**.



**NOTE**: You can also add custom values for the Interval, which governs how often the test is performed, and the Time-out, which determines how long the health test will wait for a response. On slower configurations, the default settings may return false errors.

- 5. Click Verify URL Test.
- 6. In the Minimum servers field, enter 1.
- 7. Click **Apply**.
- 8. From the Connections list, select Server Farms > PatientSecure User Interface Server, and then click Monitoring and Management.
- 9. On the Monitoring and Management page, the entries in the Health Status column should be **Healthy**. There may be a brief delay (set by the Interval time) to update the server statuses.

### Step 5: Configure the Admin Console

#### Step 5a: Install the Admin Console on the Application Servers

To install the Admin Console on the application servers:

- 1. From the PatientSecure Server Dashboard, click the server row for the first application server to open its Server Details page.
- 2. In the Services PatientSecure Admin Console section, select the drive, and then click **Install ADMIN**. The Admin Console installs on port 80 and port 443 (if SSL is used).
- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat this procedure for all application servers.

#### Step 5b: Create a Server Farm for the Admin Console

To create a server farm for Admin Console:

- 1. On the Load Balance server, open IIS Manager and select **Server Farms > Create Server Farm**.
- 2. In the **Server farm name** field, type PatientSecure Admin Console.
- 3. Make sure that the **Online** checkbox is selected.
- 4. Click **Next** and add both of the application servers to the server farm.
- 5. Enter the information for the first server.



**NOTE**: Do not configure advanced settings for the port on either application server.

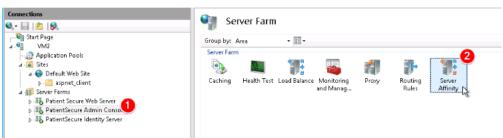
- 6. Click **Add** and repeat the procedure for additional servers.
- 7. Click **Finish**. A dialog displays with a request to create URL rewrite rules automatically.
- 8. Click Yes.
- 9. From the Connections list, click the server farm name (PatientSecure Admin Console) and then click **Routing Rules**.
- 10. On the Routing Rules page, clear the **Enable SSL offloading** checkbox, and then click **Apply** in the Actions pane.
- 11. In the Advanced Routing pane on the left, click **URL Rewrite**.

				Actions	
URL Rewrite				Add Rule(s)	
Provides rewriting capabilities based on rules for the requeste	ed URL address and the content of an H	HTTP response.		Manage Server Varial	bles
Inbound rules that are applied to the requested URL address:				View Server Variables	
Name	Input	Match	Pattern	Manage Providers	
🐵 🧰 ARR_PatientSecure Identity Server_Ioadbalance_SSL	URL Path	Matches	*	View Rewrite Maps	
🗉 🚞 ARR_Patient Secure Web Server_Ioadbalance_SSL	URL Path	Matches	*	View Providers	
💻 🚞 ARR_PatientSecure Admin Console_Ioadbalance_SSL	URL Path	Matches	*	Conditions	$\frown$
🚺 🗃 ARR_PatientSecure Admin Console_Ioadbalance 👘	URL Path	Matches	*	2 Add	
				Inbound Rules	
Add Co	ndition ?	x		Edit	
				Rename	
Condition input:				X Remove	
{SERVER_PORT}				Disable Rule	
<			>	1 Move Up	
Check if input string:				Move Down	
Outbound rul Matches the Pattern	~			Outbound Rules	
Name		Action Value	Stop Proce Entry Typ	View Preconditions	
Pattern:				View Custom Tags	
9 80 T	Test pattern				-
				🔞 Help	
✓ Ignore case					
	-				
(	5 OK Cancel				

- Select the rewrite rule that does not include SSL, and then click Add in the Conditions pane.
   The Add Condition dialog box opens.
- 13. In the **Condition Input** field, type {SERVER\_PORT}.
- 14. In the **Pattern** field, enter 80.

				Actions	
URL Rewrite				Add Rule(s)	
rovides rewriting capabilities based on rules for the requested UR	address and the content of an h	TTP response.		Manage Server Varia	bles
nbound rules that are applied to the requested URL address:				View Server Variables.	
Name	Input	Match	Pattern	Manage Providers	
E ARR_PatientSecure Identity Server_Ioadbalance_SSL	URL Path	Matches		View Rewrite Maps	
ARR_Patient Secure Web Server_Ioadbalance_SSL	URL Path	Matches	•	View Providers	
ARR_PatientSecure Admin Console_loadbalance_SSL	URL Path	Matches	*	Conditions	. 6
	{HTTPS}	Matches the Pattern	on	Add	
ARR_PatientSecure Admin Console_Ioadbalance	URL Path	Matches	•	Inbound Rules	(
	{SERVER_PORT}	Matches the Pattern	80	Edit	
Add	Condition	? X		Bename	
	a offar troff			× Remove	
Condition input:				Disable Rule	
< 3 (SERVER_PORT)			>		-
				<ul> <li>Move Up</li> <li>Move Down</li> </ul>	
Dutbound rules that an Check if input string:					
Name Matches the Pattern	*	n Value Stop	Proce Entry Typ	Outbound Rules	٢
		in ordine prop	recent chay typ	View Preconditions	
Pattern:				View Custom Tags	
413 Pattern:	Tester			🔞 Help	
443	Testp	attern			
✓ Ignore case					
Ignore case					
	6				
	ок	Cancel			

- Select the rewrite rule that includes SSL, and then click Add in the Conditions pane. The Add Condition dialog box opens.
- 16. In the **Condition Input** field, type {SERVER\_PORT}.
- 17. In the Pattern field, enter 443 and click OK.



18. Return to the Connections list, click the server farm name (PatientSecure Admin Console), and then click **Server Affinity**.



19. Select the **Client Affinity** checkbox, and then click **Apply**.

Step 5c: Configure Failover for the Admin Console.

To configure failover support within ARR for Admin Console:

- On the Load Balance server, open IIS Manager, select Server Farms > PatientSecure Admin Console, and then click Health Test.
   The URL Test form opens.
- 2. In the URL field, enter the following URL: https://<LoadBalanceServer>/AdminConsole
- 3. In the Acceptable status codes field, enter 200-399.
- 4. Click Verify URL Test.
- 5. In the **Minimum servers** field, enter 1 and click **Apply**.
- From the Connections list, select Server Farms > PatientSecure Admin Console, and then click Monitoring and Management.
- 7. On the Monitoring and Management page, the entries in the Health Status column should be **Healthy**. There may be a brief delay (set by the Interval time) to update the server statuses.

## Step 6: Configure the Reporting Service

The Reporting Service component is required for the Admin Console to display the dashboard and to run reports.

#### Step 6a: Install the Reporting Service on the Application Servers

To install the Reporting Service on the application servers:

- 1. From the PatientSecure Server Dashboard, click the server row for Application Server 1 to open its Server Details page.
- In the Services PatientSecure Reporting Service section, select the drive, and then click Install Reporting. The Reporting Service port defaults to 7004.
- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat this procedure for Application Server 2.

#### Step 6b: Configure Advanced Settings

Use the Advanced Settings page to configure the value for PatientSecure Reporting Service.

1. Click Advanced Settings at the top of the page.

The Advanced Settings page lists the installed Imprivata PatientSecure components.

 Configure the value for PatientSecure Reporting Service to match the following format: https://<LoadBalancingServer>:<ConfiguredPort>/api
 For example: https://myLoadBalancer.mydomain.com:7004/api

#### *Step 6c: Create a Server Farm for the Reporting Service*

To create a server farm for the Reporting Service:

- 1. On the Load Balance server, open IIS Manager and select Server Farm > Create Server Farm.
- 2. In the **Server farm name** field, type PatientSecure Reporting Service.
- 3. Make sure that the **Online** checkbox is selected.
- 4. Click **Next** and add both of the application servers to the server farm.
  - a. Enter the information for the first server.
  - b. In the Advanced Settings section, configure the HTTPS port value to match the port specified for the Load Balancer and the application servers.
  - c. Click **Add** and repeat the procedure for additional servers.
- 5. Click **Finish**. A dialog displays with a request to create URL rewrite rules automatically. Click **Yes**.
- 6. From the Connections list, click the server farm name (PatientSecure Reporting Service), and then click **Routing Rules**.
- 7. On the Routing Rules page, clear the **Enable SSL offloading** checkbox, and then click **Apply** in the Actions pane.
- 8. In the Advanced Routing pane, click **URL Rewrite**.
- 9. Select the rewrite rules that do not include SSL, and then click **Remove** in the Inbound Rules pane.
- Select the rewrite rule that includes SSL, and then click Add in the Conditions pane. The Add Condition dialog box opens.
- 11. In the **Condition Input** field, type {SERVER\_PORT}.
- 12. In the **Pattern** field, enter the port configured for the **Reporting Service**.

## Step 7: Configure the PatientSecure Emergency Search & Authentication Service Server

## Step 7a: Install the Emergency Search & Authentication Service on the Application Servers

To install the Emergency Search & Authentication Service on the application servers:

- 1. From the PatientSecure Server Dashboard, click the server row for Application Server 1 to open its Server Details page.
- In the Services PatientSecure Emergency Search Service section, select the drive, and then click Install Emergency Search. The Emergency Search Service ports defaults to 7005 and 7006.
- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat this procedure for Application Server 2.

#### Step 7b: Configure Advanced Settings

Use the Advanced Settings page to configure the value for PatientSecure Emergency Search Service.

1. Click Advanced Settings at the top of the page.

The Advanced Settings page lists the installed Imprivata PatientSecure components.

 Configure the value for PatientSecure Emergency Search Service to match the following format: https://<LoadBalancingServer>:<ConfiguredPort>/api
 For example: https://myLoadBalancer.mydomain.com:7005/api

#### Step 7c: Create a Server Farm for the Emergency Search & Palm Vein Authentication Service

To create a server farm for the Emergency Search & Palm Vein Authentication Service:

- 1. On the Load Balance server, open IIS Manager and select **Server Farm > Create Server Farm**.
- 2. In the **Server farm name** field, type PatientSecure Emergency Search Service.
- 3. Make sure that the **Online** checkbox is selected.
- 4. Click **Next** and add both of the application servers to the server farm.
  - a. Enter the information for the first server.
  - b. In the Advanced Settings section, configure the HTTPS port value to match the port specified for the Load Balancer and the application servers.
  - c. Click Add and repeat the procedure for additional servers.
- 5. Click Finish. A dialog displays with a request to create URL rewrite rules automatically. Click Yes.
- 6. From the Connections list, click the server farm name (PatientSecure Emergency Search Service), and then click **Routing Rules**.
- 7. On the Routing Rules page, clear the **Enable SSL offloading** checkbox, and then click **Apply** in the Actions pane.
- 8. In the Advanced Routing pane, click **URL Rewrite**.
- 9. Select the rewrite rules that do not include SSL, and then click **Remove** in the Inbound Rules pane.
- Select the rewrite rule that includes SSL, and then click Add in the Conditions pane. The Add Condition dialog box opens.
- 11. In the **Condition Input** field, type {SERVER\_PORT}.
- 12. In the **Pattern** field, enter the port configured for the **Emergency Search Service**.
- 13. Return to the Connections list, click the server farm name (PatientSecure Emergency Search Service), and then click **Server Affinity**.
- 14. Select the **Client Affinity** checkbox, and then click **Apply**.

## Step 8: Configure the PatientSecure System Health Service

The PatientSecure System Health Service monitors the status of the PatientSecure database and application servers, and powers the system health dashboard in the PatientSecure Admin Console.

#### Step 8a: Install the System Health Service on the Application Servers

To install the System Health Service on the application servers:

- 1. From the PatientSecure Server Dashboard, click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure System Health Service section, select the drive, and then click **Install System Health Service**. The service port defaults to 7007.
- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat this procedure for Application Server 2.

#### Step 8b: Configure Advanced Settings

Use the Advanced Settings page to configure the value for PatientSecure System Health Service.

1. Click **Advanced Settings** at the top of the page.

The Advanced Settings page lists the installed Imprivata PatientSecure components.

 Configure the value for PatientSecure System Health Service to match the following format: https://<LoadBalancingServer>:<ConfiguredPort>/api
 For example: https://myLoadBalancer.mydomain.com:7007/api

#### Step 8c: Create a Server Farm for the System Health Service

To create a server farm for the System Health Service:

- 1. On the Load Balance server, open IIS Manager and select **Server Farm > Create Server Farm**.
- 2. In the **Server farm name** field, type PatientSecure System Health Service.
- 3. Make sure that the **Online** checkbox is selected.
- 4. Click **Next** and add both of the application servers to the server farm.
  - a. Enter the information for the first server.
  - b. In the Advanced Settings section, configure the HTTPS port value to match the port specified for the Load Balancer and the application servers.
  - c. Click **Add** and repeat the procedure for additional servers.
- 5. Click Finish. A dialog displays with a request to create URL rewrite rules automatically. Click Yes.
- 6. From the Connections list, click the server farm name (PatientSecure System Health Service), and then click **Routing Rules**.
- 7. On the Routing Rules page, clear the **Enable SSL offloading** checkbox, and then click **Apply** in the Actions pane.
- 8. In the Advanced Routing pane, click **URL Rewrite**.
- 9. Select the rewrite rules that do not include SSL, and then click **Remove** in the Inbound Rules pane.
- Select the rewrite rule that includes SSL, and then click Add in the Conditions pane. The Add Condition dialog box opens.
- 11. In the **Condition Input** field, type {SERVER\_PORT}.
- 12. In the **Pattern** field, enter the port configured for the **System Health Service**.

## Step 9: Install the HL7 Service on the Application Servers

To install the HL7 Service on the application servers:

- 1. From the PatientSecure Server Dashboard, click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure HL7 Service section, select the drive, and then click Install HL7.
- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat this procedure for Application Server 2.

HL7 Sender and Processor services automatically pick an application server to be their active server, and switch to another healthy server when they detect that the current active server has stopped sending messages.

The Listener service should only be actively managing traffic on one application server at a time. When the HL7 Listener service fails on Application server 1, you must re-route traffic to Application server 2. You may need to manually point the HL7 engine to Application server 2, or set up a VIP.

## Step 10: Configure the FHIR Service

#### NOTE:

i

Configuring this service is optional, and depends on whether your PatientSecure environment will integrate with the FHIR service.

#### Step 10a: Install the FHIR Service on the Application Servers

To install the FHIR Service on the application servers:

- 1. From the PatientSecure Server Dashboard, click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure FHIR Service section, select the drive and specify the port, and then click **Install FHIR**.
- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat this procedure for Application Server 2.

#### Step 10b: Add Third-Party Certificate to Application Servers

Obtain the third-party SSL certificate and import it to both of the Application Servers hosting the PatientSecure FHIR service.

For more information, see your Windows documentation.

#### Step 10c: Configure Advanced Settings

Use the Advanced Settings page to configure the value for PatientSecure FHIR Service.

1. Click **Advanced Settings** at the top of the page.

The Advanced Settings page lists the installed Imprivata PatientSecure components.

 Configure the value for PatientSecure FHIR Server to match the following format: https://<LoadBalancingServer>:<ConfiguredPort>/api
 For example: https://myLoadBalancer.mydomain.com:7005/api

#### Step 10d: Create a Server Farm for the FHIR Service

- 1. On the Load Balance server, open IIS Manager and select **Server Farm > Create Server Farm**.
- 2. In the **Server farm name** field, type PatientSecure FHIR Service.
- 3. Make sure that the **Online** checkbox is selected.
- 4. Click **Next** and add both of the application servers to the server farm.
  - a. Enter the information for the first server.
  - b. In the Advanced Settings section, configure the HTTPS port value to match the port specified for the Load Balancer and the application servers.
  - c. Click **Add** and repeat the procedure for additional servers.
- 5. Click Finish. A dialog displays with a request to create URL rewrite rules automatically. Click Yes.
- 6. From the Connections list, click the server farm name (PatientSecure FHIR Service), and then click **Routing Rules**.
- 7. On the Routing Rules page, clear the **Enable SSL offloading** checkbox, and then click **Apply** in the Actions pane.
- 8. In the Advanced Routing pane, click **URL Rewrite**.
- 9. Select the rewrite rules that do not include SSL, and then click **Remove** in the Inbound Rules pane.
- 10. Select the rewrite rule that includes SSL, and then click **Add** in the Conditions pane. The Add Condition dialog box opens.
- 11. In the **Condition Input** field, type {SERVER\_PORT}.
- 12. In the **Pattern** field, enter the port configured for the **FHIR Service**.

## Step 11: Configure the EMPI Service

#### NOTE:

Configuring this service is optional, and depends on whether your PatientSecure environment will integrate with an EMPI such as Verato MPI or Initiate.

#### Step 11a: Install the EMPI Service on the Application Servers

To install the EMPI Service on the application servers:

- 1. From the PatientSecure Server Dashboard, click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure EMPI Service section, select the drive and specify the port, and then click **Install EMPI**.
- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat this procedure for Application Server 2.

#### Step 11b: Add Third-Party Certificate to Application Servers

Obtain the third-party SSL certificate and import it to both of the Application Servers hosting the PatientSecure EMPI service.

For more information, see your Windows documentation.

#### Step 11c: Configure Advanced Settings

Use the Advanced Settings page to configure the value for PatientSecure EMPI Service.

1. Click **Advanced Settings** at the top of the page.

The Advanced Settings page lists the installed Imprivata PatientSecure components.

 Configure the value for PatientSecure EMPI Server to match the following format: https://<LoadBalancingServer>:<ConfiguredPort>/api
 For example: https://myLoadBalancer.mydomain.com:7006/api

#### Step 11d: Create a Server Farm for the EMPI Service

- 1. On the Load Balance server, open IIS Manager and select **Server Farm > Create Server Farm**.
- 2. In the **Server farm name** field, type PatientSecure EMPI Service.
- 3. Make sure that the **Online** checkbox is selected.
- 4. Click **Next** and add both of the application servers to the server farm.
  - a. Enter the information for the first server.
  - b. In the Advanced Settings section, configure the HTTPS port value to match the port specified for the Load Balancer and the application servers.
  - c. Click Add and repeat the procedure for additional servers.
- 5. Click **Finish**. A dialog displays with a request to create URL rewrite rules automatically. Click **Yes**.
- 6. From the Connections list, click the server farm name (PatientSecure EMPI Service), and then click **Routing Rules**.
- 7. On the Routing Rules page, clear the **Enable SSL offloading** checkbox, and then click **Apply** in the Actions pane.
- 8. In the Advanced Routing pane, click **URL Rewrite**.
- 9. Select the rewrite rules that do not include SSL, and then click **Remove** in the Inbound Rules pane.
- Select the rewrite rule that includes SSL, and then click Add in the Conditions pane. The Add Condition dialog box opens.

- 11. In the **Condition Input** field, type {SERVER\_PORT}.
- 12. In the **Pattern** field, enter the port configured for the **EMPI Service**.

## Citrix ADC (formerly Netscaler)

#### NOTE:

Screenshots of the ADC (NetScaler) management interface are included as a courtesy to guide you through the configuration.

For more details, see your Citrix ADC documentation.

## Step 1: Add Application Servers to the Load Balancer

In the Citrix ADC management interface, add all of the PatientSecure Application Servers to the load balancer.

To add the Application servers:

- 1. In **Traffic Management > Load Balancing > Servers**, click **Add**. The Create Server page opens.
- 2. Enter the server name.
- 3. Select **Domain Name**.
- 4. Enter the full qualified domain name (FQDN) of the Application Server 1 and click **Create**.
- Repeat steps 1 through 4 of this procedure for Application Server 2. The Servers page displays the Application servers.

## Step 2: Add Service Groups

In the Citrix ADC management interface, create a service group for each PatientSecure component and bind it to the appropriate communication port.

To create a service group:

- 1. In Traffic Management > Load Balancing > Service Groups, click Add.
- 2. In Basic Settings, enter a name appropriate for the service group.

#### For example: PatientSecure Identity Service Group.

- 3. Select SSL from the Protocol list and click OK.
- 4. In the Service Group Members section, add servers:
  - a. Select Server Based.
  - b. In the Select Server box, click the arrow to select the two application servers (Application Server 1 and Application Server 2).
  - c. Enter **7001** in the **Port** box.
  - d. Click Create.

- 5. Repeat steps 2 through 4 in this procedure to add a Service Group for **PatientSecure Web Service** using port **7002** with the same two application servers.
- 6. Add a Service Group for **PatientSecure Admin Console** using port **443** with the same two application servers.
- 7. Add a Service Group for **PatientSecure User Interface** using port **7003** with the same two application servers.
- 8. Add a Service Group for **PatientSecure Reporting Service** using port **7004** with the same two application servers.
- 9. Add a Service Group for **PatientSecure Emergency Search** service using port **7005** with the same two application servers.
- 10. *Optional.* Add a Service Group for **PatientSecure FHIR Service** using port **7007** with the same two application servers.
- 11. *Optional.* Add a Service Group for **PatientSecure EMPI Service** using port **7008** with the same two application servers.

d	Edit Delete Manage Memb	ers Statisti	cs Rename	No action	$\sim$			
lick here	to search or you can enter Key : Value forr	nat						
	Service Group Name	State	Effective State	Protocol	Max Clients	Max Requests	Maximum Bandwidth (Kbps)	Monitor Threshold
	PtSec Identity Service Group	ENABLED	DOWN	SSL	0	0	0	C
	PtSec Web Service Group	ENABLED	DOWN	SSL	0	0	0	c
	PtSec User Interface Service Group	ENABLED	DOWN	SSL	0	0	0	C
	PtSec Reporting Service Group	ENABLED	DOWN	SSL	0	0	0	C
	PtSec FHIR Service Group	ENABLED	DOWN	SSL	0	0	0	C
	PtSec Verato Service Group	ENABLED	DOWN	SSL	0	0	0	C
	PtSec Admin Console	ENABLED	OOWN	SSL	0	0	0	C

## Step 3: Add Virtual Servers

In the Citrix ADC management interface, create the load balancing virtual servers for each PatientSecure component and configure the server certificate bindings.

To add virtual servers:

- 1. In Traffic Management > Load Balancing > Virtual Servers, click Add.
- 2. In the Basic Settings section, enter a name for the virtual server.

For example, PatientSecure Identity Server.

- a. Select SSL from the Protocol list.
- b. Select IP Address from the IP Address Type list.
- c. Enter the IP address for the VIP in the IP Address box.
- d. Enter **7001** in the **Port** box.
- 3. In the Services and Service Groups section, click Load Balancing Virtual Service Group Binding.

- a. Select the PatientSecure Identity Service group from the Select Service Group Name list.
- b. Click Bind.
- c. Click Server Certificate.
- d. Select the server certificate from the list and click **Bind**.
- 4. To set the persistence, in Advanced Settings, click Persistence.
  - a. a. Select SOURCEIP.
  - b. b. Enter **10** in the **Time-out** box, and click **OK**.
- 5. Repeat steps 2 through 4 in this procedure to add a virtual server for the **PatientSecure Web Service**, using port **7002**, and to bind the certificate.
- 6. Add a virtual server for the PatientSecure Admin Console, using port 443, and to bind the certificate.
- 7. Add a virtual server for the PatientSecure User Interface using port 7003, and to bind the certificate.
- 8. Add a virtual server for the PatientSecure Reporting Service using port 7004, and to bind the certificate.
- 9. 9. Add a virtual server for the PatientSecure Emergency Search service using port 7005. and to bind the certificate.
- 10. Add a virtual server for the PatientSecure Palm Vein Auth service using port 7006, and to bind the certificate.
- 11. *Optional.* Add a virtual server for the PatientSecure FHIR service using port 7007, and to bind the certificate.
- 12. *Optional.* Add a virtual server for the PatientSecure EMPI service using port 7008, and to bind the certificate.

## Step 4: Configure the PatientSecure Identity Server

Using the PatientSecure Server Console interface, install the PatientSecure Identity Server component on the two application servers and configure the URL for the VIP.

To install the Identity Server component on the application servers:

- 1. Click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure Identity Server section, select the drive and port, and then click **Install PSIS**.



NOTE: The default port value is 7001.

- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat Steps 1 through 3 of this procedure for Application Server 2.
- 5. Click Advanced Settings. The Advanced Settings page lists the installed PatientSecure components.

 Configure the value for PatientSecure Identity Server to match the following format: https://<LoadBalancingServer>:<ConfiguredPort>/identityserver
 For example: https://myLoadBalancer.mydomain.com:7001/identityserver

## Step 5: Configure the PatientSecure Admin Console

- 1. From the PatientSecure Server Dashboard, click the server row for the first application server to open its Server Details page.
- 2. In the Services PatientSecure Admin Console section, select the drive, and then click **Install ADMIN**. The Admin Console installs on port 80 and port 443 (if SSL is used).
- 3. Enter the Windows administrator credentials for the server, and then click Confirm.
- 4. Repeat this procedure for all application servers.

## Step 6: Configure the PatientSecure Web Services

To install PatientSecure Web Services (PSWS) on the application servers:

- 1. From the PatientSecure Dashboard, click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure Web Services section, select the drive and port, and then click **Install PSWS**.



**NOTE:** The port setting should match the value configured for the Load Balancer port above. The default value is 7002.

- 3. Enter the Windows administrator credentials for the server, and then click Confirm.
- 4. Repeat Steps 1 through 3 of this procedure for Application Server 2.
- 5. Click Advanced Settings. The Advanced Settings page lists the installed PatientSecure components.
- Configure the value for PatientSecure Web Services to match the following format: https://<LoadBalancingServer>:<ConfiguredPort>/psws/api
   For example: https://myLoadBalancer.mydomain.com:7002/psws/api

## Step 7: Configure the User Interface Server

To install the User Interface Server component on the application servers:

- 1. Click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure User Interface section, select the drive and port, and then click **Install CLIENT**.



**NOTE**: The default port value is 7003.

- 3. Enter the Windows administrator credentials for the server, and then click Confirm.
- 4. Repeat Steps 1 through 3 of this procedure for Application Server 2.
- 5. Use the Advanced Settings page to configure the value for PatientSecure User Interface.
- 6. Click Advanced Settings. The Advanced Settings page lists the installed PatientSecure components.
- 7. Configure the value for PatientSecure User Interface Server to match the following format: https://<LoadBalancingServer>:<ConfiguredPort>

For example: https://myLoadBalancer.mydomain.com:7003

#### BEST PRACTICE:

Imprivata recommends that you configure a health monitor in Citrix ADC for the PatientSecure User Interface. This will assist in determining the health of the application servers and fail over appropriately.

## Step 8: Configure the Reporting Service

The Reporting Service component is required for the Admin Console to display the dashboard and to run reports.

To install the Reporting Service on the application servers:

- 1. From the PatientSecure Server Dashboard, click the server row for Application Server 1 to open its Server Details page.
- In the Services PatientSecure Reporting Service section, select the drive, and then click Install Reporting.

The Reporting Service port defaults to 7004.

- 3. Enter the Windows administrator credentials for the server, and then click Confirm.
- 4. Repeat this procedure for Application Server 2.
- 5. Click Advanced Settings. The Advanced Settings page lists the installed PatientSecure components.
- Configure the value for PatientSecure Reporting Service to match the following format: https://<LoadBalancingServer>:<ConfiguredPort>/api
   For example: https://myLoadBalancer.mydomain.com:7004/api

## Step 9: Configure the Emergency Search Service & Palm Vein Auth Service

To install the Emergency Search & Authentication Service on the application servers:

- 1. From the PatientSecure Server Dashboard, click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure Emergency Search Service section, select the drive, and then click **Install Emergency Search**.

The Emergency Search Service ports default to 7005 and 7006.

- 3. Enter the Windows administrator credentials for the server, and then click Confirm.
- 4. Repeat this procedure for Application Server 2.
- 5. Click Advanced Settings. The Advanced Settings page lists the installed PatientSecure components.
- Configure the value for PatientSecure Emergency Search Service to match the following format: https://<LoadBalancingServer>:<ConfiguredPort>/api
   For example: https://myLoadBalancer.mydomain.com:7005/api

## Step 10: Configure the PatientSecure System Health Service

The PatientSecure System Health Service monitors the status of the PatientSecure database and application servers, and powers the system health dashboard in the PatientSecureAdmin Console. To install the System Health Service on the application servers:

- 1. From the PatientSecure Server Dashboard, click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure System Health Service section, select the drive, and then click **Install System Health Service**. The service port defaults to 7007.
- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat this procedure for Application Server 2.
- Click Advanced Settings at the top of the page.
   The Advanced Settings page lists the installed Imprivata PatientSecure components.
- Configure the value for PatientSecure System Health Service to match the following format: https://<LoadBalancingServer>:<ConfiguredPort>/api
   For example: https://myLoadBalancer.mydomain.com:7007/api

## Step 11: Install the HL7 Service on the Application Servers

To install the HL7 Service on the application servers:

- 1. From the PatientSecure Server Dashboard, click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure HL7 Service section, select the drive, and then click Install HL7.
- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat this procedure for Application Server 2.

HL7 Sender and Processor services automatically pick an application server to be their active server, and switch to another healthy server when they detect that the current active server has stopped sending messages.

The Listener service should only be actively managing traffic on one application server at a time. When the HL7 Listener service fails on Application server 1, you must re-route traffic to Application server 2. You may need to manually point the HL7 engine to Application server 2, or set up a VIP.

## Step 12: Configure the FHIR Service



#### NOTE:

Configuring this service is optional, and depends on whether your PatientSecure environment will integrate with the FHIR service.

To install the FHIR Service on the application servers:

- 1. From the PatientSecure Server Dashboard, click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure FHIR Service section, select the drive and specify the port, and then click **Install FHIR**.
- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat this procedure for Application Server 2.
- 5. Click Advanced Settings. The Advanced Settings page lists the installed PatientSecure components.
- 6. Configure the value for PatientSecure FHIR Server to match the following format:

https://<LoadBalancingServer>:<ConfiguredPort>/api

For example: https://myLoadBalancer.mydomain.com:7008/api

#### Step 13: Configure the EMPI Service

#### NOTE:

Configuring this service is optional and depends on whether your PatientSecure environment will integrate with an EMPI such as Verato MPI or Initiate.

To install the EMPI Service on the application servers:

- 1. From the PatientSecure Server Dashboard, click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure EMPI Service section, select the drive and specify the port, and then click **Install EMPI**.
- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat this procedure for Application Server 2.
- 5. Click **Advanced Settings** at the top of the page. The Advanced Settings page lists the installed PatientSecure components.
- 6. Configure the value for PatientSecure EMPI Server to match the following format:
- 7. https://<LoadBalancingServer>:<ConfiguredPort>/api
- 8. For example: https://myLoadBalancer.mydomain.com:7009/api

## F5 BIG-IP GTM/LTM

For more details on workflows in the F5 BIG-IP management interface, see your F5 BIG-IP documentation.

To configure connection balancing in F5 BIG-IP GTM/LTM, perform the following tasks.

## Step 1: Add Application Servers to the Load Balancer

In the F5 BIG-IP management interface, add the PatientSecure Application Servers to the load balancer.

1. Use the fully qualified domain names (FQDNs) of Application Server 1 and Application Server 2 when adding them to the load balancer.

## Step 2: Configure Traffic Groups and Rules

Imprivata recommends creating traffic groups and traffic rules in F5 to manage the different communication protocols for the PatientSecure services.

- **HTTP-based services** Identity Server, Web Services, Reporting Service, User Interface, Admin Console, Emergency Search & Palm Vein Authentication Service, System Health Service, and optionally, the EMPI and FHIR services.
- TCP/IP-based services HL7 services.

### Example

- Create the FQDN as **patientsecure.hospital.org**, and then create a rule to balance calls to it between both active servers.
- Create the FQDN as **patientsecurehl7.hospital.org**, and then create a rule that routes all traffic to it to the one server currently processing all HL7 requests for PatientSecure.
- Set the "Idle Timeout" in the TCP profile to a value sufficient to handle the longest client idle timeout. Imprivata recommends a minimum of 1860 seconds (31 minutes) to accommodate the default PatientSecure Admin Console (PSAC) session idle length (30 minutes).

## Step 3: Configure the VIP

In the F5 BIG-IP management interface, create the load balancing virtual servers for each PatientSecure component and configure the server certificate bindings.

- 1. For PatientSecure Identity Service, use port 7001.
- 2. For PatientSecure Web Service, use port 7002.
- 3. For PatientSecure Admin Console, use port 443.
- 4. For PatientSecure User Interface, use port 7003.
- 5. For PatientSecure Reporting Service, use port 7004.

- 6. For PatientSecure Emergency Search service, use port 7005.
- 7. For PatientSecure Palm Vein Auth service, use port 7006.
- 8. For PatientSecure System Health service, use port 7007.
- 9. Optional. For the PatientSecure FHIR service, use port 7008.
- 10. *Optional.* For the PatientSecure EMPI service, use port 7009.

## Step 4: Configure the PatientSecure Identity Server

Using the PatientSecure Server Console interface, install the PatientSecure Identity Server component on the two application servers and configure the URL for the VIP.

To install the Identity Server component on the application servers:

- 1. Click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure Identity Server section, select the drive and port, and then click **Install PSIS**.



**NOTE:** The default port value is 7001.

- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat Steps 1 through 3 of this procedure for Application Server 2.
- 5. Click Advanced Settings. The Advanced Settings page lists the installed PatientSecure components.
- Configure the value for PatientSecure Identity Server to match the following format: https://<LoadBalancingServer>:<ConfiguredPort>/identityserver
   For example: https://myLoadBalancer.mydomain.com:7001/identityserver

## Step 5: Configure the PatientSecure Web Services

To install PatientSecure Web Services (PSWS) on the application servers:

- 1. From the PatientSecure Dashboard, click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure Web Services section, select the drive and port, and then click **Install PSWS**.



**NOTE:** The port setting should match the value configured for the Load Balancer port above. The default value is 7002.

- 3. Enter the Windows administrator credentials for the server, and then click Confirm.
- 4. Repeat Steps 1 through 3 of this procedure for Application Server 2.
- 5. Click Advanced Settings. The Advanced Settings page lists the installed PatientSecure components.
- 6. Configure the value for PatientSecure Web Services to match the following format:

https://<LoadBalancingServer>:<ConfiguredPort>/psws/api For example: https://myLoadBalancer.mydomain.com:7002/psws/api

## Step 6: Configure the User Interface Server

To install the User Interface Server component on the application servers:

- 1. Click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure User Interface section, select the drive and port, and then click **Install CLIENT**.



**NOTE**: The default port value is 7003.

- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat Steps 1 through 3 of this procedure for Application Server 2.
- 5. Click Advanced Settings. The Advanced Settings page lists the installed PatientSecure components.
- Configure the value for PatientSecure User Interface Server to match the following format: https://<LoadBalancingServer>:<ConfiguredPort>
   For example: https://myLoadBalancer.mydomain.com:7003

## Step 7: Configure the Admin Console

- 1. From the PatientSecure Server Dashboard, click the server row for the first application server to open its Server Details page.
- 2. In the Services PatientSecure Admin Console section, select the drive, and then click **Install ADMIN**. The Admin Console installs on port 80 and port 443 (if SSL is used).
- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat this procedure for all application servers.

## Step 8: Configure the Reporting Service

The Reporting Service component is required for the Admin Console to display the dashboard and to run reports.

To install the Reporting Service on the application servers:

- 1. From the PatientSecure Server Dashboard, click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure Reporting Service section, select the drive, and then click Install Reporting.

The Reporting Service port defaults to 7004.

3. Enter the Windows administrator credentials for the server, and then click Confirm.

- 4. Repeat this procedure for Application Server 2.
- 5. Click Advanced Settings. The Advanced Settings page lists the installed PatientSecure components.
- Configure the value for PatientSecure Reporting Service to match the following format: https://<LoadBalancingServer>:<ConfiguredPort>/api
   For example: https://myLoadBalancer.mydomain.com:7004/api

## Step 9: Configure the Emergency Search Service & Palm Vein Auth Service

To install the Emergency Search & Authentication Service on the application servers:

- 1. From the PatientSecure Server Dashboard, click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure Emergency Search Service section, select the drive, and then click **Install Emergency Search**.

The Emergency Search Service ports default to 7005 and 7006.

- 3. Enter the Windows administrator credentials for the server, and then click Confirm.
- 4. Repeat this procedure for Application Server 2.
- 5. Click Advanced Settings. The Advanced Settings page lists the installed PatientSecure components.
- Configure the value for PatientSecure Emergency Search Service to match the following format: https://<LoadBalancingServer>:<ConfiguredPort>/api
   For example: https://myLoadBalancer.mydomain.com:7005/api

## Step 10: Configure the PatientSecure System Health Service

The PatientSecure System Health Service monitors the status of the PatientSecure database and application servers, and powers the system health dashboard in the PatientSecureAdmin Console. To install the System Health Service on the application servers:

- 1. From the PatientSecure Server Dashboard, click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure System Health Service section, select the drive, and then click **Install System Health Service**. The service port defaults to 7007.
- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat this procedure for Application Server 2.
- 5. Click Advanced Settings at the top of the page.

The Advanced Settings page lists the installed Imprivata PatientSecure components.

 Configure the value for PatientSecure System Health Service to match the following format: https://<LoadBalancingServer>:<ConfiguredPort>/api
 For oxample: https://mul.oadBalancor.mudomain.com:7007/api

For example: https://myLoadBalancer.mydomain.com:7007/api

## Step 11: Install the HL7 Service on the Application Servers

To install the HL7 Service on the application servers:

- 1. From the PatientSecure Server Dashboard, click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure HL7 Service section, select the drive and specify the port, and then click **Install HL7**.
- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat this procedure for Application Server 2.

HL7 Sender and Processor services automatically pick an application server to be their active server, and switch to another healthy server when they detect that the current active server has stopped sending messages.

The Listener service should only be actively managing traffic on one application server at a time. When the HL7 Listener service fails on Application server 1, you must re-route traffic to Application server 2. You may need to manually point the HL7 engine to Application server 2, or set up a VIP.

## Step 12: Configure the FHIR Service



#### NOTE:

Configuring this service is optional, and depends on whether your PatientSecure environment will integrate with the FHIR service.

To install the FHIR Service on the application servers:

- 1. From the PatientSecure Server Dashboard, click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure FHIR Service section, select the drive and specify the port, and then click **Install FHIR**.
- 3. Enter the Windows administrator credentials for the server, and then click Confirm.
- 4. Repeat this procedure for Application Server 2.
- 5. Click Advanced Settings. The Advanced Settings page lists the installed PatientSecure components.
- 6. Configure the value for PatientSecure FHIR Server to match the following format:

https://<LoadBalancingServer>:<ConfiguredPort>/api

For example: https://myLoadBalancer.mydomain.com:7008/api

## Step 13: Configure the EMPI Service



Configuring this service is optional and depends on whether your PatientSecure environment will integrate with an EMPI such as Verato MPI or Initiate.

To install the EMPI Service on the application servers:

- 1. From the PatientSecure Server Dashboard, click the server row for Application Server 1 to open its Server Details page.
- 2. In the Services PatientSecure EMPI Service section, select the drive and specify the port, and then click **Install EMPI**.
- 3. Enter the Windows administrator credentials for the server, and then click **Confirm**.
- 4. Repeat this procedure for Application Server 2.
- 5. Click Advanced Settings at the top of the page. The Advanced Settings page lists the installed PatientSecure components.
- 6. 2. Configure the value for PatientSecure EMPI Server to match the following format:
- 7. https://<LoadBalancingServer>:<ConfiguredPort>/api
- 8. For example: https://myLoadBalancer.mydomain.com:7009/api

## Connect Clients to a High Availability Environment

Install the PatientSecure client software on the endpoints that will connect to the High Availability environment.

For clients in high availability environments secured with third-party certificates:

- 1. On the client endpoints, deploy or install the third-party certificate to the local machine's truststore. For more information on installing certificates, see the Windows documentation for your version of Windows.
- 2. Install the PatientSecure client software by using either the installation program or by installing by command line.

For more information, see the topic "Installing the PatientSecure Client" in the <u>PatientSecure</u> online help.

#### (i) NOTE: When

When connecting your PatientSecure Clients to the High Availability environment, use the same FQDN and Port from the PatientSecure Web Services URL defined in the procedure Step 3b: Configure Advanced Settings.

For example: myLoadBalancer.mydomain.com and 7002.

## **Update Connection Strings**

You can update all connection strings for components installed on an application server.

This is especially helpful when migrating a PatientSecure environment from a single application server to a multiple-server High Availability environment.

To update the connections strings to pick up a URL change:

- 1. From the PatientSecure Server Dashboard, click the server row for Application Server 1 to open its Server Details page.
- 2. In the Server Info section, click **Update Service Connection Strings**. Enter your Windows credentials for the server.
- 3. Repeat the steps for Application Server 2.

## Troubleshooting

If you are unable to access or use Imprivata PatientSecure in a load-balanced configuration, try the following steps to resolve the problem:

## Microsoft IIS

1. For each server, verify that you are able to access the default IIS page. This page can be found by following the PatientSecure Identity Server link from the PatientSecure Server Console:

Services			
PatientSecure Identity Server			
Install Port			Identity Server Version
7001			6.6.000.1
Install Directory	Installed By	Install Date	Install Status
C:\Program Files\Imprivata	ps\administrator	7/30/2020 7:38:24 AM	Successful
Install Logs	SSL	Link	
Debug Error	Yes	https://arr-03.example.eng:7001/	ldentityServer
			Uninstall   Upgrade

2. Once the PSIS components have been verified, perform the same action for the PatientSecure Web Services. If PSWS is working correctly, you should receive a blank page with the word: **Success**.

PatientSecure Web Services			
Install Port 7002			Web Services Version 6.6.000.1
Install Directory C:\Program Files\Imprivata	Installed By ps\administrator	Install Date 7/30/2020 7:39:57 AM	Install Status Successful
Install Logs Debug Error	<b>SSL</b> Yes	Link https://arr-03.example.eng:7002/psws/api	-
			Uninstall  Upgrade

3. If both these services are running, the issue is likely with the Load Balancer configuration. Review your setup and verify that everything is configured correctly.