

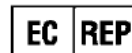
Hospira MedNet™

INSTALLATION & CONFIGURATION GUIDE



Hospira, Inc., 275 North Field Drive,
Lake Forest, IL 60045, USA

430-98300-002 (B, 2016-05)



Hospira UK Limited
Horizon, Honey Lane, Hurley,
Maidenhead, SL6 6RJ, UK

Notes:

Hospira MedNet™

Installation and Configuration Guide

Rx Only

REF 16037-75-02

IMPORTANT

Refer to the Installation and Configuration Guide for proper use, warnings and cautions associated with installing and configuring the Hospira MedNet™ Software. The help files included with the Hospira MedNet™ Meds™ Software are provided as reference only.

Intended Use

The Hospira MedNet™ Medication Management Suite (MMS) is intended to facilitate networked communication between MMS compatible computer systems and Hospira Infusion pumps. The MMS provides trained healthcare professionals with the capability to send, receive, report and store information from interfaced external systems and to configure and edit infusion programming parameters.

The MMS is intended to provide a way to automate the programming of infusion parameters, thereby decreasing the amount of manual steps necessary to enter infusion data. All data entry and validation of infusion parameters is performed by a trained healthcare professional according to doctor's orders.

Please read this entire guide before using the Hospira MedNet™ Software.

**Hospira Advanced Knowledge Centre
1-800-241-4002
Available 24 hours a day (in the USA)**






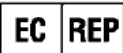


For assistance outside the USA, contact your local Hospira Representative

For device feature compatibility with Hospira MedNet™ and/or to obtain a copy of this guide, contact the Hospira Advanced Knowledge Centre or your local Hospira representative, if outside the USA.

From our Hospira website, you can access our System Operating Manuals and this guide via the Support Centre's Infusion Pumps + Clinical Software.

Change History

| Part Number | Description of Change | Pages Changed |
|----------------------------|--|----------------------|
| 430-98300-002 (A, 2016-01) | Initial release | |
| 430-98300-002 (B, 2016-05) | per SCR MEDNET 2125 delete Formulary Interface references | |

| Symbols | Description |
|---|--|
|  | Caution |
|  | Warning |
|  | CE Mark |
|  | Catalogue Number |
|  Hospira, Inc., 275 North Field Drive, Lake Forest, IL 60045, USA | Manufacturer |
|  | Authorised Representative in the European Union |
| RxOnly | CAUTION: Federal (USA) law restricts this device to sale by or on the order of a doctor or other licensed practitioner |
|  | Consult Instructions for Use |
|  | Date of Manufacture |

Notes:

Contents

| | |
|---|-----------|
| Chapter 1: Preparing Servers for Hospira MedNet Software | 1 |
| Minimum System Requirements | 1 |
| Distributed SQL Environment | 1 |
| Full Server* | 2 |
| Mini Server* | 2 |
| Software for Hospira MedNet server | 3 |
| Microsoft Windows Server Security Updates | 3 |
| Client Computers | 3 |
| Hospira MedNet Meds | 4 |
| Additional Non-Hospira Software | 4 |
| General Notes | 4 |
| General Requirements | 5 |
| General Warnings and Cautions | 5 |
| Preparation to Upgrade the Hospira MedNet Software Server Database | 6 |
| Upgrading the Hospira MedNet Software Database | 6 |
| Time Synchronisation | 6 |
| Internet Information Services (IIS) | 6 |
| Installation Notes | 7 |
| Firewall Ports on Windows Server | 7 |
| Installing SQL Server | 9 |
| XP_CMDSHELL | 9 |
| Configuring SQL Server for SSL | 9 |
| Chapter 2: Installing Hospira MedNet Software 6.2 | 11 |
| Part 1: Installing the Hospira MedNet Database | 11 |
| To install or upgrade the Hospira MedNet Software Database in a Distributed Environment | 11 |
| Migrating the Hospira MedNet Software Database | 12 |
| To install or upgrade the Hospira MedNet Database in a Non-distributed Environment | 13 |
| Part 2: Installing the Hospira MedNet Software | 15 |
| Installing Java Software Development Kit (JDK) | 15 |
| Installing the Hospira MedNet Software | 16 |
| LDAP Configuration for LDAP-enabled | 18 |
| Import the Licence File | 20 |
| Verify Connectivity (for LDAP) - Optional | 20 |
| Part 3: Configuring SSL | 23 |
| SSL Setting | 23 |
| SSL Settings for a Plum 360 | 25 |
| Enabling SSL for the database in HMSS | 26 |
| Enabling SSL for Hospira MedNet Services | 27 |
| Chapter 3: Installing Hospira MedNet Meds | 29 |
| To install or upgrade the Hospira MedNet Software Database in a Distributed Environment | 29 |
| Part 1: Installing the Hospira MedNet Meds Database | 30 |
| To install the Hospira MedNet Meds Database or upgrade the Hospira MedNet Meds Database | 30 |
| Part 2: Installing Hospira MedNet Meds Software | 31 |
| To install the Hospira MedNet Meds software | 31 |
| Enabling SSL for Hospira MedNet Meds | 32 |
| Chapter 4: Backing Up, Restoring and Maintaining Databases | 33 |

| | |
|--|-----------|
| Appendix A: Enhanced Asset Tracking | 35 |
| Pre-requisites | 35 |
| Setting up the Hospira MedNet Server Connection | 35 |
| Setting up the Asset Tracking Server | 37 |
| Recording Infuser ID for the Real-Time Location System | 37 |

Chapter 1: Preparing Servers for Hospira MedNet Software

Minimum System Requirements

Important: The Hospira MedNet Software has been developed and tested using the hardware components and software application versions described below. Any deviations from the minimum configurations listed below are not supported.

In virtual environments, reserve a minimum of 100 GB of storage. Depending on the infuser type and number of infusers, the storage requirements may grow to 1 TB over the product's expected life cycle.

Distributed SQL Environment

Important: Recommended for Auto-Programming and IHE-based client solutions for optimum performance. Recommended for installations needing to support between 500 and 2000 infusers.

For a distributed environment when Hospira MedNet software is on one machine and the Hospira MedNet database is physically located on another machine. You will need the following:

- A server* to house the Hospira MedNet Software (Server 1)
- A server* to house the Hospira MedNet Database (SQL) software (Server 2)

Note: For HMSS Server: Hex (6) Core Intel Xeon Processor - 3.0 GHz or better and
For SQL Server: Quad (4) Core Intel Xeon Processor - 3.0 GHz or better

Each machine should meet the following requirements:

- 12 GB RAM (6 GB allocated to Hospira MedNet HMSS Service)
- Redundant power supply
- SAS hardware RAID 1+0 controller card (minimum recommended RAID level 1+0)
- Reserved database disk space:
 - 1 TB volume consisting of 15K-RPM 6-Gb/s SAS disk drives or better to support non-Plum 360 devices
 - or
 - 4 TB volume consisting of 15K-RPM 6-Gb/s SAS disk drives or better to support Plum 360 devices

Note: The database size is based on your utilisation of the devices. Please use database maintenance best practices to control the size of your database.

- 120 GB volume of 15K-RPM 6-Gb/s SAS disk drives (HMSS Server disk space)
- Dual Gigabit Ethernet NICs with link aggregation support
- Internet Protocol version 4 (IPv4)
- USB port
- Backup capability

Note: *Install the software described below, including the security/Windows updates on **each** of the two servers. Security updates can be obtained from the Advanced Knowledge Centre or downloaded from the Microsoft website.

Full Server*

This configuration is to support up to 500 infusers when using the following minimum configuration (* denotes difference from 100-infuser support configuration):

Hardware

- Quad Core Intel Xeon processor - 3.0 GHz or better
- 12 GB RAM (6 GB allocated to HMSS Service)
- Redundant power supply
- SAS hardware RAID controller card (minimum recommended RAID level 1+0)
- *(4) 250 GB 15K-RPM 6-Gb/s SAS disk drives or better
- *120 GB Hard Drive for operating system
- *Dual Gigabit Ethernet NICs with link aggregation support
- Internet Protocol version 4 (IPv4)
- USB port
- Backup capability

Mini Server*

This configuration is to support 100 infusers when using the following minimum configuration:

Hardware

- Dual Core Intel Xeon processor - 3.0 GHz or better
- 12 GB RAM
- Redundant power supply
- (2) 250 GB 15K-RPM 6-Gb/s SAS disk drives or better
- 120 GB Hard Drive for operating system & HMSS
- Dual Gigabit Ethernet NICs, teamed
- Internet Protocol version 4 (IPv4)
- USB port
- Backup capability

Software for Hospira MedNet server

- Microsoft™ Windows™ Server 2012 R2 Standard with Updates
- Microsoft SQL Server™ 2014 Standard Edition with Service Pack 1
- McAfee™ Virus Scan Enterprise 8.7.0i or better (Optional)
- Internet Explorer 11 configured in compatibility mode
- Adobe™ Reader 9 or 10

Tip: Please consult the Hospira Advanced Knowledge Centre's article **Configuring Antivirus Software on a Hospira MedNet server**.

- A copy of the Hospira MedNet Software Installation and Configuration Guide
- The Hospira MedNet Software
- The Hospira MedNet Meds software

Microsoft Windows Server Security Updates

Please contact the Advanced Knowledge Centre for this information or download directly from the Microsoft website.

Important: The above configurations are for licensable features of Hospira MedNet including Auto-Programming, Auto-Documentation and Enhanced Asset Tracking via the Hospira MedNet Clinical Integration Interface.

Calling Hospira MedNet Clinical Integration interface `GetPumpStatus`, `GetMatchingPumps` to retrieve information from the Hospira MedNet server should occur on a low frequency to avoid overwhelming the server and interrupting normal operations.

Client Computers

The Client is used to host the web browser. Most computing is done on the server but display and processing of 1000-2000 infusers requires significant client side memory as well.

Hardware

- 1 GHz or faster 32-bit (x86) or 64-bit (x64) processor
- 2 GB of RAM or better
- 40 GB hard drive or better
- Network adapter (Ethernet or Wi-Fi)
- USB Port

Note: Most laptops and desktops can support this hardware configuration.

Software (Web Browser Access to Hospira MedNet Server)

- Microsoft Internet Explorer™ 11, configured as the default web browser in compatibility mode
- Adobe™ Reader 9 or 10

Hospira MedNet Meds

Hardware

- 1 GHz or faster 32-bit (x86) or 64-bit (x64) processor
- 2 GB of RAM or better
- 40 GB hard drive or better
- Network adapter (Ethernet or Wi-Fi)
- USB port for installation

Software

- Windows 7 Professional
- Adobe™ Reader 9 or 10
- Hospira MedNet Meds software
- Microsoft Internet Explorer 11 in compatibility mode

Additional Non-Hospira Software

Note: Additional software is bundled with Hospira MedNet™. Refer to the Click Wrap Agreement for details.

General Notes

- It may only be necessary to install antivirus software once, at the end of the entire installation process, to ensure system safety; if there is any question, consult with your System Administrator regarding advisability of when to perform this step.
- Illustrations and screen representations are for illustrative purposes only and may vary from the actual software. Your computer display may affect screen representation.
- Some features described in this document are enabled by the software licence agreement. Your licence may not enable all of these features.

General Requirements

Important: Installation of the Hospira MedNet software should be performed by Information Technology professionals with experience in Windows Server and SQL server administration.

General Warnings and Cautions

- Ensure all applicable system and device settings are appropriate for optimum response times.

Important: Do not install the Hospira MedNet software on the same computer as the Hospira MedNet Meds software.

- Except for virus data files (typically called “dat” files), do not install upgrades, service packs or patches to non-Hospira software on computers on which the Hospira MedNet Software or Hospira MedNet Meds is installed, except as authorised by Hospira.

Important: We strongly recommend the use of a virus checking software. However, we suggest you consider ignoring scanning directories where the datafiles reside or to ignore MDF and LDF type files. Updates or changes to the antivirus software after installation could affect Hospira MedNet server performance. Please contact the Hospira Advanced Knowledge Centre for information or assistance.

Ensure that **C:\Hospira\Hospira-MedNet-6.2\jboss-4.2.3.GA\server\hmssv6** is excluded from the virus scan product’s list of directories to scan. If applicable, replace the “C” with the drive on which you install the Hospira MedNet software.

- Do not enable automatic updates to operating systems on computers on which the Hospira MedNet Software or Hospira MedNet Meds is installed.

To disable automatic updates:

1. Go to the **Start Menu/Control Panel/System/System Properties/Automatic Updates**.
2. Click the radio button to **Turn off Automatic Updates** (or follow a similar procedure for your system).

Note: Ensure procedures are in place to prevent cross-talk from wireless networks outside of your organisation.

Note: Please ensure that PCs and servers on which Hospira MedNet software is installed are in a safe and secure physical location.

Preparation to Upgrade the Hospira MedNet Software Server Database

Important: If you are installing Hospira MedNet Software for the first time, please proceed to the next part of this chapter.

Upgrading the Hospira MedNet Software Database



Caution! Verify that the HMSS Service is not started or operating before performing the migration.

1. Backup the Hospira MedNet Software database that you are using to migrate.

Important: We highly recommend that you regularly back up and purge your database. A database can grow to a large size that will affect the performance of your Hospira MedNet system.

Although we suggest purging a database every four years at a minimum, if you have more than 2000 infusers it would be wise to consider doing so more often. Complete backup instructions are in this guide or you can consult our Advanced Knowledge Centre.

2. Remember to install hotfixes available from the Advanced Knowledge Centre.
3. Using Add/Remove Programmes, uninstall any previous version of the Hospira MedNet Server Suite.
4. We recommend that you reboot your computer after the uninstallations.

Time Synchronisation

Time synchronisation accuracy must be within a median error of less than one second. To that end the HMSS host should synchronise its time with the Domain Controller, and the Domain Controller is to synchronise its time to the Network Time Protocol (NTP - RFC 1305) server pool.

For additional information about time synchronisation, please contact the Advanced Knowledge Centre.

Internet Information Services (IIS)

From your control panel, you will need to verify that the Internet Information Services (IIS) is not installed.

Installation Notes

Firewall Ports on Windows Server

Important: No matter what configuration you use, please ensure that ports 8080 and 8443 remain open.

In order to establish communication with Hospira MedNet, you will need to address inbound and outbound traffic by going in the firewall and opening closed ports:

Server Manager > Windows Firewall > Properties

| Inbound Ports | |
|---|----------------------------------|
| Servers Hosting | Port No. |
| Hospira MedNet without SSL | 8080 |
| Hospira MedNet (SSL enabled) | 8443 |
| Remote SQL Server default instance | 1433 inbound from Hospira MedNet |
| Hospira MedNet (SSL with Mutual Authentication enabled) | 11444 |

| Outbound Ports | |
|--|-----------------------|
| Servers Hosting: any configuration of Hospira MedNet | |
| Outgoing Communication with: | Port No. |
| SMTP | 25 |
| LDAP | 389 |
| Infuser (SSL disabled) | 80 |
| Infuser (SSL enabled) | 443 |
| Infuser (SSL with mutual authentication enabled) | 11443 |
| Remote SQL Server default instance | 1433 |
| Remote Named Instances of SQL Server | One Port per instance |
| IVCI Interface Consumers | One or more Port(s) |

Note: Port 9292 and Port 5100 should be open for inbound/outbound communication between the latest generation of infusers supporting the Hospira Device Protocol and Hospira MedNet.

The following are our recommendations but will depend on your requirements and policies:

- Enable auto updates for antivirus software.
- Ensure that procedures are in place for backing up data.
- Ensure the network security policies are in place for the networks on which the Hospira MedNet Software and Hospira MedNet Meds software are connected.
- Ensure that user passwords are protected.
- Use a backup power supply (uninterrupted power source).

Note: It is your organisation's responsibility to assure a safe, validated and functioning environment. This includes providing proper training of hospital staff, protecting systems controlling medical devices from network threats, and performing maintenance on hardware.

Note: A strong password is recommended for passwords on all Hospira systems. If your organisation has minimum password requirements, your password should satisfy your organisational requirements. Regardless of the password used, even null, the password is required for the Hospira MedNet Software server set-up. A strong password consists of at least eight characters, a combination of numbers and letters, at least one uppercase and one lowercase, no symbols (For example: 23HoSpiTal).

We suggest that you avoid using Windows and SQL "illegal" characters. These typically include & / ? < > \ : * | " ^ and any character you can type with the Ctrl key.

Note: We are using "sa" as the DB System Administrator throughout the installation. Should you use a different user name, you will need to use it not only for SQL but also for the Hospira MedNet and Hospira MedNet Meds software installations.

Installing SQL Server

Feature Selection, place a tick mark in the following:

Under **Instance Features**:

- Data Engine Services

Under **Shared Features**:

- Client Tools Connectivity
- Client Tools Backwards Compatibility
- Documentation Components
- Management Tools - Basic
 - Management Tools - Complete

Database Engine Configuration:

- Under Authentication Mode, select **Mixed Mode (SQL Server authentication and Windows Authentication)**.
- Enter the system administrator (sa) password. A strong, secure password is recommended.
- Confirm password.
- Under Specify SQL Server Administrators, click **Add Current User** and it will populate the box above with the administrator data.

XP_CMDSHELL

Important: XP_Cmdshell is required to perform certain installation tasks. Once the installation is complete, it is no longer required and will no longer be enabled. Please refer to Microsoft SQL Server documentation for information regarding this configuration.

Configuring SQL Server for SSL

Important: Please see Microsoft's documentation or MSDN for configuring SQL Server that supports SSL. You will require a suitable certificate that supports SSL communication between Hospira MedNet and SQL.

Please contact the Advanced Knowledge Centre for details.

Notes:

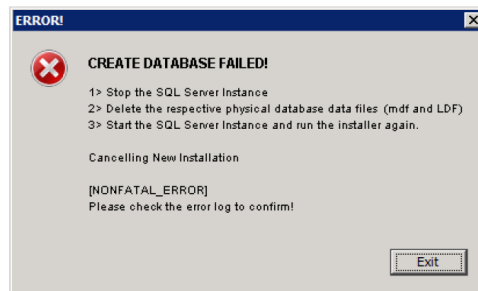
Chapter 2: Installing Hospira MedNet Software 6.2

Part 1: Installing the Hospira MedNet Database

Important: You must have System Administrator privileges to perform this installation.

The Hospira MedNet Database **must** be installed before installing the Hospira MedNet software in order for the application to work properly.

Note: Should you encounter the following error message, please check the TEMP directory/log files to investigate before deleting any mdf and LDF files which may not be necessary.



To install or upgrade the Hospira MedNet Software Database in a Distributed Environment

Caution! Verify that HMSS and MNS services are not started or operating before performing the migration.

Important: *If you are performing the installation on a machine that DOES NOT have SQL Server, you will need to download both the **Microsoft SQL Server Native Client** and the **Microsoft SQL Server 2014 Command Line Query Utility**.*

Click on the appropriate links provided in the html, based on your hardware (x86 or 64-bit). Set the PATH environment variable for the location of the SQLCMD.EXE

Once you have completed the download, continue with the instructions provided for the database installation.

Note: If you do not have SQL installed, proceed with the instructions provided in the next section.

Migrating the Hospira MedNet Software Database

Caution! Verify that HMSS and MNS services are not started or operating before performing the migration.

1. Restore the Hospira MedNet database into SQL.

Note: From SQL Server Management Studio, you will need to edit the credentials. This applies only if migrating from a different server. If using shared SQL, please consult the Advanced Knowledge Centre for instructions.

2. Scroll down to **Security** and expand.
3. Click **Logins**.
4. You will need to select each of the following:
mednet_app
mednet_archive
MEDNET_REPORTS
5. Right-click and select **Delete** for each. Instructions are provided for **mednet_app** to be duplicated for **mednet_archive** and **MEDNET_REPORTS**.
6. The **Deleted Objects** screen displays the selected item. Click **OK**.
7. The following message displays:

Deleting server logins does not delete the database users associated with the logins. To complete the process, delete the users in each database. It may be necessary to first transfer the ownership of schemas to new users.

Click **OK**. (Repeat steps 5, 6 and 7 for MEDNET.REPORTS and mednet_archive).
8. Close SQL Server Management Studio and reboot your computer.

To install or upgrade the Hospira MedNet Database in a Non-distributed Environment

Note: You must have System Administrator privileges to perform the installation.

1. From the Hospira download centre, locate the install.html files and select the one in the language you prefer. The installation instructions display.
2. Click the word [here](#) to install.
3. When asked if you want to run hmss db-install.exe, click **Run**.
4. When asked if you are sure you want to run the programme, click **Run**.
5. At the **User Account Control**, click **Yes**.

Wait to see the Hospira MedNet SoftwareInstallAnywhere installer **Introduction** screen.

Note: *The database can be installed on a different drive, provided it is the same as where Microsoft SQL is installed. Refer to the Distributed Environment information throughout this guide.*

Database Server Access Information

Database Server Host: Accept the server name default value in the field.

Note: *In a distributed environment, enter the name of the Server housing SQL instead of localhost.*

Database Server Instance is an optional field to be used if you have created a separate instance during the installation of SQL. In such a case, enter the name you have chosen for that instance.

Accept the default value in the field **Database Server Port**.

Note: We are using the default Port 1433 throughout the installation. Should you select to use a different port, you will need to use your port selection throughout.

At **Installer DB User ID:** type in **sa** (or the same DB user name you used in SQL).

Enter the case-sensitive password used throughout this installation manual.

In the field **Hospira MedNet DB Password:** type in the DB password.

In the field **Hospira MedNet DB Custom Reports Password,** type in the password.

Note: Keep track of the passwords.

Installation Type

Note: If you do not have enough disk space, a message displays to give you the option to either provide enough disk space or select **New Installation**. The upgrade path will not continue until disk space is available.

The estimated disk space required to perform the upgrade is: x GB. (x will be the exact amount.) **Restart when disk space is available or perform a new installation.**

Click **OK** to dismiss the message.

Database Name and Choose Report Database

Important: Use alpha-numeric characters to create the name of the database. Special characters cannot be used except for underscores.

Note: If a previous version of the Hospira MedNet server database is found, it will get renamed and archived. Click **OK** to continue with the installation.

For **Upgrade only**: You will be asked for the **Upgrade Source** for the **Report Database Name**.

Important: Please check the logs to ensure the installation was successful.

Part 2: Installing the Hospira MedNet Software

Note: *In a distributed environment, install the Hospira MedNet Software (HMSS) on Server 1.*

Before installing the Hospira MedNet Software, you will first need to install the Java Software Development Kit.

Installing Java Software Development Kit (JDK)

1. Click on the word [here](#) to install the Java Software Development Kit.
2. Click **Run** at the Security Warning(s).
3. Click **Yes** at User Account Control.

Note: If you already have the Java Development Kit (JDK), a pop-up message displays to confirm you already do. Verify the update is directly on the C: drive (or the drive on which you are installing the Hospira MedNet software) **not** in the Programme Files and proceed with the installation of the Hospira MedNet Software.

4. The wizard displays. Click **Next**.

With **Development Tools** highlighted, click **Change**.

Change the **Folder name** from the Programme Files\Java default.

Important: Services will not start unless you relocate JDK and JRE directly onto the C: drive or the drive on which you are installing the Hospira MedNet software.

Wait for Java to install. This may take a few minutes.

Reboot the computer.

Installing the Hospira MedNet Software

Note: You must have *System Administrator* privileges for the target server in order to perform the installation.

Important: Before starting, you are advised to confirm the following:

- Review all related **WARNINGS** and **CAUTIONS**.
 - Verify that the computer meets **all system requirements**.
 - Verify that **all necessary components** have been installed.
 - Uninstall any previous version of Hospira MedNet using Add/Remove programmes, if applicable. You will need to reboot the system once the uninstall process completes.
1. Follow the software installation instructions described in the web browser.
If you already have JDK installed, follow the instruction at **After installing the Java Development Kit** to click [here](#) to install Hospira MedNet Software.
 2. At the security warning screen, select **Run**.
 3. Select **Yes** at the User Account Control screen.
 4. Wait for the Hospira MedNet Software InstallAnywhere installer **Introduction** screen.

Select JBoss Naming Ports: Accept the IP port defaults.

- Set JBoss JMX Console Parameters
- Enter a User Name or accept the **admin** default.
- Enter a password for access to the JMX Console. Keep track of the password.

Database Server Access Information

- Accept the default value in the field **Database Server Host (localhost)**.
- In a distributed environment, enter the name of Server 2 (housing SQL) instead of localhost.
- **Database Server Instance** is an optional field for your use, if you so desire.
- Accept the default value in the field **Database Server Port**.
- At **Installer DB user ID**, type in **sa** (or the user name used in SQL).
- Enter the case-sensitive password used throughout this installation manual.
- In the field **Hospira MedNet DB Password**, type in the password you used in the preceding Hospira MedNet Software database installation.

Important: If you do not have Microsoft SQL Server installed, you will get an error message and the installation will end.

Note: *At Choose Report Database: In a distributed environment, with multiple servers, each instance of HMSS requires its own instance of HMSS reporting database.*

Enable LDAP Support

LDAP (Lightweight Directory Access Protocol) is an optional feature. It enables you to use your existing network directory listing for user names and passwords, allowing your network administrator to manage login access from one central source.

Important: The selection you make to enable LDAP or not can only be changed by uninstalling and reinstalling the Hospira MedNet Software

The *Hospira MedNetSoftware User Guide* describes in full details both the LDAP-enabled and non-LDAP environments.

Note: Should you select to enable LDAP, a sample configuration information follows this installation. Additional LDAP information is available through our Advanced Knowledge Centre.

Verify System Configuration

Review the minimum system requirements. Not meeting the minimum will affect the performance of the programme. Discrepancies will show in red.

LDAP Configuration for LDAP-enabled

The following screen is of the `ldap-login-config.xml` file located in the `server\hmsv6\conf` directory.

Note: You will need to edit this file according to your organisational requirement and security policies. This configuration should be performed by trained IT personnel familiar with LDAP. You may want to make a copy of the configuration script and save to a different folder prior to editing.

Important: HMSS Service should be turned off.

Full Read Access to the Active Directory

If you have read access to the Active Directory, only four module options need to be changed:

1. Change from: the `flag="required"` to: `flag=optional`
2. Change from the `ldap://EXAMPLESERVERNAME:389` setting to match your LDAP server IP address or FQDN adding the port of your LDAP server typically port 389:

Example: `ldap://ad-srv1.myhospital.com:389`

3. Change from: the `CN=Users,DC=example,DC=corp` line to: `DC=MyHospital,DC=local`
4. Change from the `@Example.corp` line to: `@MyHospital.local`

```

<policy>
  <application-policy name="Active Directory">
    <authentication>
      <login-module code="org.jboss.security.auth.spi.LdapLoginModule" flag="required">
      <module-option name="java.naming.provider.url">ldap://EXAMPLESERVERNAME:389/</module-option>
      <module-option name="rolesCtxDN">CN=Users,DC=example,DC=corp</module-option>
      <module-option name="principalDNSuffix">@example.corp</module-option>
      <module-option name="java.naming.factory.initial">com.sun.jndi.ldap.LdapCtxFactory</module-option>
      <module-option name="java.naming.security.authentication">simple</module-option>
      <module-option name="matchOnUserDN">false</module-option>
      <module-option name="uidAttributeID">sAMAccountName</module-option>
      <module-option name="roleAttributeID">memberOf</module-option>
      <module-option name="roleAttributeIsDN">>true</module-option>
      <module-option name="roleNameAttributeID">name</module-option>
      <module-option name="allowEmptyPasswords">false</module-option>
    </login-module>
  </authentication>
</application-policy>

```

CHANGE TO:

```

<policy>
  <application-policy name="Active Directory">
    <authentication>
      <login-module code="org.jboss.security.auth.spi.LdapLoginModule" flag="optional">
      <module-option name="java.naming.provider.url">ldap://ad-srv1.myhospital.local:389/</module-option>
      <module-option name="rolesCtxDN">DC=myhospital,DC=local</module-option>
      <module-option name="principalDNSuffix">@myhospital.local</module-option>
      <module-option name="java.naming.factory.initial">com.sun.jndi.ldap.LdapCtxFactory</module-option>
      <module-option name="java.naming.security.authentication">simple</module-option>
      <module-option name="matchOnUserDN">false</module-option>
      <module-option name="uidAttributeID">sAMAccountName</module-option>
      <module-option name="roleAttributeID">memberOf</module-option>
      <module-option name="roleAttributeIsDN">>true</module-option>
      <module-option name="roleNameAttributeID">name</module-option>
      <module-option name="allowEmptyPasswords">false</module-option>
    </login-module>
  </authentication>
</application-policy>

```

No Read Access to the Active Directory

If Active Directory has been locked down so that a user does not have full read access of the entire Active Directory, then the following block of code must be recreated for each organisational unit where an Hospira MedNet user account resides and the full path to the LDAP leaf must be called out.

Please note that the LdapLoginModule must be changed from “**required**” to “**optional**” as indicated below with an arrow.

```
<login-module>
<login-module code="org.jboss.security.auth.spi.LdapLoginModule" flag="optional">
  <module-option name="java.naming.provider.url">ldap://EXAMPLESERVERNAME:389/</module-option>
  <module-option name="rolesCtxDN">OU=BiomedS,DC=example,DC=corp</module-option>
  <module-option name="principalDNSuffix">@example.corp</module-option>
  <module-option name="java.naming.factory.initial">com.sun.jndi.ldap.LdapCtxFactory</module-option>
  <module-option name="java.naming.security.authentication">simple</module-option>
  <module-option name="matchOnUserDN">>false</module-option>
  <module-option name="uidAttributeID">sAMAccountName</module-option>
  <module-option name="roleAttributeID">memberOf</module-option>
  <module-option name="roleAttributeIsDN">>true</module-option>
  <module-option name="roleNameAttributeID">name</module-option>
  <module-option name="allowEmptyPasswords">>false</module-option>
</login-module>
<login-module>
<login-module code="org.jboss.security.auth.spi.LdapLoginModule" flag="optional">
  <module-option name="java.naming.provider.url">ldap://EXAMPLESERVERNAME:389/</module-option>
  <module-option name="rolesCtxDN">OU=Pharmacists,DC=example,DC=corp</module-option>
  <module-option name="principalDNSuffix">@example.corp</module-option>
  <module-option name="java.naming.factory.initial">com.sun.jndi.ldap.LdapCtxFactory</module-option>
  <module-option name="java.naming.security.authentication">simple</module-option>
  <module-option name="matchOnUserDN">>false</module-option>
  <module-option name="uidAttributeID">sAMAccountName</module-option>
  <module-option name="roleAttributeID">memberOf</module-option>
  <module-option name="roleAttributeIsDN">>true</module-option>
  <module-option name="roleNameAttributeID">name</module-option>
  <module-option name="allowEmptyPasswords">>false</module-option>
</login-module>
```

5. Save the changes to the ldap-login-config.xml file and exit out of the text editor.
6. Start HMSS service. At a command prompt, type:

C:\> NET START HMSS

Note: Additional information about LDAP is available through the Hospira Advanced Knowledge Centre.

Import the Licence File

In order for the Hospira MedNet software features to activate, you will need to import the licence file.

1. Access the server through the web browser.
2. Login ID and password.
 - Username: **mednet_admin**
 - Password: **12345678** (can only be used once)
3. Click **Login**.
4. You will be prompted to change the password. Enter the information requested. Click **Change Password**.
5. Click **Hospira MedNet Administrator**.
6. Select the **Administrative Set-up** tab.
7. Click the **Licence Information** tab section of the screen.
8. Click **Import New Licence File** to locate and select the appropriate **.jkey** file.
9. The selected licence displays. Click **Start Import**.

A message displays: **Valid licence file was imported** and the details of the licence imported appears in the **Current Licence Details** box.

Note: The setting of user accounts and privileges are fully described in the Users and Roles and Authentication Services chapters of the *Hospira MedNet Software User Guide*.

10. Click **Close**.

Verify Connectivity (for LDAP) - Optional

11. Click the **Authentication Services** tab.
12. Select **Active Directory** from the **Authentication Service** drop-down list.
13. Enter a valid network login ID.
14. Enter password.
15. Select **Test Connection**.

A "Connection successful" response will be returned as well as a list of all LDAP groups that the user account is a member of.

Group Mapping

Following is a spreadsheet to be used as a guide to select predefined roles and LDAP global group assigned to that role. Each role must be defined separately.

| Privilege ID | Privilege Title | 1-Administrator | 2-Administrator Limited | 3-Clinical Administrator | 4-Reports Limited | 5-Reports Full | 6-Pharmacist I | 7-Pharmacist II | 8-Biomed | 9-IT | 10-Materials Management |
|--------------|---|-----------------|-------------------------|--------------------------|-------------------|----------------|----------------|-----------------|----------|------|-------------------------|
| 1 | My Account | X | X | X | X | X | X | X | X | X | X |
| 2 | Users & Roles | X | X | X | | | | | | | |
| 3 | Administrative Setup | X | X | X | | | | | | X | |
| 4 | Reports Limited | | | | X | | | | | | |
| 5 | Reports Full | X | X | X | | X | X | X | X | X | X |
| 6 | Library Download | X | X | X | | | | | X | X | X |
| 7 | Infuser Management | X | X | X | | | | | X | X | X |
| 8 | Access Point Mapping | X | X | | | | | | X | X | X |
| 9 | Manage Finalized Libraries | X | | X | | | | X | | | |
| 10 | Manage Worksheets | X | | X | | | X | X | | | |
| 11 | View Drug Libraries | X | X | X | | | X | X | | | |
| 12 | Software Management | X | X | | | | | | X | X | X |
| 13 | View Medications | X | X | X | | | X | X | | | |
| 14 | Manage Medications | X | | X | | | | X | | | |
| 15 | Configure Formulary Interface | X | | X | | | | | | | |
| 16 | Authentication Services | X | | | | | | | | X | |
| 17 | Infusion Status | X | X | X | X | X | X | X | X | X | X |
| 18 | Manage Patient/Pump Assignments | X | | | | | | | | | |
| 19 | View Protected Health Information | | | | | | | | | | |
| 20 | Manage Message Queues | X | | | | | | | | X | |
| 21 | Infuser Logs | X | X | | | | | | X | X | X |
| 22 | Administrative Setup/Database Maintenance | | | | | | | | | X | |

Note: Each role must be defined separately.

Important: We recommend that you assign a single user to populate all the LDAP groups on the HMSS server and that this user be a part of each LDAP group, i.e. Administrator.

If this is not done, the LDAP groups will not be populated until a user in a specific group logs on and roles can only be attributed to that one specific group.

1. From the **Users & Roles** tab of the Hospira MedNet Administrator, select the **Roles** tab.
2. Select **Administrator**.
3. Click **Edit**.
4. At **LDAP Group**, enter the name of the group (Administrator, for our example).
5. Using the arrows, select the privileges you wish to assign to this group.
6. Save the changes.
7. Select the next role and repeat the process from step 3:
 - edit
 - assign privileges
 - save the changes
8. Once all the roles and privileges have been entered and saved, reboot the server.
9. Exit the screen.

Part 3: Configuring SSL

SSL Setting

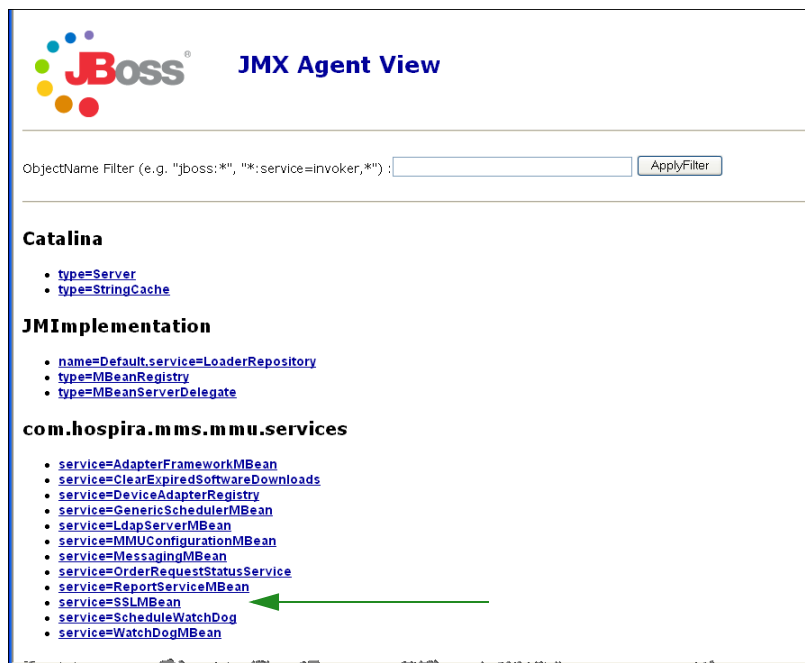
Important: Ensure that you enable SSL when you have finished setting up the network for use with the Hospira MedNet software.
If you enable SSL on Hospira MedNet, you must also enable SSL on the infuser's Communication Engine. Refer to each infuser's CE Configuration Guide for complete instructions.

Note: Enter the same User ID and password for JBoss JMX that you used during the HMSS installation.



To enable SSL:

1. Enter the following address in Internet Explorer:
`http://localhost:8080/jmx-console`
2. Scroll down to **com.hospira.mms.mmu.services** and click **service=SSLMBean**.



3. To prohibit non-secure transmission to infusers, set **SecureTransmissionToCE** to **True**.
4. To prohibit non-secure transmissions from infusers, set **AllowNonSecureTransmissionFromCE** to **False**.
5. To prohibit non-secure transmissions from BCMA handheld devices, set **AllowNonSecureTransmissionFromPDA** to **False**.

The screenshot shows the JBoss JMX MBean View console for the SSLMBean service. The MBean name is 'com.hospira.mms.mmu.services.service:SSLMBean'. The MBean Java Class is 'org.jboss.mx.model.mbean.XMBean'. The MBean description is 'SSLMBean provides access to SSL configuration'. The list of MBean attributes is as follows:

| Name | Type | Access | Value | Description |
|-----------------------------------|-------------------|--------|---|---|
| SecureTransmissionToCE | java.lang.Boolean | RW | <input checked="" type="radio"/> True <input type="radio"/> False <input type="radio"/> Null | Controls whether the Http transmission to CE should be secure or not |
| AllowNonSecureTransmissionFromCE | java.lang.Boolean | RW | <input type="radio"/> True <input checked="" type="radio"/> False <input type="radio"/> Null | Controls whether the non secure Http transmission from CE should be allowed or not |
| AllowNonSecureTransmissionFromPDA | java.lang.Boolean | RW | <input type="radio"/> True <input checked="" type="radio"/> False <input type="radio"/> Null | Controls whether the non secure Http transmission from PDA should be allowed or not |

Below the table is an 'Apply Changes' button. The list of MBean operations is empty.

6. Click **Apply Changes**.



Caution! Do not change any other settings in the JMX™ console. Changing settings other than those described above can cause the server software to function improperly.

SSL Settings for a Plum 360

SSL setting for a Plum 360 is done through the Hospira MedNet Services (MNS) server.

1. Remote desktop on the Hospira MedNet server.
2. Access Windows Service:
Start > Control Panel > Administrative Tools > Services
3. Shutdown Hospira HMSS, MNS and QMS services.
4. From **C:\Hospira\Hospira-MedNet-6.2\virgo-tomcat-server-3.6.1.RELEASE\pickup\mdashboard.war\WEB-INF\classes\META-INF\spring\settings.properties**

You will need to edit the text as follows:

- a. **Set mns.SSLEnabled=true**
- b. **Set isSecureWebSocket=true**

as shown framed in red in the illustration below.

```

# where software download files are stored on the filesystem
swdownload.filePath=C:\\Hospira\\Hospira-MedNet-6.1/virgo-tomcat-
# Enable/disable ssl for the retrieval of files. Used when sendir
mns.SSLEnabled=true
#mns.SSLEnabled=false

#communicate with HMSS thru SSL or not
hmss.SSLEnabled=true
#hmss.SSLEnabled=false

#This flag is used to enable SSL communication with database
database.sslEnabled=false

# max number of retries to attempt
hmss.maxRetries=60
# retry delay in milliseconds
hmss.retryDelay=60000

# SSL keystores
ssl.keyStore=C:\\Hospira\\Hospira-MedNet-6.1/virgo-tomcat-server-
ssl.trustStore=C:\\Hospira\\Hospira-MedNet-6.1/virgo-tomcat-serve
# Secure the access to HDPservices or not
isSecuredWebSocket=true

# Logretriever settings

```

5. Start Hospira HMSS, MNS and QMS services.

Enabling SSL for the database in HMSS

Important: The following can only be performed after Hospira MedNet Server and Hospira MedNet Meds have been installed.

1. Open mmu_configuration.xml for editing using Notepad:

C:\Hospira\Hospira-MedNet-6.2\jboss-4.2.3.GA\server\hmssv6\conf\mmu_configuration.xml

2. Scroll down to **Database SSL setting** (in the red box below).
3. Change the word **request** to **require**, that is:

From `<config>request</config>`

to `<config>require</config>`

```

707     <messagegovernor>
708         <enabled>True</enabled>
709         <messageLimit>20000</messageLimit>
710     </messagegovernor>
711
712     <!-- XSD Validation -->
713     <xsdValidation>
714         <enabled>true</enabled>
715     </xsdValidation>
716
717     <!-- Database SSL setting -->
718     <databaseSSL>
719         <!-- Default value: request -->
720         <!-- Allowed values: off, request, require, authenticate -->
721         <config>request</config>
722     </databaseSSL>
723
724     <!-- SSL for MedNet Services connection -->
725     <sslForMNS>
726         <enabled>true</enabled>
727     </sslForMNS>
728
729     <!-- Pump Observation logging -->
730     <mmuCommunicationLog>
731         <samplePumpObservation>true</samplePumpObservation>
732         <sampleRate>10</sampleRate>
733     </mmuCommunicationLog>
734
735     <!-- Download Infuser Logs -->
736     <downloadInfuserLogs>
737         <repositoryPath>@install.root.folder@\Dropzone</repositoryPath>
738     </downloadInfuserLogs>

```

4. You can now enable Hospira MedNet Services.

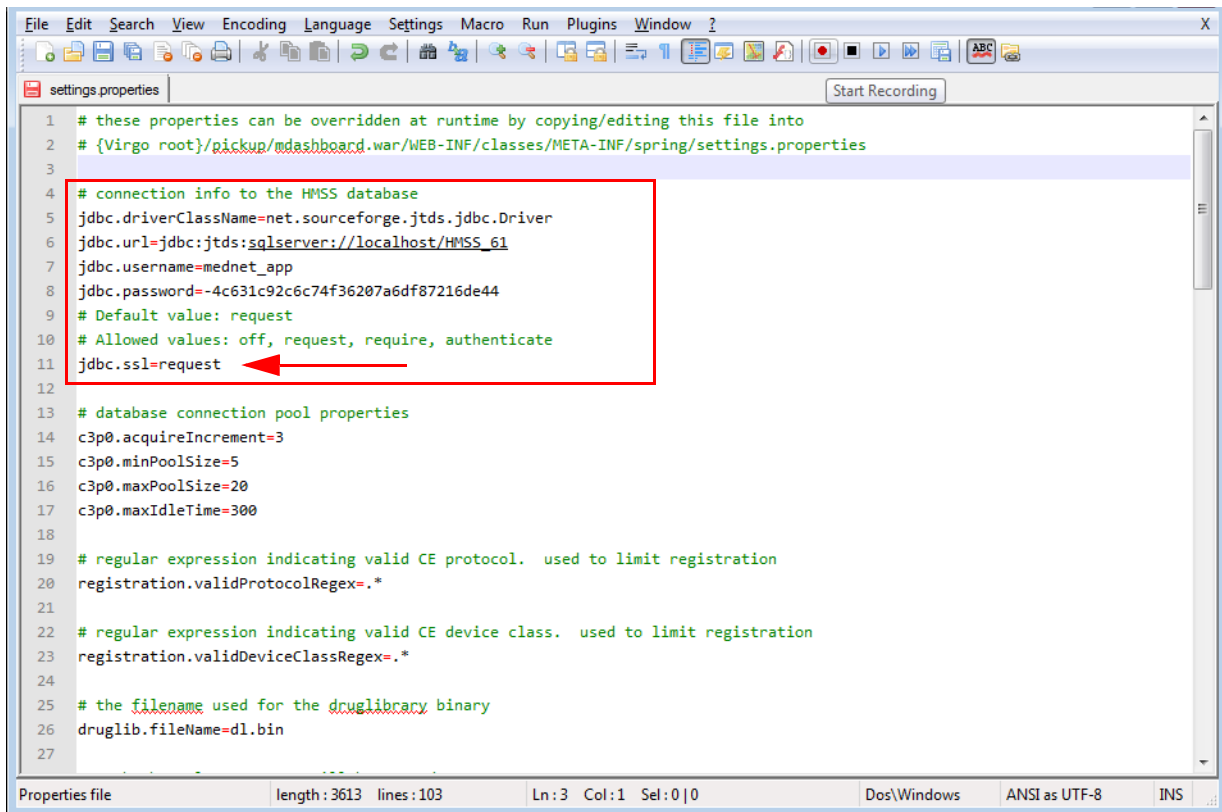
Enabling SSL for Hospira MedNet Services

You will need to edit `settings.properties`:

1. Access Hospira MedNet Services `settings.properties` as follows:

C:\Hospira\Hospira-MedNet-6.2\virgo-tomcat-server-3.6.1.RELEASE\pickup\mdashboard.war\WEB-INF\classes\META-INF\spring\settings.properties

2. Using Notepad navigate to **Connection info to the HMSS database** section (in the red box below).



```
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
settings.properties Start Recording
1 # these properties can be overridden at runtime by copying/editing this file into
2 # {Virgo root}/pickup/mdashboard.war/WEB-INF/classes/META-INF/spring/settings.properties
3
4 # connection info to the HMSS database
5 jdbc.driverClassName=net.sourceforge.jtds.jdbc.Driver
6 jdbc.url=jdbc:jtds:sqlserver://localhost/HMSS_61
7 jdbc.username=mednet_app
8 jdbc.password=-4c631c92c6c74f36207a6df87216de44
9 # Default value: request
10 # Allowed values: off, request, require, authenticate
11 jdbc.ssl=request
12
13 # database connection pool properties
14 c3p0.acquireIncrement=3
15 c3p0.minPoolSize=5
16 c3p0.maxPoolSize=20
17 c3p0.maxIdleTime=300
18
19 # regular expression indicating valid CE protocol. used to limit registration
20 registration.validProtocolRegex=.*
21
22 # regular expression indicating valid CE device class. used to limit registration
23 registration.validDeviceClassRegex=.*
24
25 # the filename used for the druglibrary binary
26 druglib.fileName=dl.bin
27
Properties file length: 3613 lines: 103 Ln: 3 Col: 1 Sel: 0 | 0 Dos\Windows ANSI as UTF-8 INS
```

3. Change from `jdbc.ssl=request` to `jdbc.ssl=require`
4. Restart the server.

Notes:

Chapter 3: Installing Hospira MedNet Meds



Caution! Before installing Hospira MedNet Meds, please ensure that no one is connected to any version of the Hospira MedNet Meds database. You can do this by stopping and then restarting the Microsoft SQL Server.



Caution! If you are upgrading the database, we suggest that you back up your data.

Note: You must have System Administrator privileges on the computer to perform the installation.

To install or upgrade the Hospira MedNet Software Database in a Distributed Environment

Note: *In a distributed environment, the Hospira MedNet Meds database must be installed on Server 2 (SQL Server).*

Important: *If you are making the installation on a machine that DOES NOT have SQL Server, you will need to download both the **Microsoft SQL Server Native Client** and the **Microsoft SQL Server Command Line Query Utility**, if not already present.*

Once you have completed the download, continue with the instructions provided for the database installation.

Part 1: Installing the Hospira MedNet Meds Database

To install the Hospira MedNet Meds Database or upgrade the Hospira MedNet Meds Database

1. From the Hospira download centre, locate the install.html files and select the one in the language you prefer.

The installation instructions display.

Tip: We suggest that you print a copy of the html page before beginning the installation process.

2. Click the [here](#) link to start the install/upgrade process.
3. At the **File Download- Security Warning**, click **Run** (or **Open**).
4. At **User Account Control**, click **Yes** and wait for the installation wizard to display the Introduction screen.

Choose Install Folder

Note: **Restore the Default Folder** is only necessary if the path is changed.

Local Database Server Location

Enter the Database Server IP Address or Host Name.

Note: Database Server Instance is an optional field to be used if you have created a separate instance during the installation of SQL. In such a case, enter the name you have chosen for that instance.

Database Name

Accept the default or enter the name of the new Hospira MedNet Meds database, which will be created as part of the upgrade process.

Note: If you should change the Database Name, keep a record of it. Use alpha-numeric characters to create the name of the database. Special characters cannot be used except for underscores.

Part 2: Installing Hospira MedNet Meds Software

1. From the Hospira download centre, locate the install.html files and select the one in the language you prefer.

The installation instructions display.

Note: If autorun is disabled and the installation page does not display automatically, then open Internet Explorer. Select **File > Open**; click **Browse** and navigate to the location of the installation files. Open the file **install.html**.

Tip: We suggest that you print a copy of the html page before beginning the installation process.

To install the Hospira MedNet Meds software

1. Follow the installation instructions displayed in the web browser window.

Important: This section applies only if you are installing Hospira MedNet Meds for the first time and **do not** have Hospira MedNet Meds on this computer.

Please refer to Chapter 1 to verify that your computer meets the minimum system requirements before installing Hospira MedNet Meds.

Note: You **MUST** have System Administrator privileges to perform this installation.

2. Click the [here](#) link on the **Installing** portion of the Hospira MedNet Meds installation screen to install Java Runtime Environment, if you don't have one. Select either JRE 32-bit or JRE 64-bit depending on your system.
 - a. Click **Install**.
 - b. Accept defaults and complete the installation.

Note: If you have the JRE update installed, a pop-up will confirm it.

3. Click the [here](#) link to install Hospira MedNet Meds.
4. When the **File Download** dialogue box displays, click **Run**.
5. At the **User Account Control** screen, click **Yes**.

Wait for the Introduction screen to display.

Choose Install Folder

Note: **Restore the Default Folder** is only necessary if the path is changed.

Locate HMSS Server

At **Server**, remove the “localhost” default and type the **IP Address** (or host name) of the server where the Hospira MedNet Server Suite is installed.

In a distributed environment, type the IP Address (or Device Name or fully qualified Domain Name) of Server 1 (hosting HMSS).

Locate HMSS Database Server

At **Database Server**, remove the “localhost” default and type the **IP Address** (or host name) of the server where the Hospira MedNet Software database is installed.

In a distributed environment, type the IP Address (or Device Name or fully qualified Domain Name) of Server 2 (housing SQL).

At **Database Server Instance**, enter the named instance, if applicable. This would be the **Instance Name** you entered when installing SQL Server.

Accept the Database Port default.

Note: You will need your Username and password to log in. Refer to the *Hospira MedNet Software User Guide 6.2*, User Administration chapter for complete instructions.

Enabling SSL for Hospira MedNet Meds

You will need to access the **MedNet.properties** file where Hospira MedNet is installed.

Using Notepad, navigate to

No. Allowed values: off, request, require, authenticate

Verify the following text:

database.ssl=require

Chapter 4: Backing Up, Restoring and Maintaining Databases

You must configure the backup device before continuing. For instructions on setting up a backup device to work with SQL Server, refer to the SQL Server documentation.

Backing up the Hospira MedNet Databases

Note: In addition to backing up the Hospira MedNet database we suggest you also back up the “Master” file.

Restoring the Hospira MedNet Databases

You must configure the backup device before continuing. For instructions on setting up a backup device to work with SQL Server, refer to the SQL Server documentation.



WARNING! Restoring a backup of the database requires stopping the Hospira MedNet server software service.

Database Maintenance

We highly recommend that you set up a database maintenance plan, if you don’t already have one in place.

Note: After several years, the database may grow to a very large size. You may consider using the purge process described in the *Hospira MedNet Software User Guide*.

Notes:

Appendix A: Enhanced Asset Tracking

Pre-requisites

- Hospira MedNet Software
- Valid software licence supporting enhanced asset tracking. External real-time location system (RLTS)
- RFID tags
- SSL server certificate (i.e. X.509 certificate)

Setting up the Hospira MedNet Server Connection

Note: Information such as the asset tracking server will be provided by the RLTS. Please set the selection according to the RLTS provider's instructions.

1. At **Enhanced Asset Tracking**, in the **ServerName[:port]** field, enter the following:
IPaddress:portnumber
or
servername:portnumber

Important: In order to ensure secure transmission, you will need to type in the secure port number: (**443** is the default). (The default port without secure transmission is **80**.)

2. **User** will be determined between RLTS provider and the customer.
3. At password, enter the password received from the RLTS provider.
4. At **Preferred Identifier**, select **Device ID**.
5. The **Location Detail** is **Space**.

The screenshot shows the Hospira MedNet administrative interface. At the top left is the logo. On the right, there are links for 'Welcome!', 'mednet_admin', 'Logout', and 'Help'. Below this is a navigation menu with buttons for 'Home', 'My Account', 'Users & Roles', 'Infusion Status', 'Infuser Management', 'Infuser Logs', 'Downloads', 'Software Import', 'Administrative Setup', 'Authentication Services', 'Patient Assignment', and 'Message Queues'. A status message reads: 'Enhanced Asset Tracking is receiving location change events.' Below this is a sub-menu with buttons for 'Institution Settings', 'Software Download Settings', 'License Information', 'Database Maintenance', 'Enhanced Asset Tracking', 'Locale Setting', 'SMTP Maintenance', and 'Integration Settings'. The main form area contains the following fields:

- Server Name(:port): ssettrack.hospira.corp:443
- User: system
- Password: [masked with asterisks]
- Preferred Identifier: Device ID (dropdown menu)
- Location Detail: Space (dropdown menu)
- Category Name: hospiratest
- Use secure transmission when sending messages to the receiving system:

At the bottom of the form are two buttons: 'Test Connection' and 'Save Changes'.

Important: Although the **Use secure transmission...** box is ticked by default, you will still need to ensure the SSL server certificate is present for the Asset Tracking service to be activated.

You will need to copy then paste the SSL server certificate into the HMSS configuration file by navigating to the HMSS configuration directory: **ljboss-4.2.3.GA\server\hmssv6\conf**

Stop then restart HMSS service.

or

Import the certificate via the JMX-Console:

Navigate to **AssetTrackingConfigurationMBean**, using <http://localhost:8080/jmx-console/>

Under **assettrackingconfiguration.certfilepath** select the certificate path then click **Apply Changes**.

6. Once the certificate is into the HMSS system, click **Save Changes** in the Administrative Set-up window.

The screenshot shows the 'Enhanced Asset Tracking' configuration page in the Hospira MedNet administrative interface. The page includes a navigation menu at the top with options like Home, My Account, Users & Roles, Infusion Status, Infuser Management, Infuser Logs, Downloads, Software Import, Administrative Setup, Authentication Services, Patient Assignment, and Message Queues. Below the navigation, there are tabs for various settings: Institution Settings, Software Download Settings, License Information, Database Maintenance, Enhanced Asset Tracking (selected), Locale Setting, SMTP Maintenance, and Integration Settings. The main configuration area contains the following fields:

- Server Name(port): ssettrack.hospira.corp:443
- User: system
- Password: [masked with asterisks]
- Preferred Identifier: Device ID (dropdown menu)
- Location Detail: Space (dropdown menu)
- Category Name: hospiratest
- Use secure transmission when sending messages to the receiving system:

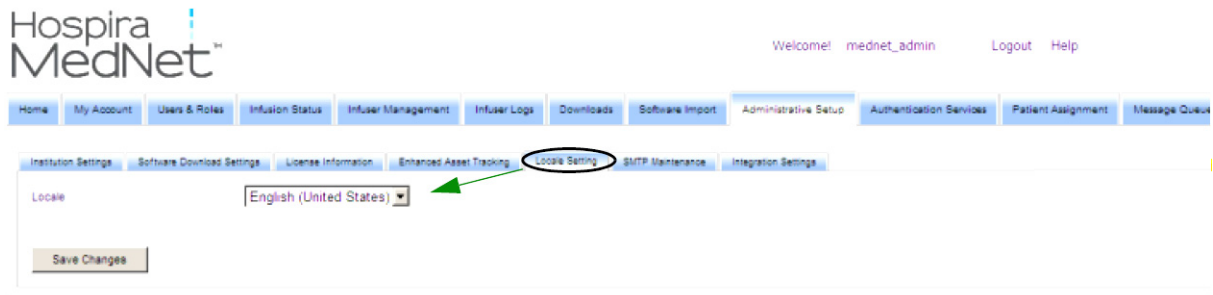
At the bottom of the configuration area, there are two buttons: 'Test Connection' and 'Save Changes'. The 'Save Changes' button is circled in red.

You can now go to the **Infuser Management** screen and see the actual location of all the infusers. It may take a while to populate, depending on the amount of data.

Note: Additional information on Enhanced Asset Tracking is available in the Hospira MedNet Software User Guide 6.2, Appendix C.

Locale Setting

Locale must be set to **English (United States)** in order to work with Hospira MedNet software.



Setting up the Asset Tracking Server

Instructions and additional information to set up the server(s) is to be provided by the Real-Time Location System vendor.

Important: Although Hospira MedNet employs the same field names as the RTLS, the names are not interchangeable.

The screenshot shows the Hospira MedNet interface with a table of infusers. The 'Device' column is highlighted with a red box. The table has columns for Select, Infuser Type, Device, Serial Number, Location, and Software Release. The data rows show four infusers of type 'PlumA+' with device IDs PLM000001 through PLM000004, all with serial numbers starting with SN_PLMCE000000 and software release version 13.40.00.006 20...

| Select | Infuser Type | Device | Serial Number | Location | Software Release |
|--------------------------|--------------|-----------|----------------|------------------|------------------------|
| <input type="checkbox"/> | PlumA+ | PLM000001 | SN_PLMCE000001 | 3rd floor ALO | Ver:13.40.00.006 20... |
| <input type="checkbox"/> | PlumA+ | PLM000002 | SN_PLMCE000002 | 1st Floor ALT ES | Ver:13.40.00.006 20... |
| <input type="checkbox"/> | PlumA+ | PLM000003 | SN_PLMCE000003 | CC Azalea | Ver:13.40.00.006 20... |
| <input type="checkbox"/> | PlumA+ | PLM000004 | SN_PLMCE000004 | 1st Floor ALT HR | Ver:13.40.00.006 20... |

Recording Infuser ID for the Real-Time Location System

An RFID tag needs to be affixed to each infuser.

Additional data will need to be provided for recognition by the Real-Time Location System. Instructions and specifics are to be provided by the RTLS vendor.

Notes:

Australia Sponsor:

Hospira Pty Ltd,
Melbourne VIC,
Australia

Telephone: 1300 046 774