



Australian Government

Australian Digital Health Agency



HIPS

Initial and Clean Installation Guide (P2P)

7 November 2016

V6.1

Approved for external use

Australian Digital Health Agency

Level 25, 56 Pitt Street

Sydney, NSW 2000

Australia

www.digitalhealth.gov.au

Acknowledgements**Council of Australian Governments**

The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.

Disclaimer

The Australian Digital Health Agency ("the Agency") makes the information and other material ("Information") in this document available in good faith but without any representation or warranty as to its accuracy or completeness. The Agency cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Document control

This document is maintained in electronic form and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

Copyright © 2016 Australian Digital Health Agency

This document contains information which is protected by copyright. All Rights Reserved. No part of this work may be reproduced or used in any form or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems – without the permission of the Australian Digital Health Agency. All copies of this document must include the copyright and other information contained on this page.

Document information

Key information

Owner	Executive General Manager Innovation and Development
Date of next review	[Next scheduled date of review]
Contact for enquiries	Australian Digital Health Agency Help Centre
t:	1300 901 001
e:	help@digitalhealth.gov.au

Product version history

Product version	Date	Release comments
1.0	February 2014	Initial release (HIPS 4.1.0).
2.0	February 2015	See release note (NEHTA-2040:2015) for details of changes and bug fixes.
2.0.1 2.0.2		Unpublished updates.
2.0.3	February 2016	See release note (NEHTA-2185:2016) for details of changes and bug fixes.
6.0.0	March 2016	See release note (NEHTA-2263:2016) for details of changes and bug fixes.
6.1	November 2016	See release note (DH-2445:2016) for details of changes and bug fixes.

Table of contents

1.	Important Information	6
1.1	System Environments	6
2.	Introduction	7
2.1	Purpose	7
2.2	Scope.....	7
2.3	Assumptions	7
2.4	Definitions and Acronyms	8
3.	Prerequisites	9
3.1	Installation of HIPS Core module	9
3.2	Application Server Operating Environment	9
3.3	Database Operating Environment	9
3.4	Active Directory Service Account	9
3.5	SMD Hosting Environment	10
4.	P2P.....	11
4.1	Database Preparation	11
4.1.1	Create the P2P Data Store Database	11
4.1.2	HIPS Active Directory Service Account Access.....	11
4.1.3	Configure and execute the P2P Data Store Scripts.....	11
4.2	P2P Application Server Operating System Preparation	13
4.2.1	Prepare HIPS IIS Application Pool Account	15
4.3	P2P Application Server Site Installation	15
4.3.1	Removing an earlier HIPS version for a new installation	16
4.3.2	Installing the new web site and application	16
4.4	P2P Application Server Self-Signed SSL Certificate.....	17
4.5	P2P Web Configuration Setup	18
4.6	P2P Application Server Code Installation	18
4.7	Confirm P2P Installation	19
4.7.1	Confirm Available Web Services	19
5.	SMD Front End and Decrypter	21
5.1	SMD Application Server Operating System Preparation	21
5.1.1	Service Accounts	22
5.1.2	File System Folders	22
5.2	P2P Application Server Site Installation	23
5.2.1	SMD Decrypter Server.....	23
5.2.2	SMD Front-End Server.....	24
5.3	NASH Certificates Installation.....	25
5.3.1	SMD Decrypter Server.....	25

Appendix A P2P Application Server Configuration Explanation 29

1. Important Information

It is important to note that this installation document has been written as an installation guide for both a test or production environment of the HIPS product suite. The scripts and configuration files have been provided for both SVT (software vendor testing) and production environments.

1.1 System Environments

This installation guide is targeted at the system test environment ("TEST"). A profile of this installation guide should be created for each system environment that is to be created. Suggested values for each environment are given below:

Environment	Database Name	App Site
Production	P2PDataStoreProd	PROD
Pre-Production	P2PDataStorePreProd	PREPROD
System Test	P2PDataStoreTest	TEST
Development	P2PDataStoreDvlp	DEV

2. Introduction

HIPS is a communications solution to enable Patient Administration Systems and Clinical Information Systems to interact with the National My Health Record System.

The P2P component enables the sending and receiving of clinical documents both interstate and intrastate.

The HIPS P2P component extends the HIPS Core and the HIPS UI product by providing the following key capabilities:

- Directory maintenance, providing a Local Health Service Directory (LHSD) used for the purposes of addressing during P2P messaging, and a mechanism for maintaining and synchronising this LHSD from the National Health Service Directory (NHSD) and associated data sources exposed by the National Endpoint Proxy Service (NEPS).
- Secure message delivery (SMD), providing mechanisms to address, send and receive messages securely between providers, supported by the information maintained within the LHSD.

The HIPS Release 6.1 has been through system testing, performance testing and Agency Conformance Assessment Process (CAP).

2.1 Purpose

The purpose of this document is to provide the technical details and steps required to install the 6.1 version of the HIPS P2P, SMD and Decrypter components which are all parts of HIPS the product suite.

It can be used by health facilities to install the HIPS P2P, SMD and SMD Decrypter components of the product suite into a targeted environment.

This document describes the prerequisites and steps that are required for the HIPS P2P, SMD and SMD Decrypter components to be installed for the first time (clean installation).

2.2 Scope

This document covers prerequisites required for the targeted environment, the database server preparation and application server operating system. The document will then go on to describe the steps required for the installation of the HIPS P2P module on the database server and application server(s).

The SMD Hosting Environment will then be detailed and the installation instructions for the SMD and SMD Decrypter components will be described.

This document does not describe any functional requirements or features of the HIPS product suite as these are covered by other documentation.

2.3 Assumptions

The following assumptions have been made during the development of this document:

- The user carrying out the installation has server administration access to the targeted database server and application server(s).
- The facility installing the HIPS product suite has appropriate software versions and server operating systems.

The deployment instructions within this document assume the following:

- The HIPS P2P and SMD components have not been previously deployed to the target environment, or if they have been previously deployed then they have been removed following the instructions provided in [Rollback](#).

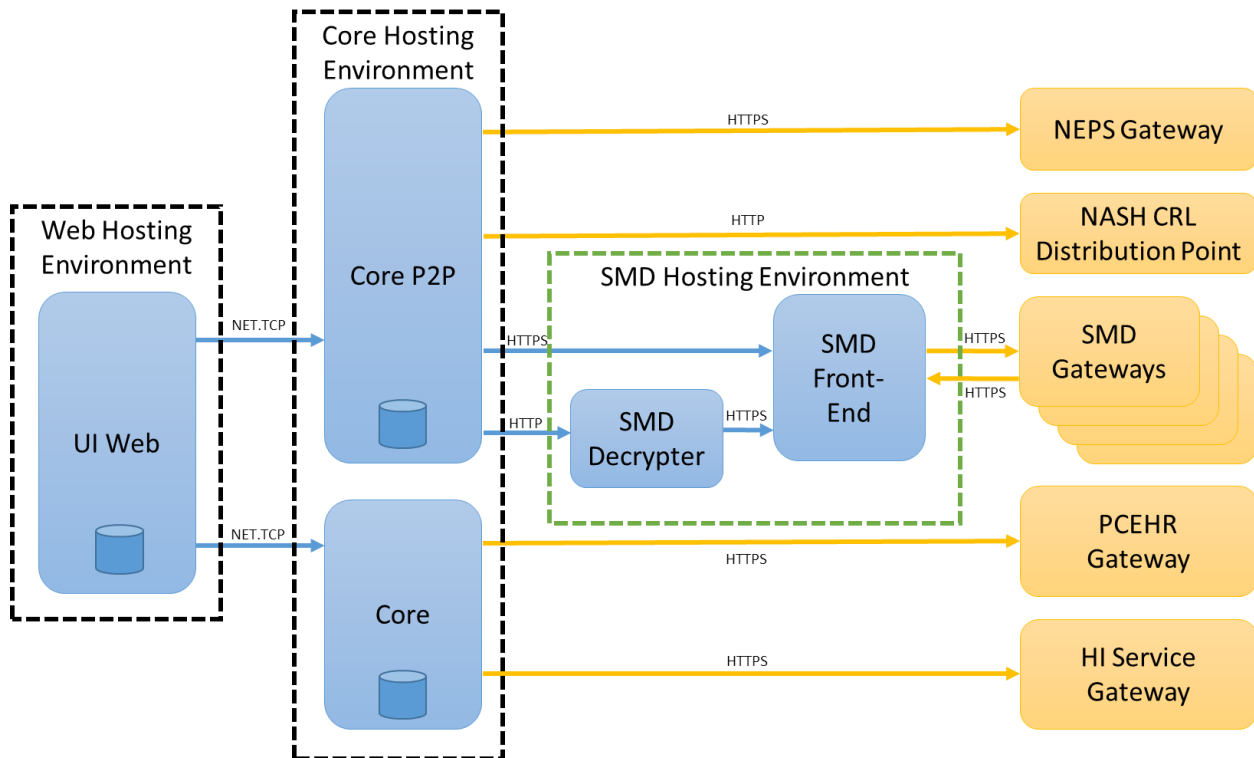
- Domain firewall rules allow inbound connections to the HIPS **SMD Front-End Application Server** from the **Internet** on port 443.
- Domain firewall rules allow inbound connections to the HIPS **SMD Front-End Application Server** from the HIPS **SMD Decrypter Application Server**.
- Domain firewall rules allow inbound connections to the HIPS **SMD Front-End Application Server** from the HIPS **Core P2P Application Server**.
- Domain firewall rules allow inbound connections to the HIPS **SMD Decrypter Application Server** from the HIPS **Core P2P Application Server**.
- Domain firewall rules allow inbound connections to the HIPS **Core Application Server** from the HIPS **Core P2P Application Server**.
- Domain firewall rules allow inbound connections to the HIPS **Core Application Server** from the HIPS **UI Web Application Server**.
- Domain firewall rules allow inbound connections to the HIPS **Core P2P Application Server** from the HIPS **UI Web Application Server**.

2.4 Definitions and Acronyms

Item	Definition
PAS	Patient Administration System
LIS	Laboratory Information System
RIS	Radiology Information System
HIPS	Healthcare Identifier and PCEHR System
ESB	Enterprise Service Bus
CAP	Conformance Assessment Process
CIS	Clinical Information System
HPI-O	Health Provider Identifier – Organisation
P2P	Provider to Provider
SMD	Secure Message Delivery

3. Prerequisites

This section outlines the major prerequisites that an implementer will need to obtain before implementing HIPS in either a test or production environment. The following diagram illustrates the HIPS modules:



3.1 Installation of HIPS Core module

The HIPS P2P module is dependent on the HIPS Core module. The HIPS Core module must be installed prior to the installation of the HIPS P2P module. See the *HIPS Release 6.1 – Initial and Clean Installation Guide (Core)* for HIPS Core installation instructions.

3.2 Application Server Operating Environment

To install the HIPS P2P application server, the organisation may install on the existing HIPS Core application server.

3.3 Database Operating Environment

To install the P2P Data Store database, the organisation may:

- Install on the existing Microsoft SQL Server 2008 R2 that the HIPS Core database has been installed on.
- Provision a separate Windows Server 2008 R2 operating environment and install Microsoft SQL Server 2008 R2. This setup is preferable for the production environment.

3.4 Active Directory Service Account

HIPS uses Active Directory to secure its internal connections and it is recommended that an AD service account is used (one that does not expire and will not lock). This will be called the “HIPS AD Service account user” for the remainder of the document.

3.5 SMD Hosting Environment

To install the SMD and SMD Decrypter components the organisation may install on separate servers the following components:

- *HIPS-SMD Front-End Application Server.* Server node that hosts the IIS instance into which the HIPS-SMD Front-End application server components will be deployed. Requires:
 - Internet Information Services 7.5
 - .NET Framework 4.5
 - HIPS-SMD Front-End 6.1 (Under the SMD_AppServer folder in the Core Software Package)
- *HIPS-SMD Decrypter Application Server.* Server node that hosts the IIS instance into which the HIPS-SMD Decrypter application server components will be deployed.
 - Internet Information Services 7.5
 - .NET Framework 4.5
 - HIPS-SMD Decrypter 6.1 (Under the SMD_Decrypter folder in the Core Software Package)

4. P2P

4.1 Database Preparation

4.1.1 Create the P2P Data Store Database

1. On the database server create a new database using the database name suggested in section 1.1 System Environments (example P2PDataStoreTest) with the following settings:
2. Add a new Filegroup (in the Filegroups tab) called INDEXES (leave the PRIMARY as the default).
3. For the database files (these are recommended minimum sizes):
 - a. For greater performance it is recommended that the Rows Data, Log Data and Index Data should be located on different disc partitions or SAN LUNs.
 - b. The initial data store rows data (P2PDataStoreTest) with PRIMARY file group requires an initial size of 1024MB, with an auto growth of 250MB and unrestricted file growth.
 - c. The initial Log (P2PDataStoreTest_log) requires an initial size of 500MB, with an auto growth of 10% and unrestricted file growth.
 - d. A new database file is required and is to be named P2PDataStoreTest_Index (or appropriate name based on system environment setup) (Rows Data) with the INDEXES file group and requires an initial size of 500MB, with an auto growth of 250MB and unrestricted file growth.

4.1.2 HIPS Active Directory Service Account Access

1. Add the HIPS AD Service account user to the SQL Server and assign it db_datareader and db_datawriter to the new P2PDataStore database.

4.1.3 Configure and execute the P2P Data Store Scripts

1. In the folder "HIPS Core Database\HIPS_P2P\" in the Core Software Package with the supplied binaries are 8 script files.
2. The 06_P2P_LocalOrganisationTemplate.sql script outlines the data and scripts required to define your organisation structure within the P2P database. You will need to update this script with your organisation information (Networks, Organisations and NEPS subscriptions) before running this script. Make the following changes in the script (being mindful of whether you are creating this script for SVT or Production):
 - a. For the AccessingOrganisation table:
 - Replace [HPIO] column with the HPI-O of the Healthcare Provider Organisation.
 - Replace [Organisation Legal Name] column with the name of the Healthcare Provider Organisation.
 - Replace [SMDClientCert] column with the serial number of the certificate from the SMD Front End Client.
 - Replace [NEPSCClientCert] column with the serial number of the certificate that will connect to NEPS.
 - Replace [SMDPayloadCert] column with the serial number of the certificate that will be used to encrypt the message payloads.
 - Replace [Authorised Employee Name] column with the name of the person who within the organisation has the authority to make calls to any intermediaries.

- Replace [Authorised Employee UserId] column with the identifier or username of the person who within the organisation has the authority to make calls to any intermediaries.
- b. For the Subscription table:
 - Replace the [NEPS Subscription Id] column with the provided subscription id for the NEPS interface.
- 3. The 07_P2P_Roles.sql script is used to ensure the application service account is a member of the roles necessary to read and write the tables, read from the views and execute the stored procedures. You will need to update this script with the name of the application service account before running this script.
- 4. These scripts then need to be executed in the P2P Data Store database **in order**:
 - a. 01_P2P_Schema.sql
 - b. 02_P2P_TableScript.sql **** Note** This script must be run twice.
 - c. 03_P2P_Indexes.sql
 - d. 04_P2P_Code.sql **** Note** This script must be run twice.
 - e. 05_P2P_Data.sql
 - f. 06_P2P_LocalOrganisationTemplate.sql **** Note** this script was updated in Step 2.
 - g. 07_P2P_Roles.sql **** Note** this script was updated in Step 3.
 - h. 08_P2P_PermissionScript.sql
- 5. This completes the P2P Data Store setup.
- 6. Verify the following objects have been created in the database:
 - 61 Tables, the first being [els].[Delegate], the last being [smd].[TransportResponseStatus].
 - 2 Functions named [nhsd].[GetProviderEntityTypeId] and [nhsd].[Split].
 - 3 Stored Procedures named [nhsd].[ProviderIndividual_Delete], [nhsd].[ProviderIndividual_Insert] and [nhsd].[ProviderIndividual_Update].
- 7. Verify the following tables have data:
 - [p2p].[ChangeType]
 - [els].[DocumentType]
 - [smd].[MessageDirection]
 - [smd].[MessageStatus]
 - [els].[PayloadPackaging]
 - [nhsd].[ProviderEntityType]
 - [nhsd].[ProviderIdentifierStatus]
 - [els].[ServiceInterface]
 - [smd].[Sex]
 - [smd].[TransportResponseClass]
 - [smd].[TransportResponseStatus]
 - [els].[PayloadScheme]
 - [p2p].[Setting]
 - [nhsd].[ReferenceProfile]

- [nhsd].[ReferenceSet]
- [nhsd].[ReferenceItem]
- [nhsd].[ProviderIdentifierType]
- [nhsd].[ProviderStatus]
- [p2p].[AccessingOrganisationNetwork] at least 1 record for the seed HPIO
- [p2p].[AccessingOrganisation] at least 1 record with the Accessing Organisations HPIO details
- [neps].[Subscription] at least 1 record with the NEPS Subscription ID.

4.2 P2P Application Server Operating System Preparation

The following steps are for installation on the assigned HIPS P2P application server on a Windows 2008 R2 Server.

- Ensure that Microsoft .NET Framework v4.5 is installed.
- Under the Server Manager “Features” enable the following items (as well as any default settings):
 - Message Queuing
 - Message Queuing Services
 - Message Queuing Server
 - Directory Service Integration
 - HTTP Support
 - Windows Process Activation Service
 - Process Model
 - .NET Environment
 - Configuration APIs
 - .NET Framework 3.5.1 Features
 - NET Framework 3.5.1
 - WCF Activation
 - HTTP Activation
 - Non-HTTP Activation
 - Remote Server Administration Tools
 - Role Administration Tools
 - Web Server (IIS) Tools

NOTE: Restart may be required.

NOTE: If Message Queuing Services has already been installed on an existing server but Directory Service Integration was not installed then simply checking the Directory Service Integration may not correctly install the service, due to a known issue with MSMQ configuration. Uninstalling Message Queuing Services and reinstalling with Directory Service Integration (and other items as above) has been known to resolve this issue if it occurs.

- Under the Server Manager “Roles” enable the following items for the Web Server (IIS) (as well as any default settings):
 - Web Server
 - Common HTTP Features
 - Static Content
 - Default Content
 - Directory Browsing
 - HTTP Errors
 - HTTP Redirection
 - Application Development
 - ASP.NET
 - .NET Extensibility
 - Health and Diagnostics
 - HTTP Logging
 - Logging Tools
 - Request Monitor
 - Tracing
 - Security
 - Basic Authentication
 - Windows Authentication
 - Client Certificate Mapping Authentication
 - IIS Client Certificate Mapping Authentication
 - URL Authorisation
 - Request Filtering
 - IP and Domain Restrictions
 - Performance
 - Static Content Compression
 - Dynamic Content Compression
 - Management Tools
 - IIS Management Console
 - IIS Management Scripts and Tools
 - Management Service
- Under the Servers Services, ensure that the following items are set to Automatic start up:
 - Net.Tcp Listener Adapter
 - Net.Tcp Port Sharing Service
 - Net.Msmq Listener Adapter
- Ensure that PowerShell is installed

- Start PowerShell as Administrator and execute commands:

```
Get-ExecutionPolicy
```

```
Set-ExecutionPolicy Unrestricted
```

```
Get-ExecutionPolicy
```

Record the initial value, and ensure that the final value is Unrestricted. This will ensure that the unsigned PowerShell scripts used in Section 4.3 can run. The execution policy can be set back to the original value after the installation scripts have run.

4.2.1 Prepare HIPS IIS Application Pool Account

The HIPS service will execute using the account set in the IIS Application Pool.

- On the HIPS Application Server check that the HIPS AD Service account user is added to the local server group **IIS_IUSRS**.

4.3 P2P Application Server Site Installation

The directory “P2P_AppServer\ps_scripts” in the Core Software Package, contains the main installation PowerShell script P2P_SiteCreate.ps1 and the environment-specific configuration scripts BuildP2PSite_DEV.ps1, BuildP2PSite_PROD.ps1, BuildP2PSite_TEST.ps1.

Open the “BuildP2PSite_TEST.ps1” script and edit as following:

- The default location for the Application Files is under the “D:\Projects\P2P_TEST\” directory, this can be changed in **both** the AppSitePath and AppServerPath entires in this script (keeping the ‘blank’ and ‘Build’ text).
It is recommended that the Application Files are not on the same drive as the system drive, however this may depend on the server configuration and will not affect performance.
- Replace the “Domain\ServiceAccount” (in the ProcessUserName item) with the HIPS AD Service account user.
- Replace the “ProcessPassword” with the password of the HIPS AD Service account user.

The code will be installed beneath the directory “AppSitePath”, which will be created when the PowerShell scripts are run.

The following table indicate the settings in BuildP2PSite_TEST.ps1 for the System Testing environment:

Option Name	Suggested Value	Description
-AppSiteName	P2P_TEST	An IIS site will be created with this name.
-AppSitePath	D:\Projects\P2P_TEST\blank	The IIS site will be served from this directory, which should be empty.
-AppPoolName	P2PServerAppPool_TEST	An IIS application pool will be created with this name
-ProcessUserName	<i>domain\serviceaccount</i>	P2P will run under this user account (Note: this is the same account that was given permissions in the SQL database)
-ProcessPassword	Password within file	Password for the user account above
-HTTPBinding	61500	The web services will be accessible using HTTP protocol on this port.
-NETTCPBinding	61000	The web services will be accessible using net.tcp protocol on this port.

Option Name	Suggested Value	Description
-HTTPSBinding	61443	The web services will be accessible using HTTPS protocol on this port.
-AppServerName	P2PServer_TEST	An IIS application will be created using this name, within the above site.
-AppServerPath	D:\Projects\P2P_TEST\Build	The IIS application will be served from this directory, which should contain the svc files, Web.config file and bin directory. The bin directory should contain all the DLL files.
Out-File	"P2P_TEST_Creation.log"	The setup process will be logged to a file with this name.

4.3.1 Removing an earlier HIPS version for a new installation

*****If you are installing Release 6.1 onto a server running an earlier release and you are NOT performing an upgrade, then the existing web site MUST be removed first.**

Follow these steps to remove the old web site and application:

1. From the File Explorer take a backup of the entire site content under "D:\Projects\P2P_TEST" (or where ever the existing version of HIPS resides) and move it to a safe location.
2. Open IIS Manager and right click on the "P2P_TEST" (or whatever the existing version of HIPS is named) site
3. Select "Remove" from the context menu and accept the removal.
4. Also within the IIS Manager navigate to the Application Pools and right click the "P2PServerAppPool_TEST" application pool (or whatever the existing version of the HIPS application pool is named).
5. Select "Remove" from the context menu and accept the removal.
6. Open a command window as an administrator and type in "iisreset".
7. Go back to the File Explorer under "D:\Projects\" and delete the entire "P2P_TEST" (or where ever the existing version of HIPS resides) directory.
8. This has now cleaned the server ready for the new implementation.

4.3.2 Installing the new web site and application

Follow these steps to install the new web site and application:

1. Start PowerShell as Administrator
2. Change to the directory containing the build scripts
(\"P2P_AppServer\ps_scripts\")
3. Execute command:
./BuildP2PSite_TEST.ps1

Check the on-screen output and the log file to ensure that the installation completed successfully.

Select the P2PServerAppPool_TEST application pool and click the “Advanced Settings”

1. Set the “Queue Length” to **2000**
2. Ensure “Start Automatically” is *True* or “Start Mode” is *AlwaysRunning*
3. Set the Idle Time-out to 1440 minutes (one day) or longer
4. Set the Load User Profile as True
5. Under the “Generate Recycle Event Log Entry” set all sub values as True.
6. Set the “Regular Time Interval (minutes)” to **1740**.

By default, the P2P web services will not automatically start on a server or IIS restart. We will use the Windows Server AppFabric to ensure that they do start after a server or IIS restart.

1. Select the P2PServer_TEST application from the P2P_TEST website
2. In the Actions pane under the Manage WCF and WF Services click “Configure”
3. Select “Auto-Start” from the left hand navigation
4. Select the “Enabled (all services will auto-start)” radio option.

4.4 P2P Application Server Self-Signed SSL Certificate

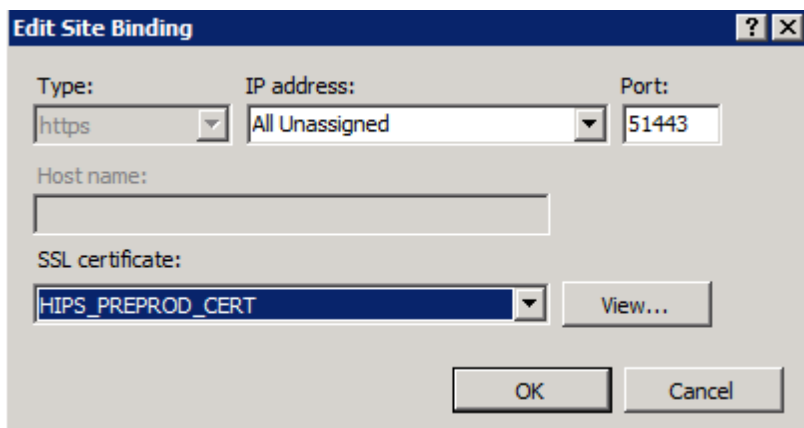
HIPS P2P can be configured to use HTTP or HTTPS connectivity.

A risk assessment of the HIPS solution has resulted in a recommendation that all traffic between HIPS and internal applications should occur using an encrypted connection, i.e. using HTTPS rather than HTTP. However, this is not essential to the connectivity of HIPS, so if your datacentre allows HTTP communications between applications within the datacentre then this is also possible.

While it is possible to use an internal PKI certificate service, or a commercial certificate, a Self-Signed SSL certificate is also considered an acceptable solution for communication between internal applications and HIPS.

A self-signed certificate may be configured via the steps below:

1. Select the main IIS instance of the application server and double-click the “Server Certificates” icon.
2. On the far right click the action “Create Self-Signed Certificate...”
3. Specify a friendly name as “HIPS_TEST_CERT” and click OK.
4. To apply the self-signed certificate - Select the “HIPS_TEST” site and in the far right select the “Bindings” action.
5. Select the “https” row from the “Site Bindings” dialogue and click “Edit”.
6. In the “Edit Site Bindings” dialogue, select the “HIPS_TEST_CERT” from the “SSL Certificate” drop down and click OK.



7. Close the “Site Bindings” dialogue.

4.5 P2P Web Configuration Setup

Edit the web.config file provided in the ‘P2P_AppServer\binaries’ folder as follows:

1. Modify the connection string in the ‘connectionStrings’ element to allow connection to the P2P Data Store database.
2. Modify the certificate thumbprint in the ‘clientCertificate’ element to be the thumbprint of one of the installed NASH PKI Certificates for HPI-O that are configured as an internal certificate on the HIPS SMD Front-End server.

NOTE: There is a hidden spacebar character in the first of the certificate number if you copy and paste it from certificate details. Please remove this hidden character by using Backspace key.

3. Modify the port numbers and URLs in the ‘client’ element to establish connectivity with the HIPS Core, HIPS SMD Decrypter and HIPS SMD Front-End servers already installed.

Edit the log4net.xml file provided in the same folder as follows:


















1. Modify the connection string in the ‘connectionString’ element to allow connection to the P2P Data Store database.
2. Modify the logging level in the ‘level’ element to “DEBUG”, “INFO” or “WARNING” depending on the level of tracing required to diagnose issues in the environment. The logging level is set as “DEBUG” as default.

4.6 P2P Application Server Code Installation

From the “P2P_AppServer\binaries” folder that was copied to the application server:

1. Ensure that the configuration files that were edited in the above step are present.

2. Copy all files and directories under the “P2P_AppServe\binaries” folder into the “D:\Projects\P2P_TEST\Build” folder (or to your customised folder location) on the application server. Ensure that the modified web.config file is placed with the *.svc files as below.

 bin	File folder
 HIPS.P2P.Service.DirectoryConfigurationService.svc	WCF Web Service
 HIPS.P2P.Service.DirectorySynchronisationService.svc	WCF Web Service
 HIPS.P2P.Service.LogService.svc	WCF Web Service
 HIPS.P2P.Service.MessageDeliveryService.svc	WCF Web Service
 HIPS.P2P.Service.MessagePublishingService.svc	WCF Web Service
 HIPS.P2P.Service.MessageReceiptService.svc	WCF Web Service
 HIPS.P2P.Service.ProviderIndividualDirectoryService.svc	WCF Web Service
 HIPS.P2P.Service.ProviderLocationDirectoryService.svc	WCF Web Service
 HIPS.P2P.Service.ProviderOrganisationDirectoryService.svc	WCF Web Service
 HIPS.P2P.Service.ReferenceDataService.svc	WCF Web Service
 HIPS.P2P.Service.ResponseDeliveryService.svc	WCF Web Service
 HIPS.P2P.Service.ResponseReceiptService.svc	WCF Web Service
 HIPS.P2P.Service.SubscriptionService.svc	WCF Web Service
 log4net.xml	XML File
 packages.config	CONFIG File
 Web.config	CONFIG File

3. Ensure that there are 13 SVC files, a log4net.xml file, packages.config and a web.config file in this folder.
4. Ensure that there are 43 DLL files and 1 XML files under the “bin” folder.

****At this time it is reasonable to perform an iisreset while logged into a command prompt as an Administrator.**

4.7 Confirm P2P Installation

4.7.1 Confirm Available Web Services

In a web browser, navigate to the following URLs and check that the page “You have created a service” appears. If using HTTPS then update the URLs below to use https and the port number the secure connection was created on.

For HTTP

- http://servername:61500/P2PServer_TEST/HIPS.P2P.Service.DirectoryConfigurationService.svc
- http://servername:61500/P2PServer_TEST/HIPS.P2P.Service.DirectorySynchronisationService.svc
- http://servername:61500/P2PServer_TEST/HIPS.P2P.Service.LogService.svc
- http://servername:61500/P2PServer_TEST/HIPS.P2P.Service.MessageDeliveryService.svc
- http://servername:61500/P2PServer_TEST/HIPS.P2P.Service.MessagePublishingService.svc
- http://servername:61500/P2PServer_TEST/HIPS.P2P.Service.MessageReceiptService.svc
- http://servername:61500/P2PServer_TEST/HIPS.P2P.Service.ProviderIndividualDirectoryService.svc
- http://servername:61500/P2PServer_TEST/HIPS.P2P.Service.ProviderLocationDirectoryService.svc

- http://servername:61500/P2PServer_TEST/HIPS.P2P.Service.ProviderOrganisationDirectoryService.svc
- http://servername:61500/P2PServer_TEST/HIPS.P2P.Service.ReferenceDataService.svc
- http://servername:61500/P2PServer_TEST/HIPS.P2P.Service.ResponseDeliveryService.svc
- http://servername:61500/P2PServer_TEST/HIPS.P2P.Service.ResponseReceiptService.svc
- http://servername:61500/P2PServer_TEST/HIPS.P2P.Service.SubscriptionService.svc

5. SMD Front End and Decrypter

The table below describes a number of deployment variables representing implementation or environment-specific items that will be referenced throughout this section. Where possible the value for the “Value” column in the table should be determined prior to deployment execution.

Deployment Variable	Description	Suggested Value
HIPS SMD Decrypter Server	Server node that hosts the IIS instance into which the HIPS Decrypter application will be deployed.	
HIPS SMD Decrypter App Pool	IIS application pool used as a thread pool by the HIPS SMD Decrypter application.	DecrypterAppPool_TEST
HIPS SMD Decrypter Site	IIS web site used to host the HIPS SMD Decrypter application.	Decrypter_TEST
HIPS SMD Decrypter Physical Path	File system folder containing the HIPS SMD Decrypter web site components.	D:\Projects\Decrypter_TEST
HIPS SMD Decrypter Service Account	Active Directory domain service account used as the identity of the HIPS SMD Decrypter App Pool.	
HIPS SMD Front-End Server	Server node that hosts the IIS instance into which the HIPS Front-End application will be deployed.	
HIPS SMD Front-End App Pool	IIS application pool used as a thread pool by the HIPS SMD Front-End application.	SMDAppPool_TEST
HIPS SMD Front-End Site	IIS web site used to host the HIPS SMD Front-End application.	SMD_TEST
HIPS SMD Front-End Web Site Folder	File system folder containing the HIPS SMD Front-End web site components.	D:\Projects\SMD_TEST
HIPS SMD Front-End Service Account	Active Directory domain service account used as the identity of the HIPS SMD Front-End App Pool.	
HIPS SMD Front-End Data Storage Folder	File system folder in which the HIPS SMD Front-End will store secure messages, transport responses and errors.	D:\Secure Messaging
HIPS SMD Front-End Server Certificate	SSL Server Certificate used to host SMD services on the HIPS SMD Front-End. This must be a commercial SSL certificate or else every external party must configure peer trust.	

5.1 SMD Application Server Operating System Preparation

The following features are expected to be configured and available on the HIPS **SMD Decrypter Server** and HIPS **SMD Front-End Server** (via the Web Server role configured through Server Manager):

- Web Server
 - Common HTTP Features
 - Static Content
 - Default Document
 - Directory Browsing
 - HTTP Errors

- HTTP Redirection
- Application Development
 - ASP.NET
 - .NET Extensibility
- Health and Diagnostics
 - HTTP Logging
 - Logging Tools
 - Request Monitor
 - Tracing
- Security
 - Basic Authentication
 - Windows Authentication
 - Client Certificate Mapping Authentication
 - IIS Client Certificate Mapping Authentication
 - URL Authorisation
 - Request Filtering
 - IP and Domain Restrictions
- Performance
 - Static Content Compression
 - Dynamic Content Compression
- Management Tools
 - IIS Management Console
 - IIS Management Scripts and Tools
 - Management Service

5.1.1 Service Accounts

The HIPS SMD components use a service account as the identity of the HIPS **SMD Decrypter App Pool** and HIPS **SMD Server App Pool** IIS application pools and to connect to resources such as the file system folder where secure messages are stored.

These service accounts will be referred to as the HIPS **SMD Service Accounts**.

5.1.2 File System Folders

This section provides instructions for creating required file system folders and permissions on or accessible from the HIPS **SMD Front-End Server** in the target environment.

1. In an appropriate location on the server create a new folder “Secure Messaging”.
2. Under the “Secure Messaging” folder create the following folder structure:
 - “Error Messages”
 - “Archive”
 - “Sealed Messages”
 - “Archive”
 - “Error”
 - “Inbox”
 - “Transport Responses”

- “Archive”
 - “Inbox”
3. Edit permissions for the Secure Messaging folder
 4. Add the HIPS **SMD Front-End Service Account**
 5. Set the “Full Control” permission for the service account to “Allow”

5.2 P2P Application Server Site Installation

This section provides instructions for deploying web components to the servers in the target environment.

5.2.1 SMD Decrypter Server

The following steps should be performed via a Remote Desktop session connected to the HIPS **SMD Decrypter Server**.

1. Open Computer Management.
 - a. Ensure the HIPS **SMD Decrypter Service Account** is a member of the local “IIS_USRS” group.
2. Open File Explorer.
 - a. Copy the contents of the “SMD_Decrypter” folder in the Core Software Package of the Deployment Package to a suitable filesystem location on the HIPS **SMD Decrypter Server**, for example “D:\Projects\Decrypter_TEST”. This folder will be referred to as the HIPS **SMD Decrypter Site Folder**.
 - b. Ensure the HIPS **SMD Decrypter Service Account** has **Full Control** permissions to the folder and its contents.
3. Open IIS Manager.
 - a. Review the list of application pools. If not previously created, create a new application pool to be utilised by the HIPS SMD Decrypter component.
 - i. Name: HIPS **SMD Decrypter App Pool**
 - ii. General:
 1. .NET Framework Version: v4.0
 2. Managed Pipeline Mode: Integrated
 - iii. Process Model:
 1. Identity: HIPS **SMD Decrypter Service Account**
 2. Load User Profile: True
 - iv. Recycling:
 1. Regular Time Interval (minutes): 10080
 - b. Create a new web site to host the HIPS SMD Decrypter components.
 - i. Site Name: HIPS **SMD Decrypter Site**
 - ii. Physical Path: HIPS **SMD Decrypter Site Folder**
 - iii. Application Pool: HIPS **SMD Decrypter App Pool**
 - iv. Bindings: HTTP and/or HTTPS, ports & host headers as desired
 - v. Logging:
 1. Enabled
 2. Schedule: Daily
 3. Use Local Time: True
 - vi. Authentication:

1. Anonymous: Enabled
 2. All others: Disabled
- vii. Configuration Editor
 1. system.webServer/serverRuntime/uploadReadAheadSize: 2147483647
- c. Ensure the application pool and web site are started.
4. Open Windows Firewall.
 - a. Create rules to allow inbound connections to the ports utilised by the previously created web site.

5.2.2 SMD Front-End Server

The following steps should be performed via a Remote Desktop session connected to the HIPS **SMD Front-End Server**.

1. Open Computer Management.
 - a. Ensure the HIPS **SMD Front-End Service Account** is a member of the local "IIS_USRS" group.
2. Open File Explorer.
 - a. Copy the contents of the "SMD_AppServer" folder in the Core Software Package of the Deployment Package to a suitable filesystem location on the HIPS **SMD Front-End Server**, for example "D:\Projects\SMD_TEST". This folder will be referred to as the HIPS **SMD Front-End Site Folder**.
 - b. Ensure the HIPS **SMD Front-End Service Account** has **Full Control** permissions to the folder and its contents.
3. Open IIS Manager.
 - a. Review the list of application pools. If not previously created, create a new application pool to be utilised by the HIPS SMD Front-End component.
 - i. Name: HIPS **SMD Front-End App Pool**
 - ii. General:
 1. .NET Framework Version: v4.0
 2. Managed Pipeline Mode: Integrated
 - iii. Process Model:
 1. Identity: HIPS **SMD Front-End Service Account**
 2. Load User Profile: True
 - iv. Recycling:
 1. Regular Time Interval (minutes): 10080
 - b. Create a new web site to host the HIPS SMD Decrypter components.
 - i. Site Name: HIPS **SMD Front-End Site**
 - ii. Physical Path: HIPS **SMD Front-End Site Folder**
 - iii. Application Pool: HIPS **SMD Front-End App Pool**
 - iv. Bindings: HTTPS, ports & host headers as desired. Select the HIPS **SMD Front-End Server Certificate**.
 - v. Logging:
 1. Enabled
 2. Schedule: Daily
 3. Use Local Time: True
 - vi. Authentication:

1. All: Disabled
 2. Windows Authentication: Enabled if desired
- vii. SSL Settings
 1. Require SSL: Enabled
 2. Client Certificates: Require
- viii. Configuration Editor
 1. system.webServer/serverRuntime/uploadReadAheadSize: 2147483647
- c. Ensure the application pool and web site are started.
4. Open Windows Firewall.
 - a. Create rules to allow inbound connections to the ports utilised by the previously created web site.

5.3 NASH Certificates Installation

This section provides instructions for deploying digital certificates to the servers in the target environment.

5.3.1 SMD Decrypter Server

The following steps should be performed via a Remote Desktop session connected to the HIPS **SMD Decrypter Server**.

1. Open the Microsoft Management Console (MMC) and select the Certificates snap-in for the local computer.
2. Highlight the Personal node and import the **NASH HPI-O Certificates** for Payload Encryption.
3. If the Client Certificate that will be used for connection to the HIPS **SMD Front-End Server** is not one of the **NASH HPI-O Certificates**, highlight the Personal node and import the Client Certificate.
4. Highlight the “Trusted Root Certification Authorities” node and import the “Medicare Australia Root Certification Authority” certificate.
5. If the root certification authority of the HIPS **SMD Front-End Server Certificate** is not already present in the Trusted Root Certification Authorities list, then import its root authority.

5.3.2 SMD Front-End Server

The following steps should be performed via a Remote Desktop session connected to the HIPS **SMD Front-End Server**.

1. Open the Microsoft Management Console (MMC) and select the Certificates snap-in for the local computer.
2. Highlight the Personal node and import or generate the HIPS **SMD Front-End Server Certificate**.
3. Highlight the Personal node and import the **NASH Certificate** that will be used for connection to external SMD services.
4. Highlight the “Trusted Root Certification Authorities” node and import the “Medicare Australia Root Certification Authority” certificate.
5. Highlight the “Intermediate Certification Authorities” node and import the “Medicare Australia Organisation Certification Authority” certificate.

5.4 SMD Web Configuration Setup

This section provides instructions for configuring the HIPS SMD components prior to first use.

5.4.1 SMD Decrypter Server

Perform the following steps via a Remote Desktop session connected to the HIPS **SMD Decrypter Server**.

1. Open File Explorer.
 - a. Browse to the HIPS **SMD Decrypter Site Folder** in the filesystem of the HIPS **SMD Decrypter Server**.
 - b. Open the Web.config file in Notepad.
 - c. Locate and modify the following configuration settings as relevant to the target environment:
 - i. *system.serviceModel/client*: Ensure the value for the *address* attribute of child *endpoint* elements reflects the target environment. In particular, ensure "https://**host:port/site**" is replaced with the protocol, host, port and site (where relevant) of the SealedMessageRetrieval endpoint provided by the HIPS **SMD Front-End Application Server**.
 - ii. *System.serviceModel/behaviours/endpointBehaviors*: Ensure the value for the *findValue* attribute of child *clientCertificate* element reflects the target environment. This must be the thumbprint of a client certificate that will be used to authenticate connections to the HIPS **SMD Front-End Server**.

NOTE: There is a hidden spacebar character in the first of the certificate number if you copy and paste it from certificate details. Please remove this hidden character by using Backspace key.
 - iii. *secureMessagingGroup/certificateConfigSection/internalPayloadEncryptionCertificates*: Modify or add child elements of as required to represent the list subject key identifiers for certificates that may be used to decrypt the payload of a received message.
 - d. Save and close the file.
2. Open Command Prompt (as Administrator).
 - a. Execute the following command: iisreset

5.4.2 SMD Front-End Server

Perform the following steps via a Remote Desktop session connected to the HIPS **SMD Front-End Server**.

1. Open File Explorer.
 - a. Browse to the HIPS **SMD Front-End Site Folder** in the filesystem of the HIPS **SMD Front-End Server**.
 - b. Open the Web.config file in Notepad.
 - c. Locate and modify the following configuration settings as relevant to the target environment:
 - i. *system.serviceModel/behaviours/endpointBehaviors*: Ensure the value for the *findValue* attribute of child *clientCertificate* element reflects the target environment. This must be the thumbprint of a client certificate that will be used to authenticate connections to external SMD services.

NOTE: There is a hidden spacebar character in the first of the certificate number if you copy and paste it from certificate details. Please remove this hidden character by using Backspace key.
 - ii. *secureMessagingGroup/healthcareIdentifierConfigSection/internalOrganisationIdentifiers*: Modify or add child elements as required to represent the list of HPI-O's that may invoke services as an internal caller.
 - iii. *secureMessagingGroup/certificateConfigSection/internalOrganisationClientCertificates*: Modify or add child elements as required to represent the client certificates that will be used by the HIPS **P2P Application Server** and the HIPS **SMD Decrypter Server** to connect to this server.
 - iv. *secureMessagingGroup/sealedMessageConfigSection*: Modify the *receiveFolder*, *archiveFolder* and *errorFolder* to match folders within the HIPS **SMD Front-End Data Storage Folder**.

- v. *secureMessagingGroup/transportResponseConfigSection*: Modify the *receiveFolder* and *archiveFolder* to match folders within the HIPS **SMD Front-End Data Storage Folder**.
 - vi. *secureMessagingGroup/errorServiceConfigSection*: Modify the *errorFolder* and *archiveFolder* attributes to match folders within the HIPS **SMD Front-End Data Storage Folder**.
 - vii. *secureMessagingGroup/loggingConfigSection*: Modify the *logFileDirectory* attribute to match a folder within the HIPS **SMD Front-End Data Storage Folder**.
 - d. Save and close the file.
2. Open Command Prompt (as Administrator).
 - a. Execute the following command: iisreset

5.5 Confirm SMD Decrypter and SMD Front-End Installation

Perform the following steps to verify the correct behaviour of the HIPS SMD Front-End and HIPS SMD Decrypter components.

1. Open a web browser (e.g. Internet Explorer).
2. Browse to each of the HIPS SMD Front-End service endpoints.
3. Provide a valid authentication certificate when prompted.
4. Verify the service information is displayed.
5. Browse to the HIPS SMD Decrypter service endpoint.
6. Provide valid authentication credentials if prompted.
7. Verify the service information is displayed.

5.6 Rollback SMD Decrypter and SMD Front-End

In the case that rollback is required, perform the following steps in order to remove the components previously deployed via the instructions above.

1. Web Site:
 - a. Windows Firewall:
 - i. Remove inbound rules.
 - b. IIS Manager:
 - i. Remove HIPS **SMD Front-End Site**
 - ii. Remove HIPS **SMD Front-End App Pool**
 - iii. Remove HIPS **SMD Decrypter Site**
 - iv. Remove HIPS **SMD Decrypter App Pool**
 - c. File Explorer:
 - i. Delete HIPS **SMD Front-End Site Folder**
 - ii. Delete HIPS **SMD Decrypter Site Folder**
 - d. Computer Management:
 - i. Remove HIPS **SMD Front-End Service Account** from "IIS_USRS" group.
 - ii. Remove HIPS **SMD Decrypter Service Account** from "IIS_USRS" group.
2. Data Storage:
 - a. Delete HIPS **SMD Front-End Data Storage Folder**
3. Credentials:

- a. Remove HIPS **SMD Front-End Service Account**
- b. Remove HIPS **SMD Decrypter Service Account**
- c. Remove HIPS **SMD Front-End Server Certificate**
- d. Remove **Medicare Root Certificate**
- e. Remove **Medicare Intermediate Certificate (OCA)**
- f. Remove **NASH HPI-O Certificates**

Appendix A P2P Application Server Configuration Explanation

Most application-wide configuration options are held in the Web.config file in the directory “D:\Projects\P2P_TEST\Build”.

Section	Option Name	Suggested Value	Description
Connection String	Data Source	<i>Name of SQL server</i>	P2P will attempt to connect to this SQL server.
	Initial Catalog	P2PDataStoreTest	P2P will use the database with this name.
	Integrated Security	SSPI	If set to SSPI as recommended, then HIPS will use the IIS application pool's Windows account credentials for authentication to the database. Otherwise, and this is not recommended, set to False and provide a User ID and Password. This will only work if SQL Server Authentication is enabled on the server.
Directory Configuration Service	baseAddress	net.tcp://servername: 61000 /	The Directory Configuration service will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername: 61500 /DirectoryConfigurationService/	The Directory Configuration service will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername: 61443 /DirectoryConfigurationService/	The Directory Configuration service will be accessible using HTTPS protocol at this URL.
Directory Synchronisation Service	baseAddress	net.tcp://servername: 61000 /	The Directory Synchronisation service will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername: 61500 /DirectorySynchronisationService/	The Directory Synchronisation service will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername: 61443 /DirectorySynchronisationService/	The Directory Synchronisation service will be accessible using HTTPS protocol at this URL.

Section	Option Name	Suggested Value	Description
Provider Individual Directory Service	baseAddress	net.tcp://servername: 61000 /	The Provider Individual Directory Service will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername: 61500 /ProviderIndividualDirectoryService/	The Provider Individual Directory Service will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername: 61443 /ProviderIndividualDirectoryService/	The Provider Individual Directory Service will be accessible using HTTPS protocol at this URL.
Provider Organisation Directory Service	baseAddress	net.tcp://servername: 61000 /	The Provider Organisation Directory Service will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername: 61500 /ProviderOrganisationDirectoryService/	The Provider Organisation Directory Service will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername: 61443 /ProviderOrganisationDirectoryService/	The Provider Organisation Directory Service will be accessible using HTTPS protocol at this URL.
Provider Location Directory Service	baseAddress	net.tcp://servername: 61000 /	The Provider Location Directory Service will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername: 61500 /ProviderLocationDirectoryService/	The Provider Location Directory Service will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername: 61443 /ProviderLocationDirectoryService/	The Provider Location Directory Service will be accessible using HTTPS protocol at this URL.
Message Delivery Service	baseAddress	net.tcp://servername: 61000 /	The Message Delivery Service will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername: 61500 /MessageDeliveryService/	The Message Delivery Service will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername: 61443 /MessageDeliveryService/	The Message Delivery Service will be accessible using HTTPS protocol at this URL.
Message Receipt Service	baseAddress	net.tcp://servername: 61000 /	The Message Receipt Service will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername: 61500 /MessageReceiptService/	The Message Receipt Service will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername: 61443 /MessageReceiptService/	The Message Receipt Service will be accessible using HTTPS protocol at this URL.

Section	Option Name	Suggested Value	Description
Message Publishing Service	baseAddress	net.tcp://servername: 61000 /	The Message Publishing Service will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername: 61500 /MessagePublishingService/	The Message Publishing Service will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername: 61443 /MessagePublishingService/	The Message Publishing Service will be accessible using HTTPS protocol at this URL.
Reference Data Service	baseAddress	net.tcp://servername: 61000 /	The Reference Data Service will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername: 61500 /ReferenceDataService/	The Reference Data Service will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername: 61443 /ReferenceDataService/	The Reference Data Service will be accessible using HTTPS protocol at this URL.
Subscription Service	baseAddress	net.tcp://servername: 61000 /	The Subscription Service will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername: 61500 /SubscriptionService/	The Subscription Service will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername: 61443 /SubscriptionService/	The Subscription Service will be accessible using HTTPS protocol at this URL.

In addition to the web.config setting P2P stores application-wide settings in the P2P Data Store p2p.Settings Table. The following is the settings required to be added to this table (populated when the 05_P2P_Data.sql is run see section [4.1.3](#)). The settings highlighted below are required to be updated with the correct values before the application is executed.

Setting	Default Value	Description
HPI-I validity period (hours)	24	The number of hours the HPI-I is validated for making reference to the LastValidatedDate before re-validation occurs.
HPI-O validity period (hours)	24	The number of hours the HPI-O is validated for making reference to the LastValidatedDate before re-validation occurs.
Default Responsible User Identifier	'default'	The user ID of the authorised employee responsible for background operations of the P2P application.

Setting	Default Value	Description
Default Responsible User Name	'default'	The name of the authorised employee responsible for background operations of the P2P application.
Default Responsible User Accessing HPI-O	'default'	The HPI-O of the organisation that employs the authorised employee responsible for background operations of the P2P application. This must correspond to a record in the p2p.AccessingOrganisation table.
Message Publishing Interval (seconds)	60	The scheduled message publishing interval in seconds.
Response Receipt Interval (seconds)	60	The scheduled response receipt interval in seconds.
Response Delivery Interval (seconds)	60	The scheduled response delivery interval in seconds.
Response Delivery Timeout Period (seconds)	86400	The timeout period for a response delivery in seconds.
Message Publishing Target Persistence Path	Published Messages path	A valid file path where the published messages are stored. The HIPS AD Service Account user will require write access to this path.
Message Delivery Interval (seconds)	60	The scheduled message delivery interval in seconds.
IHI validation flag	True	Flags whether the patient demographics and IHI should be validated against the HI Service.
Message Receipt Service Interval (seconds)	60	The scheduled message receipt service interval in seconds.
Message Receipt Service Limit (number of messages to retrieve)	5	The maximum number of messages the message receipt service limit retrieves.
External URL for Transport Response Delivery service endpoint	https://.../TransportResponseDelivery.svc	The external URL required for the transport response delivery service endpoint.
Error Message Interval (seconds)	60	The scheduled log service interval in seconds
Error Message Limit (number of error messages to retrieve)	5	The maximum number of error messages to retrieve from the Log Service.
Audit Smd Request Xml	True	Flags whether all SMD Requests xml should be stored for auditing purposes.
Audit Smd Response Xml	True	Flags whether all SMD Responses xml should be stored for auditing purposes.

Setting	Default Value	Description
Audit Neps Request Xml	True	Flags whether all NEPS Requests xml should be stored for auditing purposes.
Audit Neps Response Xml	True	Flags whether all NEPS Responses xml should be stored for auditing purposes.
Known Valid HPI-Os (comma separated)		A list of known valid HPI-Os. This allows use of a limited number of HPI-Os that are known to be valid but not present in the Healthcare Provider Directory (HPD) in the HI Service
Max Retry Count	1440	The maximum retry count for a Sealed Message Delivery.
Reference Data Interval (seconds)	3600	The scheduled reference data service interval in seconds.
Synchronisation Interval (seconds)	60	The scheduled directory synchronisation service interval in seconds.
Subscription Changes Batch Size	50	The end batch size used when retrieving the NEPS Subscription Changes.

