



Australian Government
Australian Digital Health Agency



HIPS

Initial and Clean Installation Guide (UI)

22 January 2019 v7.0
Approved for external use

Australian Digital Health Agency ABN 84 425 496 912, Level 25, 175 Liverpool Street, Sydney, NSW 2000
Telephone 1300 901 001 or email help@digitalhealth.gov.au
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 © 2019 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.

OFFICIAL

Document information

Key information

Owner	Executive General Manager Innovation and Development
Contact for enquiries	Australian Digital Health Agency Help Centre
Phone	1300 901 001
Email	help@digitalhealth.gov.au

Product or document version history

Product or document 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2.0.1		Unpublished updates.
2.0.2		
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.
6.1.1	March 2018	See release note for details of changes and bug fixes.
6.1.2	May 2018	See release note for details of changes and bug fixes.
6.1.3	July 2018	See release note for details of changes and bug fixes.
6.1.4	September 2018	See release note for details of changes and bug fixes.
6.2	Unpublished	See release note for details of changes and bug fixes.
6.2.1		
7.0.0	December 2018	See release note for details of changes and bug fixes.

Table of contents

1	Introduction	5
1.1	Purpose	5
1.2	Scope.....	5
1.3	Assumptions.....	5
1.4	Definitions and Acronyms.....	7
2	Target Environment	8
2.1	Client Operating Environment	8
2.2	Deployment Variables.....	9
2.3	Infrastructure Roles	10
2.4	Security Configuration Recommendations	11
2.4.1	HTTPS Binding.....	11
2.4.2	Disable RC4.....	11
2.4.3	Disable SSLv3	12
2.5	Service Accounts	13
3	Deployment Instructions.....	14
3.1	Deployment Summary	14
3.2	Prerequisites	14
3.3	Database Objects & Data	14
3.4	Web Site.....	17
3.4.1	Configure Installation Artefacts.....	17
3.4.2	Execute Installation Scripts.....	17
3.4.3	Web Site Self-Signed SSL Certificate.....	18
3.5	Configuration	19
4	Product Verification Testing	33
5	Rollback or Remove HIPS-UI.....	35
Appendix A	log4net Configuration	36

1 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 User Interface (UI) component interfaces with the HIPS-Core Component via SOAP Web Services. More detail on the HIPS-Core Component can be found in the *HIPS Release 7.0 – Module Guide (Core)* document.

1.1 Purpose

This document provides instructions for deploying a specific packaged release of the HIPS-UI Web product into a target implementation environment.

It can be used by health facilities to install the HIPS-UI Web application into a targeted environment.

This document describes the prerequisites and steps that are required for the HIPS-UI Web application to be installed for the first time (clean installation).

1.2 Scope

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

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

Specifically, the document covers the following:

- The resources, responsibilities and access required to deploy the release.
- The intended target implementation environment and any environment specific configuration items.
- Any assumptions that may affect the deployment.
- Detailed instructions for deploying the release into the target environment and for performing product verification testing.
- Rollback steps in the case that the deployment is unsuccessful.

1.3 Assumptions

The deployment instructions within this document assume the following:

- The facility installing the HIPS-UI Web application has appropriate software versions and server operating systems.
- The user following roles and required access exist within the organisation:

Resource	Role	Access
Server Administrator	Implementation and configuration of server and operating system requirements.	“Administrator” access to the operating system on each target server node.
Database Administrator	Deployment of required database objects and data and subsequent configuration tasks.	“sysadm” access to the target SQL Server instance on the HIPS-UI Web Database Server node.
Web Administrator	Deployment of required web site components and subsequent configuration tasks.	“Administrator” access to the operating system on the HIPS-UI Web Application Server node.
Product Owner	Product verification testing following deployment.	Member of a Role granted access to the HIPS-UI and associated hospital (as per section 3.5 Configuration)

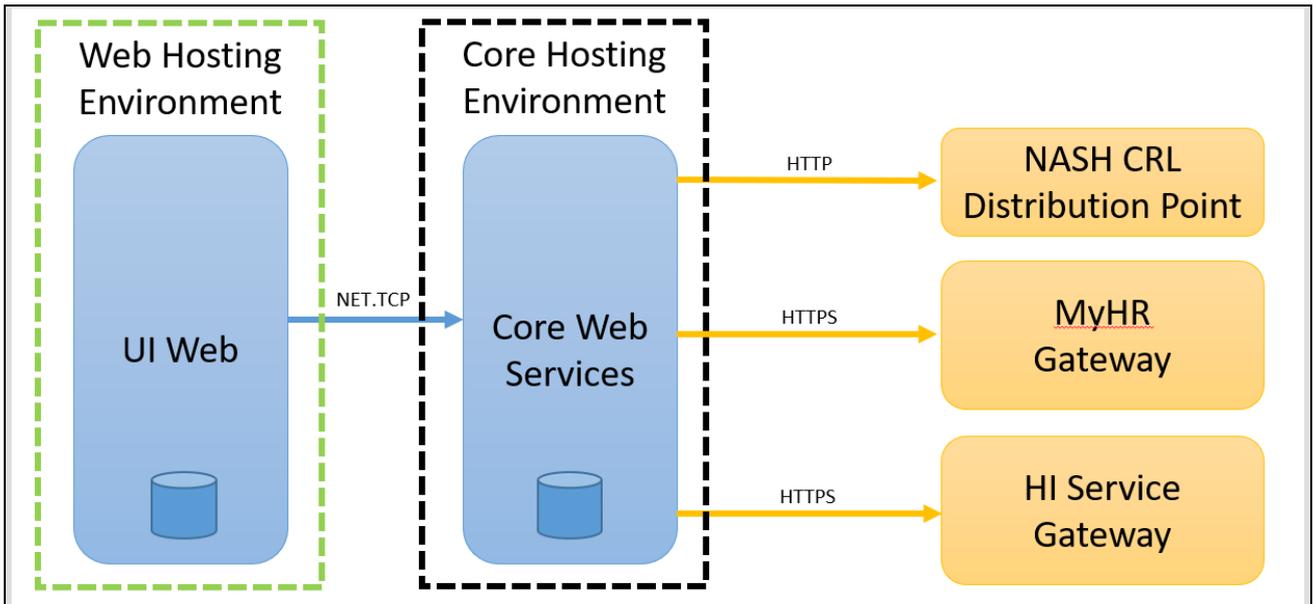
- The HIPS-UI Web product has not been previously deployed to the target environment, or if it has been previously deployed then it has been removed following the instructions provided in [Rollback](#).
- The deployment instructions are performed by suitably trained personnel with appropriate privileges to perform each activity, as described in the table above.
- The target environment has been built and configured as described in [Target Environment](#).
- The relevant release of HIPS-Core has previously been deployed, configured and verified on the **HIPS-Core Application Server**, as described in [Target Environment](#).
- Domain firewall rules allow inbound connections to the **HIPS-Core Application Server** from the **HIPS-UI Web Application Server**.

1.4 Definitions and Acronyms

Item	Definition
UI	User Interface
CCA	Conformance and Compliance Acceptance
HTTP	Hypertext Transfer Protocol
HIPS	Healthcare Identifier and PCEHR System
HTML	Hypertext Markup Language
PDF	Portable Document Format
RTF	Rich Text Format
IIS	Internet Information Server
URL	Uniform Resource Locator. Address of a web page.
IP	Internet Protocol. Protocol by which data is sent from one computer to another on a network.
ASP	Active Server Pages. A web page that includes one or more scripts that are processed on a Microsoft web server before being sent to the user.
SQL	Structured Query Language. A programming language used to manage data in a relational database management system.
ELMAH	Error Logging Modules and Handlers. Errors encountered during the processing of the web pages are handled and logged with this tool.
AD	Active Directory
HPI-I	Health Provider Individual Identifier
HPI-O	Health Provider Organisation Identifier

2 Target Environment

This installation guide covers the “Web Hosting Environment”, consisting of the HIPS-UI Web Server, as illustrated in the following diagram.



2.1 Client Operating Environment

The following constraints are assumed to be placed upon the operating environment of the **client system** from which end users will utilise the My Health Record System Web Viewer:

- Supported client devices:
 - PC, laptop, tablet running a supported operating system natively
- Supported client platforms (operating system):
 - Windows 8+, Windows 10
- Supported client web browsers:
 - Microsoft Internet Explorer 11
 - Microsoft Edge 40
 - Google Chrome 60
 - Mozilla Firefox 55
- Configuration required to meet CCA conformance requirements for rendering systems (CDAR_RS_01):
 - Web browser configuration:
 - Printing:

- The window title must be printed as the page header on every printed page.
- The page footer must include the "Page N of T" marker on every printed page.
- Background colours and images must be printed.
- Content must be shrunk to fit the printed page.
- The web browser must not allow users to override the presentation and style of documents rendered as HTML (e.g. via "developer tools").
- Client system configuration:
 - The client system must have appropriate software installed in order to open and view document attachments including HTML, PDF, RTF and Plain Text.
 - The client system's screen resolution must be at least 1024x768 pixels.

2.2 Deployment Variables

The table below describes a number of deployment variables representing implementation or environment specific items that will be referenced throughout this document. Where possible the value for the "Value" column in the table should be determined prior to deployment execution. It is recommended the installer completes this table and uses it for reference throughout the installation.

Deployment Variable	Description	Value
HIPS-UI Web Database Server	Server node that hosts the SQL Server database engine instance into which the HIPS-UI Web database will be deployed.	
HIPS-UI Web Database	Database hosted by the HIPS-UI Web Database Server into which HIPS-UI Web database objects and data will be deployed.	
HIPS-UI Web Application Server	Server node that hosts the IIS instance into which the HIPS-UI Web web site components will be deployed.	
HIPS-UI Web App Pool	IIS application pool used as a thread pool by the HIPS-UI Web Site.	
HIPS-UI Web Site	IIS web site used to host the HIPS-UI Web web site components.	
HIPS-UI Web Site Folder	Filesystem folder containing the HIPS-UI Web web site components.	
HIPS-UI Web Service Account	Active Directory domain service account used as the identity of the IIS application pool.	
HIPS-UI Web Domain Name	Active Directory domain name used to authenticate and lookup user information.	
HIPS-UI Web Privacy Policy Link	URL to an internal Privacy Policy html page if available. Can be left blank and a link will not appear in UI.	
HIPS-Core Application Server	Server node that hosts the HIPS-Core product to be utilised by the HIPS-UI Web product.	
HIPS-Core Endpoint Base	Base endpoint at which HIPS-Core services are provided, in format protocol://host:port/.	

2.3 Infrastructure Roles

The table below lists the roles of the infrastructure nodes to which the product will be deployed in a target environment. Further guidance on the allocation and configuration of these roles may be found in the *HIPS 7.0.0 Topology and Configuration Guide*. The table also lists prerequisite components that are expected to have been installed and configured on each node.

Infrastructure Role	Description	Prerequisites
HIPS-UI Web Database Server	Server node that hosts the SQL Server database engine instance into which the HIPS-UI Web database, database objects and data will be deployed.	SQL Server 2008 R2+ Database Engine
HIPS-UI Web Application Server	Server node that hosts the IIS instance into which the HIPS-UI Web web site components will be deployed.	Internet Information Services 7.5+ .NET Framework 4.5.2+
HIPS-Core Application Server	Server node that hosts the HIPS-Core product to be utilised by the HIPS-UI Web product.	HIPS-Core 7.0.0

IMPORTANT NOTE:

Due to the use of memory-based caching by the HIPS-UI Web product, it is recommended that it not be deployed in a “web farm” (e.g. a network load balancing (NLB) cluster) where multiple distinct servers may service a particular session. This does not apply if the load balancer is configured for sticky sessions.

2.4 Security Configuration Recommendations

2.4.1 HTTPS Binding

It is strongly recommended that HIPS-UI is configured such that end-user web browsers connect to HIPS UI over HTTPS. Depending on the server topology, the IIS instance that hosts the HIPS-UI web site components may handle HTTPS itself, or a load balancer or reverse proxy in front of one or more IIS instances may handle HTTPS and proxy web requests back to the IIS instances over either HTTPS or an unencrypted HTTP channel.

The following recommendations regarding disabling RC4 and SSLv3 apply to the infrastructure that terminates the HTTPS connection from the end-user browser. Where that infrastructure is hosted on non-Microsoft platforms, refer to the vendor documentation for equivalent configuration steps.

2.4.2 Disable RC4

Microsoft recommends TLS1.2 is enabled in their services and to disable RC4. Microsoft recommends TLS1.2 with AES-GCM as a more secure alternative which will provide similar performance. Further information on recommendations to disable RC4 can be found at:

<http://blogs.technet.com/b/srd/archive/2013/11/12/security-advisory-2868725-recommendation-to-disable-rc4.aspx>

An excerpt from this article explain how to completely disable RC4 is below.

Microsoft strongly encourages customers to evaluate, test and implement the options for disabling RC4 below to increase the security of clients, servers and applications. Microsoft recommends enabling TLS1.2 and AES-GCM. Clients and servers running on Windows with custom SSL/TLS implementations, such as, Mozilla Firefox and Google Chrome will not be affected by changes to SChannel.

How to Completely Disable RC4

Clients and Servers that do not wish to use RC4 cipher suites, regardless of the other party's supported ciphers, can disable the use of RC4 cipher suites completely by setting the following registry keys. In this manner any server or client that is talking to a client or server that must use RC4, can prevent a connection from happening. Clients that deploy this setting will not be able to connect to sites that require RC4 while servers that deploy this setting will not be able to service clients that must use RC4.

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128]
```

```
"Enabled"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128]
```

```
"Enabled"=dword:00000000
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128]
```

```
"Enabled"=dword:00000000
```

2.4.3 Disable SSLv3

A vulnerability in SSLv3 has emerged named POODLE (Padding Oracle On Downgraded Legacy Encryption) which can allow attackers to steal “encrypted” data, such as HTTP cookies. It is recommended to disable older versions of SSL/TLS to prevent a POODLE attack.

See the following support article from Microsoft on how to disable SSLv3 in IIS:

<https://technet.microsoft.com/en-us/library/security/3009008.aspx?f=255&MSPPError=-2147217396>

An excerpt from this article below explains the steps to disable SSLv3 on the IIS Server:

Disable SSL 3.0 in Windows

For Server Software

You can disable support for the SSL 3.0 protocol on Windows by following these steps:

Click Start, click Run, type regedt32 or type regedit, and then click OK.

In Registry Editor, locate the following registry key:

```
HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server
```

Note If the complete registry key path does not exist, you can create it by expanding the available keys and using the New -> Key option from the Edit menu.

On the Edit menu, click Add Value.

In the Data Type list, click DWORD.

In the Value Name box, type Enabled, and then click OK.

Note If this value is present, double-click the value to edit its current value.

In the Edit DWORD (32-bit) Value dialogue box, type 0.

Click OK. Restart the computer.

Note This workaround will disable SSL 3.0 for all server software installed on a system, including IIS.

Note After applying this workaround, clients that rely only on SSL 3.0 will not be able to communicate with the server.

2.5 Service Accounts

The HIPS-UI Web product utilises an Active Directory domain service account as the identity the **HIPS-UI Web App Pool** IIS application pool and to connect to remote resources such as databases and HIPS-Core.

This service account will be referred to as the **HIPS-UI Web Service Account**.

3 Deployment Instructions

3.1 Deployment Summary

The table below defines the key activities for deploying the product components and estimated timing for each activity. It is assumed that each activity is completed sequentially, with each later activity dependent upon the successful completion of earlier activities.

Activity	Description	Duration (Hours)
Prerequisites	Execution of prerequisite steps such as confirming the configuration of the target environment and ensuring current backups exist.	0.25
Database Objects & Data	Creation of required databases, database objects and data on the HIPS-UI Web Database Server .	0.5
Web Site	Deployment of required web components to the HIPS-UI Web Application Server .	0.5
Configuration	Configuration of deployed components to reflect the target environment.	0.25

3.2 Prerequisites

Perform the following steps in the target environment:

- 1 Ensure you have current and valid backups of the target environment (server, database).
- 2 Review the configuration of the target environment and confirm it matches the expectations described in [Target Environment](#).
- 3 Review the assumptions listed in Assumptions and ensure they are valid.

3.3 Database Objects & Data

This section provides instructions for creating required databases, database objects, data and permissions on the **HIPS-UI Web Database Server** in the target environment.

- 1 Create a new database in the target SQL Server instance.
 - a The database may be named as required.
 - b The database will be referred to in subsequent steps as the **HIPS-UI Web Database**.
- 2 Locate the folder <INSTALL_SOURCE>\HIPS-Web\database and application named HIPS.Web.DataStore.DBUpgrade.exe. This application will install or upgrade the HIPS UI database objects and data into an existing database.

IMPORTANT

Ideally the login used to connect to the specified SQL Server instance must be a member of the *sysadm* fixed server role. If using integrated security, this will be the domain account of the user executing the preceding command. Alternatively, modify the connection string in the preceding

command to specify the user name and password for a SQL login with the appropriate membership.

In addition, ensure the default schema of the login's user in the HIPS UI database is set to [dbo]. It should not be set to [hipsui].

If the [SchemaVersions] table exists in the target database in a schema other than the [dbo] schema, it must be moved to the [dbo] schema prior to execution.

- a Open a command-prompt as Administrator and change directory to the directory which contains the HIPS.Web.DataStore.DBUpgrade.exe application.
- b Execute the following command¹:

```
.\HIPS.Web.DataStore.DBUpgrade.exe upgrade-db "Data
Source=#{HIPS.UI.Database.Server};Initial
Catalog=#{HIPS.UI.Database.Name};Integrated
Security=SSPI;Connect Timeout=15;"
```

Modifying the highlighted values as below:

- i. #{HIPS.UI.Database.Server} is the name of the SQL Server instance hosting the database.
- ii. #{HIPS.UI.Database.Name} is the name of the previously created database to be upgraded.

The command uses a default command timeout of 3600 seconds (1 hour) that can be adjusted via the --timeout option if desired.

If the command was successful, a green 'Success!' notice should be displayed. Any errors will be displayed in red.

- 3 In the same folder as the HIPS.Web.DataStore.DBUpgrade.exe application there is a ConfigurationScripts subfolder containing the following script that needs to be modified and manually executed:
 - o HIPSUI-Data.sql

This script adds in the [ClinicalSpecialty] reference data that is required for the Discharge Summary function in HIPS UI. If your site will not manually upload PDF Discharge Summary from HIPS UI then skip this step. The data that is inserted into the [hipsui].[ClinicalSpecialty] table should be modified to reflect the Clinical Specialties within your organisation. Within the script there are 5 INSERT statements. You should modify, remove or add extra statements to reflect your organisations Clinical Specialties. For example, the statement can be changed to be:

```
IF NOT EXISTS (SELECT * FROM [hipsui].[ClinicalSpecialty] WHERE [
ClinicalSpecialtyId] = 1)
INSERT INTO [hipsui].[ClinicalSpecialty]
([ClinicalSpecialtyId],[Code] ,[Description] ,[DateCreated]
,[UserCreated] ,[DateModified] ,[UserModified])
```

¹ Optionally, for help with additional command-line options, execute the following:
.\HIPS.Web.DataStore.DBUpgrade.exe upgrade-db --help

```
VALUES (1, N'ORTH' , N'Orthopaedics' , GETDATE() , N'Admin' , GETDATE() , N'Admin')
```

If extra Clinical Specialties require to be added, then copy the IF NOT EXISTS and INSERT statement and increment the [ClinicalSpecialtyId] field by 1 each time. For example, to add a sixth Clinical Specialty:

```
IF NOT EXISTS (SELECT * FROM [hipsui].[ClinicalSpecialty] WHERE [ClinicalSpecialtyId] = 6)
INSERT INTO [hipsui].[ClinicalSpecialty] ([ClinicalSpecialtyId], [Code] , [Description] , [DateCreated] , [UserCreated] , [DateModified] , [UserModified]) VALUES (6, N'Code6' , N'Clinical Specialty 6' , GETDATE() , N'Admin' , GETDATE() , N'Admin')
```

Once modified execute the script and ensure it completes without error.

- 4 Verify data has been inserted into the following tables:
 - a [hipsui].[ClinicalSpecialty]: 5 or if modified then as many as configured above
 - b [hipsui].[IdentityVerificationMethod]: 10 records
 - c [hipsui].[IndigenousStatus]: 5 records
 - d [hipsui].[IvcDeliveryMethod]: 5 records
 - e [hipsui].[MedicareConsent]: 6 records
 - f [hipsui].[ProximityRadius]: 4 records
 - g [hipsui].[Setting]: 42 records
 - h [hipsui].[Sex]: 3 records
 - i [hipsui].[Suffix]: 2 records
 - j [hipsui].[TimePreference]: 3 records
 - k [hipsui].[Title]: 12 records
- 5 Add the HIPS-UI Web Service Account as a login to the target SQL Server database engine instance.
- 6 Add the HIPS-UI Web Service Account as a user to the HIPS-UI Web Database.
 - a In the target SQL Server in SQL Server Management Studio, object explorer; expand the Security node.
 - b Expand the Logins node and locate the **HIPS-UI Web Service Account** you just added.
 - c Double-click on the **HIPS-UI Web Service Account** to open the properties dialogue.
 - d Select the *User Mapping* property.
 - e Select the *Map* option on the **HIPS-UI Web Database** and in the Database role *membership for: eHISC-UI Web Database* select the following database roles:
 - i db_datareader
 - ii db_datawriter
 - iii RunStoredProcedure

IMPORTANT: In a High Availability topology that employs a SQL Server cluster, this HIPS-UI database and the SQL Server login for the **HIPS-UI Web Service Account** must exist on all cluster nodes.

3.4 Web Site

This section provides instructions for deploying web components to the **HIPS-UI Web Application Server** in the target environment. All steps should be performed via a Remote Desktop session connected to the **HIPS-UI Web Application Server**.

3.4.1 Configure Installation Artefacts

Perform the following steps to configure installation artefacts to reflect the target environment:

- 1 Open the file `<INSTALL_SOURCE>\HIPS-Web\setup\HIPS-UI-Configuration.psd1` in a text editor such as Notepad or Notepad++.

The `HIPS-UI-Configuration.psd1` file is a Windows PowerShell data file containing a PowerShell hashtable of key/value pairs representing configuration data required during installation. By default, the file contains placeholders for each value that must be modified, for example in the following line:

```
Path = '#{HIPS.UI.Path}\web'
```

`Path` is the key of the hashtable entry, and the highlighted text `#{HIPS.UI.Path}\web` is the value that will need to be reviewed and modified as appropriate.

The `HIPS-UI-Configuration.psd1` file contains extensive comments describing each item that must be configured. In addition, a complete example is provided for reference in the `HIPS-UI-Configuration.sample.psd1` file.

- 2 Review and modify the values for each item as appropriate to the target environment. These values will be used during installation and injected into configuration files as appropriate.
- 3 Save and close the file.

IMPORTANT: It may also be desirable to review and modify additional configuration settings in the following files prior to installation:

- a `<INSTALL_SOURCE>\HIPS-Web\runtime\web\web.config`
- b `<INSTALL_SOURCE>\HIPS-Web\runtime\web\log4net.config`

Refer to the *Configuration* section for further information regarding configuration settings.

3.4.2 Execute Installation Scripts

Perform the following steps to deploy HIPS-Web runtime components to the target environment:

- 1 Open a Windows PowerShell console as Administrator.
- 2 Execute the following command to change directory to the location where the HIPS-UI installation artefacts are located:

```
cd <INSTALL_SOURCE>\HIPS-Web\setup
```

- 3 Execute the following command to install all HIPS-Web runtime components using the previously configured installation artefacts:

```
.\HIPS-UI-Install.ps1 -Interactive -ConfigurationDataFile  
'HIPS-UI-Configuration.psd1' -Remove -Install -Prerequisites -  
Web
```

This command will invoke the `HIPS-UI-Install.ps1` PowerShell script using the previously configured `HIPS-UI-Configuration.psd1` file as input to remove HIPS-Web (if already present), then install prerequisites and web components.

- 4 Ensure the command completes successfully.

Following installation, perform the following additional steps:

- 1 Open Windows Firewall.
 - a. Create rules to allow both inbound and outbound connections to the ports utilised by the previously created web site.

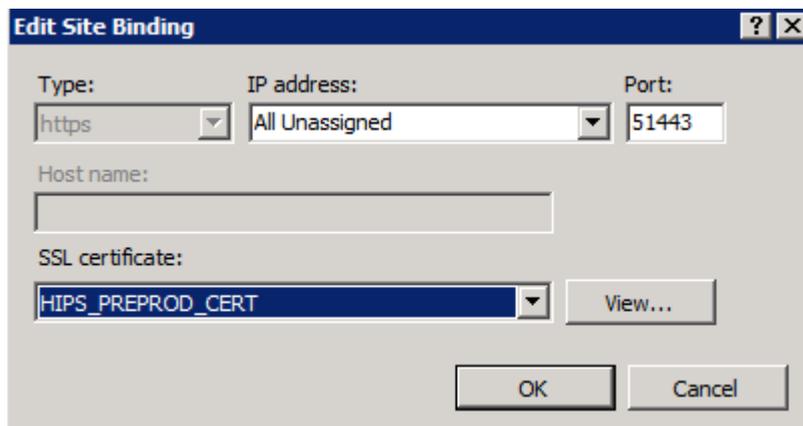
3.4.3 Web Site Self-Signed SSL Certificate

HIPS Web can be configured to use HTTP or HTTPS connectivity. HTTPS connectivity is recommended to ensure the encryption of the user’s credentials when submitted in the login form.

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 HIPS Web.

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 such 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 certificate previously configured from the “SSL Certificate” drop down and click OK.



- 7 Close the “Site Bindings” dialogue.

3.5 Configuration

This section provides instructions for configuring the HIPS-UI Web components prior to first use.

Perform the following steps via SQL Server Management Studio connected to the relevant database engine instance on the **HIPS-UI Web Database Server**.

- 1 Open the [hipsui].[Setting] table in the **HIPS-UI Web Database**. Review and modify where relevant the value of the [Value] column for each setting.
 - a The table below describes each setting:

Feature	Setting	Description	Suggested Value
All	DefaultHospitalCodeSystem	The default hospital code system used by the application.	pasFacCd
My Health Record View	PcehrViewServiceDateDocumentClasses	CSV of document class codes for which service dates should be displayed. Used when displaying document metadata in the document lists.	18842-5
My Health Record View	PcehrViewFromDateOffsetMonths	Negative integer value representing the number of months the "From" date criterion for the Prescription Dispense View will be offset from the current date by default.	-24
My Health Record View	PcehrViewPDDocumentClasses	CSV of document class codes for the Prescription and Dispense document classifications.	100.16764,100.16765
My Health Record View	PcehrViewPatientDaysDischarged	The number of days since the patient has been discharged to still consider a patient to be "currently in hospital". Used when retrieving the list of patients currently in hospital.	0
My Health Record View	EventSummaryDocumentTypeCode	The document type code that identifies a document as an Event Summary.	34133-9
My Health Record View	PcehrViewPatientDaysBeforePreAdmit	My Health Record View: The number of days before a patient is to be admitted for PreAdmit.	7
My Health Record View	PcehrViewPatientDaysAfterService	My Health Record View: The number of days after service date that non-inpatients are included in the list.	5

Feature	Setting	Description	Suggested Value
Data Integrity	PatientsWithoutIhiDaysDischarged	The number of days since a patient has been discharged to still show the patient on the list of patients without an IHI.	5
Disclose Hidden Digital Health Record	DiscloseHiddenPcehrDaysDischarged	The number of days since a patient has been discharged to still show the patient on the list of patients who can disclose the existence of a Digital Health Record.	5
Disclose Hidden Digital Health Record	DiscloseHiddenPcehrDaysAfterService	Disclose Hidden PCEHR: The number of days after service date that non-inpatients are included in the list. Set to 0 to exclude non-inpatients.	5
Disclose Hidden Digital Health Record	DiscloseHiddenPcehrDaysBeforePreAdmit	Disclose Hidden Health Record: The number of days before a patient is to be admitted for PreAdmit.	7
Withdraw Consent	WithdrawConsentPatientListDaysDischarged	The number of days since a patient has been discharged to still show the patient on the list of patients who can withdraw consent to upload documents to their Digital Health Record.	5
Withdraw Consent	WithdrawConsentEpisodeListDaysDischarged	The number of days after the patient has been discharged to show an episode on the list of episodes for which the patient can withdraw consent.	365
Withdraw Consent	WithdrawConsentPatientDaysBeforePreAdmit	Withdraw Consent: The number of days before a patient is to be admitted for PreAdmit.	7

Feature	Setting	Description	Suggested Value
Withdraw Consent	WithdrawConsentEpisodeDaysBeforePreAdmit	Withdraw Consent: The number of days before admission that show an episode on the episode list for which the patient can withdraw consent.	365
Remove Document	RemoveDocumentDaysDischarged	The number of days since a patient has been discharged to still show the patient on the list of patients whose documents can be removed from their Digital Health Record.	30
Remove Document	RemoveDocumentDaysAfterService	Remove Document: The number of days after service date that non-inpatients are included in the list. Set to 0 to exclude non-inpatients.	0
Discharge Summary	DischargeSummaryPatientListDaysDischarged	Discharge Summary: The number of days since a patient has been discharged.	5
Discharge Summary	DischargeSummaryEpisodeListDaysDischarged	Discharge Summary: The number of days after the patient has been discharged to show an episode on the list of episodes for which the patient can upload or supersede documents to their Digital Health Record.	365
Discharge Summary	DischargeSummaryDocumentTypeCode	Discharge Summary: The document type code for Discharge Summary.	18842-5
Discharge Summary	DischargeSummaryDocumentFormatCode	Discharge Summary: The document format code for Discharge summary. HPI-I enforced by default.	1.2.36.1.2001.10 06.1.20000.23

Feature	Setting	Description	Suggested Value
Discharge Summary	DischargeSummaryAuthor	Discharge Summary: The author for Discharge summary. Possible values are: 'User': logged on user, 'Provider': Health Provider 'None': empty and user must enter value.	User
Discharge Summary	DischargeSummaryRHP	Discharge Summary: The responsible health professional (RHP) for Discharge summary. Possible values same as DischargeSummaryAuthor.	User
All	SecurityGroupCodeSystem	The System Code for the Active Directory Security Groups mapped to Hospitals.	SecurityGroup
Secure Messaging	MessageDeliveryViewFromDateOffsetDays	Message Delivery View: Negative integer value representing the number of days of the "From" date criterion for the Message Delivery View will be offset from the current date by default.	-7
Secure Messaging	MessageReceiptViewFromDateOffsetDays	Message Receipt View: Negative integer value representing the number of days of the "From" date criterion for the Message Receipt View will be offset from the current date by default.	-7
JWT	TokenSigningCertificateSerialNumber	HIPS-UI will accept JWT tokens signed by the certificate in the Personal folder of the Local Machine store having this serial number.	<i>Serial number of certificate</i>

Feature	Setting	Description	Suggested Value
JWT	TokenEncryptionSharedSecretKey	HIPS-UI will accept JWT tokens encrypted with this base-64 encoded shared secret key.	<i>Base64 encoding of 64 bytes of secure random data</i>
JWT	TokenAudience	HIPS-UI will accept JWT tokens with this value in the Audience field.	HIPS
JWT	TokenIssuer	HIPS-UI will accept JWT tokens with this value in the Issuer field.	CIS
JWT	TokenValidityPeriodClockSkewSeconds	HIPS-UI will validate the NotBefore and Expiry fields of JWT tokens allowing for this many seconds of clock skew between the issuing and consuming server.	0
Assisted Registration	AssistedRegistrationByDVA	Flag to allow assisted registration using DVA Number.	True
Assisted Registration	AssistedRegistrationDaysBeforePreAdmit	Assisted Registration: The number of days before a patient is to be admitted for PreAdmit.	7
My Health Record View	ShowAllCurrentPatientsCodeSystem	Code System for a facility to indicate if the View My Health Record patient list should list all patients or redirect to a search.	ShowAllPatientsUI

Feature	Setting	Description	Suggested Value
All	EnablePatientRegistrationCodeSystem	Code System for a facility to indicate if the Patient Registration function is enabled for this hospital, allowing facilities with no ADT feeds to register patients in HIPS. NOTE: This setting is the Code System's code value in HIPS Core. The actual configuration to enable patient registration is in HIPS Core HospitalCode table.	EnableRegisterUI
Remove Document	DefaultRemoveDocumentTab	HIPS UI will show the configured tab when user selects a patient in the remove document page.	General <i>or</i> Pathology <i>or</i> DiagnosticImaging

- b It is expected the default values for each setting row will not be required to be modified unless JSON Web Tokens are to be used.

Perform the following steps via a Remote Desktop session connected to the **HIPS-UI Web Application Server**.

- 1 Open File Explorer.
 - a Browse to the **HIPS-UI Web Site Folder** in the filesystem of the **HIPS-UI Web Application Server**.
 - b Open the Web.config file in Notepad.
 - c Locate and modify the following configuration settings as relevant to the target environment:
 - i `appSettings`: Modify the value of the *value* element for each child *key* element as required, based on the following description of each setting:

Setting Name	Description	Suggested Value
AccountManagement.ContextType	The principal context for the Active Directory Account Management. Depending on the Account Manager set-up, if local SAM then <i>Machine</i> , if AD DS then <i>Domain</i> , if AD LDS then <i>ApplicationDirectory</i> .	Domain
AccountManagement.DomainName	Depending on value for AccountManagement.ContextType, if <i>Domain</i> then this is AD Domain Name in full domain name format (i.e. mydomain.com.au), if <i>Machine</i> then local machine name, if <i>ApplicationDirectory</i> then LDS server name & port.	
AccountManagement.TrustedDomains	A comma separated list of trusted domains that users will enter to login. The Web UI application checks that the domain entered by the user in the login form matches one of these domains in this list. If the application will be used in a single domain, then this will simply be that domain which would be the same as the AccountManagement.DomainName	<i>The same value as in AccountManagement.DomainName</i>
Account.ProfileImagePath	The file path under the root web site where the user's profile images will be created as jpg files. This folder will need write access for the HIPS-UI Web Service Account	/Content/images/profileimages/
Account.ProfileImageUriDefault	If the user does not have a profile image stored in AD, then this is the default image that will be displayed.	defaultUser.jpg
Account.ProfileImageProperty	The name of the Profile Image Attribute in AD.	thumbnailPhoto
ApplicationCookie.Timeout	The value in minutes for the application to timeout if left inactive.	20
ApplicationCookie.Secure	The security level for the cookie. Always: always send using HTTPS. Never: never send using HTTPS. SameAsRequest: send using HTTPS if the request was sent using HTTPS.	SameAsRequest

Setting Name	Description	Suggested Value
UI.PrivacyPolicyLink	A deployment specific local privacy policy link if one exists. This is displayed on the footer. If this value is empty, then no link will be displayed in the footer.	
UI.HideLogoutLink	Flag to determine if the Logout Link should be displayed. False: displays the logout link. True: hides the logout link.	false
Database.CommandTimeout	Database Connection Timeout (in seconds).	30
Mrn.Padding	Configuration of zero padding for local identifiers. Value must be between 0 to 40.	9

- ii `system.web/httpCookies`: The default setting for `httpCookies` is `httpOnlyCookies="true"` and `requireSSL="true"`. This should remain if the recommended HTTPS bindings has been implemented. If HTTP is being used, then the `requireSSL` will need to be updated to be "false".
- iii `system.webServer/httpProtocol/customHeaders`: Change the `X-Frame-Options` value for the required option for the embedded pages. The default is `SAMEORIGIN`.
- iv `MvcAuthorization`: This area of the web config is where the authorisation to access each application function is set. Each controller allows access to specific functions on the Web UI. The `roles` attribute lists the AD security groups and JWT roles whose members have access. The list is case-sensitive and must not have spaces after the commas. For sites that need to restrict access to specific healthcare facilities, unique AD groups should be set up for each healthcare facility. The default set up for the `MvcAuthorization` is to allow any user in the 'Administrators', 'Users' or 'Domain Users' groups to gain access. This must be changed before running HIPS UI in production.

```
<MvcAuthorization>
  <areas>
    <area>
      <policies>
        <policy name="DenyAnonymousAccess" />
      </policies>
      <controllers>
        <controller name="Home" />
        <controller name="AssistedRegistration"
roles="Administrators,Users,Domain Users" />
        <controller name="HpiiSearch"
roles="Administrators,Users,Domain Users" />
        <controller name="PcehrView"
roles="Administrators,Users,Domain Users" />
      </controllers>
    </area>
  </areas>
</MvcAuthorization>
```

```

        <controller name="Common">
            <actions>
                <action name="SessionInfo" />
                <action name="LogOff" />
                <action name="SelectHpo"
roles="Administrators,Users,Domain Users" />
            </actions>
        </controller>
        <controller name="DataIntegrity"
roles="Administrators,Users,Domain Users" />
        <controller name="ConsentManagement"
roles="Administrators,Users,Domain Users" />
        <controller name="DocumentManagement"
roles="Administrators,Users,Domain Users" />
        <controller name="DocumentUpload"
roles="Administrators,Users,Domain Users" />
        <controller name="DisclosureManagement"
roles="Administrators,Users,Domain Users" />
        <controller name="Delegates">
            <policies>
                <policy name="DenyNoRoleAccess" />
            </policies>
        </controller>
        <controller name="PayloadSchemes">
            <policies>
                <policy name="DenyNoRoleAccess" />
            </policies>
        </controller>
        <controller name="Subscription">
            <policies>
                <policy name="DenyNoRoleAccess" />
            </policies>
        </controller>
        <controller name="Messaging">
            <policies>
                <policy name="DenyNoRoleAccess" />
            </policies>
        </controller>
        <controller name="Error">
            <policies>
                <policy name="DenyAnonymousAccess"
ignoreInherited="true" />
            </policies>
        </controller>
        <controller name="Account">
            <actions>
                <action name="Login">
                    <policies>
                        <policy name="DenyAnonymousAccess"
ignoreInherited="true" />
                    </policies>
                </action>
            </actions>
        </controller>
    
```

```

        </policies>
    </action>
    <action name="Register">
        <policies>
            <policy name="LocalOnly" />
        </policies>
    </action>
    <action name="Manage">
        <policies>
            <policy name="LocalOnly" />
        </policies>
    </action>
    <action name="ExternalLoginConfirmation">
        <policies>
            <policy name="LocalOnly" />
        </policies>
    </action>
    <action name="ExternalLoginFailure">
        <policies>
            <policy name="LocalOnly" />
        </policies>
    </action>
</actions>
</controller>
<controller name="Role">
    <policies>
        <policy name="LocalOnly" />
    </policies>
</controller>
</controllers>
</area>
</areas>
</mvcAuthorization>

```

The table below maps the Controller access above to the Web UI Menu Functions.

Controller	Menu Functions
Home	Home
AssistedRegistration	Register Current Patients Register New Adult Register New Child
HpiiSearch	HPI-I Validation HPI-I Search
PcehrView	View My Health Record
Common/SessionInfo	Common Header
Common/LogOff	Log Off
Common/SelectHPO	Select Health Provider Organisation
DataIntegrity	Patients Without IHI

Controller	Menu Functions
ConsentManagement	Withdraw Consent
DocumentManagement	Remove Document
DocumentUpload	Discharge Summary
DisclosureManagement	Disclose Hidden Digital Health Record
Delegates	Interactions with Delegates (disabled)
PayloadSchemes	Interactions with PayloadSchemes (disabled)
Subscription	Areas of Interest (disabled)
Messaging	Message Delivery and Receipt (disabled)
Error	Generic error display, deny anonymous access
Account/Login	User login action, deny anonymous access
Account/Register	Local Access Only
Account/Manage	Local Access Only
Account/ExternalLoginConfirmation	Local Access Only
Account/ExternalLoginFailure	Local Access Only

For the users to be able to access a healthcare facility in HIPS-UI, a new Security Code is added in the HIPS-CORE Database [hips].[CodeSystem] table. Each facility must have a row inserted into the HIPS-CORE Database [hips].[HospitalCode] table with a comma-separated list of AD security groups or JWT roles whose members are authorised to select the facility. The list is case-sensitive and must not have spaces added after the commas. For each facility in the [hips].[Hospital] table the following SQL script can be run in the HIPS-CORE Database:

```

INSERT INTO [hips].[HospitalCode]
    ([HospitalId]
    , [CodeSystemId]
    , [Code]
    , [DateCreated]
    , [UserCreated]
    , [DateModified]
    , [UserModified])
VALUES
    (<HospitalId: from hips.Hospital table>
    , <CodeSystemId: default is 107>
    , <Code: A comma separated list of AD groups to grant access to
(example 'Users, Domain Users'>
    , GETDATE()
    , <UserCreated: your username>
    , GETDATE()
    , <UserModified: your username>)
GO

```

- v *applicationSettings/HIPS.Web.UI.Properties.Settings*: Modify the value of the *value* element for child *setting* elements as required, based on the following description of each setting (referenced by its *name* attribute):

Setting Name	Description	Suggested Value
SettingsRepository_ AbsoluteExpirationOffset	Provides a timespan value that represents the absolute amount of time application settings will be cached in memory. Format: <i>hh:mm:ss</i> , where <i>hh</i> represents the number of hours, <i>mm</i> represents the number of minutes, and <i>ss</i> represents the number of seconds.	02:00:00
HospitalRepository_ AbsoluteExpirationOffset	Provides a timespan value that represents the absolute amount of time the list of hospitals available for selection within the application will be cached in memory. Format: <i>hh:mm:ss</i> , where <i>hh</i> represents the number of hours, <i>mm</i> represents the number of minutes, and <i>ss</i> represents the number of seconds.	02:00:00
PatientRepository_ AbsoluteExpirationOffset	Provides a timespan value that represents the absolute amount of time patient data will be cached in memory. Format: <i>hh:mm:ss</i> , where <i>hh</i> represents the number of hours, <i>mm</i> represents the number of minutes, and <i>ss</i> represents the number of seconds.	00:05:00
PcehrViewRepository_ AbsoluteExpirationOffset	Provides a timespan value that represents the absolute amount of time Digital Health Record data for a patient (such as document metadata, document and view content) will be cached in memory. Format: <i>hh:mm:ss</i> , where <i>hh</i> represents the number of hours, <i>mm</i> represents the number of minutes, and <i>ss</i> represents the number of seconds.	00:05:00
AssistedRegistrationReferenceRepository_ AbsoluteExpirationOffset	Provides a timespan value that represents the absolute amount of time reference data used for assisted registration will be cached in memory. Format: <i>hh:mm:ss</i> , where <i>hh</i> represents the number of hours, <i>mm</i> represents the number of minutes, and <i>ss</i> represents the number of seconds.	00:05:00
PatientsWithoutPcehrRepository_ AbsoluteExpirationOffset	Provides a timespan value that represents the absolute amount of time patient data for assisted registration will be cached in memory. Format: <i>hh:mm:ss</i> , where <i>hh</i> represents the number of hours, <i>mm</i> represents the number of minutes, and <i>ss</i> represents the number of seconds.	00:05:00

- d Save and close the file.
- 2 Open Command Prompt (as Administrator).
 - a Execute the following command: iisreset

4 Product Verification Testing

Perform the following steps to verify the correct behaviour of the HIPS-UI Web product.

NOTE: Specific steps performed are dependent upon the local policies of the implementing organisation and upon the state of integration between the organisation's PAS and CIS, HIPS-Core, and the My Health Record System.

- 1 Open a web browser (e.g. Internet Explorer).
- 2 Browse to the HIPS-UI Web site.
- 3 Provide valid authentication credentials when prompted.
- 4 Verify the Home page is displayed and provides the following menu items:
 - a Healthcare Identifiers
 - b My Health Record Registration
 - c Clinical Documentation
 - d Verify behaviour of the My Health Record Registration feature:

NOTE: This does not test HIPS connectivity. However, performing an actual Digital Health Record registration is not desirable.
 - e Click the "My Health Record Registration" menu item and select the "Register Current Patients" option.
 - f Select a hospital and click "Select Hospital".
 - g Select a patient and click "Register". Verify the form loads without error.

NOTE: Depending on the state of integration at the implementing organisation, no patients may be available for selection.
 - h Click the "My Health Record Registration" menu item and select the "Register New Adult" option. Verify the form loads without error.
 - i Click the "My Health Record Registration" menu item and select the "Register New Child" option. Verify the form loads without error.
- 5 Verify behaviour of the Healthcare Identifiers feature:
 - a Click the "Healthcare Identifiers" menu item and select the "HPI-I Validation" option.
 - b Enter search criteria and click "HPI-I Search".
 - c Verify an HPI-I result is found and returned.
 - d Click the "Healthcare Identifiers" menu item and select the "HPI-I Validation" option.
 - e Enter search criteria and click "Search by Demographics".
 - f Verify an HPI-I result is found and returned.
- 6 Verify behaviour of the Clinical Documentation feature:
 - a Click the "Clinical Documentation" menu item, then click on "View My Health Record".

- b Verify the “Patient List” screen is displayed and allows selection of a hospital.
- c Upon selecting a hospital, verify a list of patients at the selected hospital is displayed.
- d Click the “View Patient Summary” button for a particular patient.
- e Verify the “Health Record Overview” screen is displayed and displays a list of documents for the selected patient (you may need to expand the collapsed sections of the Health Record Overview, or select another View such as Pathology, Diagnostic Imaging, Prescription and Dispense or Other Documents).
- f Click the “View Document” button for a particular document.
- g Verify the “Document View” screen is displayed and displays the contents of the selected document. Click “Close” to close the “Document View” screen.
- h Return to the “Patient List” screen for the selected hospital via the back button.

5 Rollback or Remove HIPS-UI

In the case that rollback is required, perform the following steps in order to remove the components previously deployed via the instructions in [Deployment Instructions](#).

- 1 Web Site:
 - a Windows Firewall:
 - i Remove inbound rules.
 - b IIS Manager:
 - i Remove **HIPS-UI Web Site**.
 - ii Remove **HIPS-UI Web App Pool**.
 - c File Explorer:
 - i Delete **HIPS-UI Web Site Folder**.
 - d Computer Management:
 - i Remove **HIPS-UI Web Service Account** from "IIS_USRS" group.
- 2 Database Objects & Data:
 - a Delete **HIPS-UI Web Database**.
 - b Remove **HIPS-UI Web Service Account** login.

Appendix A log4net Configuration

HIPS UI uses the log4net which offers flexible logging configuration options for implementers. The default settings are configured in the log4net.config file which can be found in the HIPS installation folder alongside the web.config.

A.1 Configuring Appenders

log4net supports many types of appenders for logging to different formats. The HIPS UI configuration file is pre-configured to use the following types of appenders:

- ADO.NET (Logs to the hips.ELMAH table)
- RollingFileAppender (referenced by BufferingForwarder_File)

For more configuration examples refer to the [log4net config documentation](#).

A.2 Filtering log messages based on custom properties

It is often useful to apply custom property filters to appenders. The following RollingFileAppender example contains a filter element which has been configured to only log messages where the custom property facility_code is 'RCH' and outputs any logged messages to a HIPS.Hospital_RCH.log file:

```
<appender name="HIPS.Hospital_RCH" type="log4net.Appender.RollingFileAppender">
  <file value="HIPS.Hospital_RCH.log" />
  <appendToFile value="true" />
  <rollingStyle value="Size" />
  <maxSizeRollBackups value="5" />
  <maximumFileSize value="10MB" />
  <staticLogFileName value="true" />
  <layout type="log4net.Layout.PatternLayout">
    <conversionPattern value="%date Facility code:(%property{facility_code}) [%thread] %level %logger
- %message%newline%exception%newline" />
  </layout>
  <filter type="log4net.Filter.PropertyFilter">
    <Key value="facility_code" />
    <StringToMatch value="RCH" />
  </filter>
  <filter type="log4net.Filter.DenyAllFilter" />
</appender>
```

A.3 Configuring the layout pattern

The default layout pattern used by HIPS UI to write to files specifies the date, facility, thread, level, logger, message and exception. If needed, the layout conversion patterns can be modified to show only relevant details.

Default log4net properties can be specified in the layout conversion pattern by adding a '%' in front of the property name. For a full list of log4net properties available refer to the [log4net Pattern Layouts documentation](#).

A.4 HIPS UI custom properties

The `facility_code` is the sole custom property written by HIPS UI (when available) and can be used in the logger layout conversion patterns.

Custom properties can be added to layout conversion patterns with the following syntax:

```
property{<propertyname>}
```

For example, the following can be used to display the username property:

```
Facility Code: %property{facility_code}
```

A.5 Log Levels

HIPS UI is currently configured to log messages with the ERROR log level only.